AN ASSESSMENT OF SECURITY MEASURES AT THE MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

by

MKATEKO PHILLIS MUNYAI

Submitted in accordance with the requirements for the degree of

MASTERS

In the subject

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR DORAVAL GOVENDER

OCTOBER 2022

DECLARATION

Name: **Mkateko Phillis Munyai**

Student Number: **38893207**

Degree: **MASTER OF ARTS IN CRIMINAL JUSTICE**

Title: **AN ASSESSMENT OF SECURITY MEASURES AT THE MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA**

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

2023/02/16

MKATEKO PHILLIS MUNYAI **DATE**

ACKNOWLEDGEMENTS

First and foremost, I would like give praise to “God All Powerful” for giving me strength and encouragement throughout all the processes of completing this dissertation. I am truly grateful for His unconditional grace, mercy and favour well displayed to make this journey smooth. I also convey my gratitude to the following individuals and entities:

- To my Supervisor, Professor Doraval Govender, I am extremely grateful for your invaluable advice, continuous support, patience and feedback during my Master’s dissertation. You truly shepherded me; without you, I do not know where I would be. With your unselfish experience in the public and private security and police service you managed to pick me up and take me where I am supposed to be. May God Bless you.
- To my amazing family – especially my dearest husband – Lufuno Munyai, my two beautiful children, Unarine and Ndivho Munyai, thank you for your patience, support and encouragement in my endeavours throughout this very long journey. You were used to see me carrying my laptop and books the whole day, from the bedroom, to the kitchen, sitting room and even eating with it on my lap.
- To Lucert Chabalala, my dear friend. I am grateful for our friendship chats and your personal support along the way. Very often, our conversations gave me insight, clarity, new ideas, inspiration and direction that helped me complete this research.
- To my wonderful mother; “Mamaila Florar Rhangani” – you helped me to take care of my house and children whenever I was committed with my studies and work. I do not think you know how much your presence helped me to the end of this process. I am the luckiest person in this world to have you. “Niri leyi I mihandu ya nwina ‘nwa Mahlaule, Mapengo wa homu ya ntima khoveni.”
- To the South African Police Service, its management and personnel at Durban and Cape Town Maritime Ports of Entry. Thank you for giving me written permission and for your willingness to impart your knowledge to make sure that this study becomes a success.
- To Unisa, thank you for affording me the opportunity to develop in knowledge

and experience through this study.

- This endeavour would not have been possible without the generous support from my employer and Unisa M and D Bursary, who financed my research.

SUMMARY

This research was conducted because of the increase in national, cross border and international threats at Maritime Ports of Entry in South Africa. The purpose of the study was to improve security at Maritime Ports of Entry in South Africa.

The researcher followed a qualitative research approach using the case study design. Two Maritime Ports of Entry, Durban and Cape Town, were purposively sampled for this study, based on specific criteria. Data were collected using interviews, observations, and document study. The data were analysed descriptively using the thematic analysis process.

It was found that the reducing of threats, eliminating vulnerabilities and mitigating security risks has been challenging owing to weak security control measures at Maritime Ports of Entry. The study suggests that skilled human resources, improved physical protection systems (PPS) and a centre for managing security information and intelligence will enhance security measures at Maritime Ports of Entry.

Keywords: maritime security, threats, vulnerabilities, security risks, security risk control measures, security survey, physical security, port officials, illegal goods, Ports of Entry.

ABBREVIATIONS

AIM	African Integrated Maritime
AIS	Automatic Identification Systems
AU	African Union
BCOCC	Border Control Operational Coordinating Committee
BRICS	Brazil, Russia, India and South Africa
CBP	Customs and Border Patrol
CCTV	Closed Circuit Television
COVID	Coronavirus Disease
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership against Terrorism
DAFF	Department of Agriculture Forestry and Fisheries
DEFF	Department of Environment, Forestry and Fisheries
DHA	Department of Home Affairs
DOT	Department of Transport
EEZ	Exclusive Economic Zone
EU	European Union
GPS	Global Positioning System
IBSA	Indian Brazil South Africa
ICO	International Coordination Centre
IMO	International Maritime Organisation
IORA	Indian Ocean Rim Association
IRCA	Immigration Reform and Control Act
ISPS CODE	International Ship and Port Security Code
ISS	Integrated Security System

ISSC	International Ship Security Certificate
ITS	Identification and Tracking System
IUU	Illegal, Unregulated and Unreported Fishing
KM	Kilometre
LRIT	Long-Range Identification and Tracking
MLRA	Maritime Living Resources Act
MRCC	Maritime Rescue Coordination Centre
MTSA	Maritime Transport South Africa
NDOT	National Department of Transport
NSMS	National Strategy for Maritime Security
PPS	Physical Protection Systems
PSIRA	Private Security Industry Regulatory Authority
PTZ	Pan, Tilt and Zoom
RFID	Radio-Frequency Identification
SA	South Africa
SADC	Southern African Development Community
SAFE	Security and Accountability for Every Port
SAMSA	South African Maritime Safety Authority
SANDF	South African National Defence Force
SAPS	South African Police Service
SARS	South African Revenue Services
SOLAS	Safety of Life at Sea
SSAS	Ship Security Alarm System
SUA	Convention for The Suppression of Unlawful Acts
TAPA	Transported Asset Protection Association

TNPA	Transnet National Port Authority
TPT	Transnet Port Terminals
TWIC	Transportation of Worker Identification Credential
UNISA	University of South Africa
UN	United Nations
UPS	Uninterruptible Power Supply
USA	United States of America
VTS	Vessel Traffic System

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION AND MOTIVATION FOR THE RESEARCH

1.1 Introduction

Security risks confronting Maritime Ports of Entry both nationally and internationally have provoked much public debate and media attention around the world. Maritime security in Africa remains a serious issue for the wider international maritime communities (Potgieter and Rommerin, 2009:ii). Maritime security is understood to be a task or operation conducted to protect maritime transportation to the advantage of the state and its citizens. It requires collaboration by the government and traders within marine industries. The threats posed to maritime security have been of great concern throughout maritime history because marine forces controlled the sea for their own purposes (Manig, 2017:37). The 11 September 2001 terrorist attacks against the twin towers of the World Trade Centre in New York City, the Pentagon in Arlington, Virginia and Pennsylvania and a subsequent well-known terrorist activity have significantly changed the future of our border security (Asiamah, 2018:16). Such incidents call for intensive maritime security research.

Seaborne trade handles billions of dollars in freight every year as the world commercial merchandise is shipped via the ocean, airborne and road transport, and is received from the exporter at different Ports of Entry. South Africa has the busiest international ocean trade sea routes (Botha, 2019). The eight busiest shipping ports in South Africa include the port of Saldanha Bay, Cape Town, Mossel Bay, Ggeberha (Port Elizabeth), East London, Ngqura (Eastern Cape), Durban, and Richards Bay (Ramsaroop, 2016:39). Ports and harbours in South Africa operate as an important trading hub with countries that are within the Southern African states and with shippers to and from all over the world (Manig, 2017:10). Seaborne trade contributes about 80 to 90 percent of the South African economy.

This chapter discusses the rationale for this research, the problem that has been researched and the research questions that were used to achieve the research aim and objectives of this study. This is followed by key theoretical concepts/ definitions and an outline of the study.

1.2 Rationale for the study

The reason to improve security measures at Maritime Ports of Entry justifies the need for this study (Maree, 2007:28). It is the role of the marine industry to ensure continuous effective cooperation and understanding between all maritime security stakeholders with security responsibilities (McNicholas, 2008:90). Christopher (2009:275) describes maritime security cooperation as identifying relevant challenges and providing collective mitigating actions for maritime security. In support of this, Christopher (2009:276) explains that the Port of Miami has established an executive Security Steering Committee to develop and strengthen its cooperation. The Committee helps the port to gather relevant information to neutralise its risks. A similar platform of global risk specialists has been initiated by the USA Government to assist states to develop strategies and risk assessment practices (Christopher, 2009:277). This shows a common interest and the foundation of fruitful cooperation around addressing maritime issues. This means that continuous cross-border cooperation, information sharing, and increasing joint operations among maritime security stakeholders is crucial for safety and security within the maritime environment (Bell, 2018:1).

The interest in maritime security has increased humanitarian and developmental aid, and has brought peace and security to Africa by limiting illegal immigration, combatting illegal waste dumping, and promoting fishing (Potgieter and Rommerin, 2009:ii) but enforcing the law and maintaining good order at sea is still a challenge for the marine environment (Potgieter and Rommerin, 2009:5).

The complexity of maritime security and the degree of threats it is facing require an integrated effort of states regionally and internationally (Vrey and Mandrup, 2015:11). The implementation of this protocol makes it hard to prevent illegal immigration (Ali, 2014:3). International maritime trade, security contractors and companies operating on the coastal areas of Africa require protection and safe passage for shipping (Potgieter and Rommerin, 2009:ii).

Effective security measures protect the ports from security risks. The 2015 Drugs and Crime Report of the United Nations suggests that South African ports need to be protected from becoming major routes for drug smuggling and human trafficking

(Hutsun, 2018:1). Port facilities have a continuous flow of local and international people entering and leaving the country every day. Therefore, attention should be directed to daily visitors, including, truck drivers, dock workers, vendors, security officers, and law enforcement agents who have access to critical infrastructure (Neely, 2012:3).

The economic contribution of seaborne trade has increased maritime security challenges such as weapons of mass destruction that may enter the Ports of Entry unnoticed (Neely, 2012:3). In addition, port authorities must be able to recognise illegal activities at the Maritime Ports of Entry to reduce the threats of smuggling, theft, and vandalism (Minnaar, 2001:4). Criminals and terrorists are aware of these challenges as well as the systems used to protect the critical infrastructure. They often use social media, the internet and the news to source information for criminal activities by exploiting the weaknesses of the ports.

Technology can be used to improve port security (Neely, 2012:8). It can be used to inspect containers to detect various types of contraband and unauthorised persons (McNicholas, 2008:361). Bichou, Szyliowicz and Zamparini (2013:19) point out that a port can be targeted from a remote location by technology or other means. African regions should invest in technology and focus on constructing secure information-sharing networks and maritime surveillance capabilities (Vrey and Mandrup, 2015:45). Bichou et al (2013:14) also suggests that significant investments should be made in the security of infrastructure facilities in ports which are the mainstay of global maritime transport.

The 11 September 2001 terrorist attacks have forced the International Maritime Organization (IMO) to make drastic changes to its laws regarding ports and shipping administration constitutions. The ISPS Code is a set of measurements implemented by IMO to strengthen the security of ports, goods, vessels and the shipping industry (Christopher, 2009:33). It has become an international framework for cooperation between government authorities, port authorities, shipping companies, and seafarers through a series of measures for transnational security. The code applies to ports and ships of signatory nations to the standard of the Safety of Life at Sea (SOLAS) Convention. The code further expects participating governments to establish specific

actions to ensure compliance with these standards (McNicholas, 2008:93) as a way to manage maritime security risks. It assesses maritime threats, evaluates the risk, and administers appropriate measures to protect maritime ports and ships (Bichou et al, 2013:218).

1.3 Research problem

A research problem states the issues and gaps in knowledge that require research (Welman, Kruger and Mitchell, 2005:12).

South Africa's first democracy in 1994 opened the doors to worldwide economic, political, and social developments. It also caused the rise of threats to national security that exposed the Maritime Ports of Entry in South Africa to an expanding range of criminal networks such as organised crime, drug smuggling, illegal immigrants, and weapon dealers (Minnaar, 2003:23).

The 11 September 2001 terrorist attacks brought an increased awareness of maritime security threats, vulnerabilities, and security risks within Maritime Ports of Entry (James, 2011:11). Efforts were made by the Ports of Entry to take steps to deter illegal activities. Port officials play an important role as the first line of defence against external threats, intrusion and vulnerabilities caused by cross-border people and goods that break the laws intended to protect the port (James, 2011:11).

The roles and responsibilities of maritime port officials therefore need to be investigated. The results of factor analysis have shown that, in the face of the challenges of seaports, maritime port officials have difficulty defending the consistency of their port security measures (Liwång, Sörenson and Österman, 2014:1). Presently, maritime security focuses on physical security measures, shipboard security, and marine security issues such as illegal immigrants, stowaways, port security, and terrorism. Regional and international bodies are compelled to introduce mitigation measures to improve maritime security at their different Ports of Entry (Potgieter and Rommerin, 2009:6). In assessing the level of security at Maritime Ports of Entry in Durban and Cape Town, South Africa, this research discusses the challenges of threats, vulnerabilities, and security risks at Maritime Ports of Entry in Durban and Cape Town, South Africa, to understand the processes, procedures, and requirements

of security.

1.4 Research questions

The researcher addressed the following research questions in the study:

- What are the threats, vulnerabilities, and security risks confronting Maritime Ports of Entry in Durban and Cape Town?
- What are the roles and responsibilities of maritime security officials in ensuring security at the Maritime Ports of Entry in Durban and Cape Town?
- Which security measures need to be improved at the Durban and Cape Town Maritime Ports of Entry?

1.5 Research aim and objectives

This study assessed security measures at Maritime Ports of Entry in Durban and Cape Town, South Africa. The specific objectives that were identified to achieve this aim (Fouchė and De Vos, 2011:94) include the following:

- To identify threats, vulnerabilities and security risks confronting Maritime Ports of Entry in Durban and Cape Town, South Africa;
- To establish the roles and responsibilities of maritime security officials in ensuring security at Maritime Ports of Entry in Durban and Cape Town, South Africa; and
- To identify security measures to improve security at the Maritime Ports of Entry in Durban and Cape Town, South Africa.

1.6 Key theoretical concepts

1.6.1 Maritime security

Maritime security contains preventive measures to protect the marine domain against international threats from sabotage or terrorism activities (Fransas, Niemnen, Salokorpi and Rytkonen, 2012:07). The Maritime Institute of Technology and Graduate Studies (2021) defines maritime security as the internal and external protection of vessels against dangers such as terrorism, piracy, robbery, illicit trafficking of

commodities and persons, illegal fishing, and pollution. Vrey and Mandrup (2015:166) add that maritime security is a cooperative pursuit by marine agencies for a safe and secure maritime environment.

1.6.2 Port of Entry

A Port of Entry is a facility that provides access control services to people and goods entering and leaving the country (Mashiri and Chakwizira, 2016:100). According to The "PEW" Charitable Trusts (2015:6), Ports of Entry receive immigrants, tourists, and goods, charge duties and implement the law and regulations on imports and exports.

1.6.3 Security risk

A security risk refers to an individual or circumstance that can cause a threat to the safekeeping of an environment (Govender, 2018:15). Stoneburner, Goguen and Feringa (2002:8) consider a security risk as threats to ships moving from one port to another that exploit weaknesses for the profit or personal interest of individuals or groups.

1.6.4 Vulnerability

Vulnerability is when the system or part of it fails to react favourably or to prevent damage during the occurrence of a given risk (Proag, 2014:369). Vulnerability is a weakness that may be inadvertently caused or exploited deliberately (Stoneburner et al, 2002:12). Vulnerability facilities include government structures and private sectors that form part of national economy which may be exposed to security risks (Einstein and Philpott, 2011:4).

1.6.5 Threat

A threat is an act that predicts the intention of causing pain, injury, or damage to someone, something (Brusco, 2016:2852) or an organisation's framework or system (Jenkins, 1998:6). According to Carpenter (2013:1), threats to ports include transporting illegal goods or people or using a ship as a weapon of mass destruction. Threats to ports range from organised criminal groups smuggling arms, trafficking humans and goods, stealing cargos as well as damage to port security (Jenkins,

1998:5).

1.6.6 Port officials

Port officials are responsible for the port's daily operations at the Ports of Entry (Phelps, 2014:95). Port officials comprise different institutions that work together to protect the country by detecting and removing threats to its people and goods. They carry out inspections using well-developed risk assessments to detect violations and enforce compliance (Department of Homeland Security, USA, 2015:2).

1.6.7 Illegal goods

Illegal goods are all imported commodities, weapons, drugs, or non-goods which may pose a security risk (Rosenblum, Bjelopera and Finklea, 2013:10). According to Fagan (2011:3), illegal goods are defined as goods and services (such as illicit logging and wildlife, drugs, and arms) including legal goods that are moved in and out of the borders by circumventing customs and duty taxes. Eurostat (2018:18) describes illegal goods as the production and circulation of drugs and weapons that are passed across a border where it is illegal to do so.

1.6.8 Security risk control measures

Security risk control measures are countermeasures prepared to prevent, detect, delay, or minimise security weaknesses of company property or equipment (Govender, 2018:15).

1.6.9 Security survey

A security survey is a thorough physical assessment of a business and its processes to examine the risks and the measures in place to mitigate and to guard them against criminal threats (Govender, 2018:96). According to Pena (1997:4), a security survey is a thorough examination of a port's weaknesses to eliminate risks and to countermeasure losses.

1.6.10 Physical security

Physical security is measures designed to protect people, weapons, installations

systems, and documents from threats related to terrorism, murder, robbery, corruption, and theft (Christopher, 2009:86). Physical security includes all external and internal perimeter protection equipment, technologies, and resources that include sensors, Closed Circuit Television (CCTV) cameras, lighting, and access controls (Einstein and Philpott, 2011:7).

1.7 Outline of dissertation

Chapter 2: Research Methodology

This chapter discusses the research approach, the design and development of data collection instruments, collection of data, data analysis processes, ethical considerations, reliability and validity, and the research limitations.

Chapter 3: Security at Maritime Ports of Entry

This chapter reviews the literature to support the research questions and objectives of the study. It is informed by both the national and international literature on security measures at Marine Ports of Entry.

Chapter 4: Analysis and interpretation of data

This chapter describes the methods used to analyse and interpret the data.

Chapter 5: Findings, Recommendations, and Conclusions

This chapter discusses the findings and recommendations of the study.

1.8 Conclusion

Security measures remain the most significant concern for Maritime Ports of Entry in South Africa. Maritime security measures should address the complexity of threats, vulnerabilities, and security risks experienced daily. The trafficking of drugs, weapons, and persons, and the hijacking of ships disrupt the supply chain for maritime security. Ensuring the security of Maritime Ports intended to protect people, goods, and port facilities is critical to strengthening international trade. Practical legislative measures taken by the state to deal with this problem should be appraised regularly. The problem

of threats, vulnerabilities, and security risks is a very complex issue that affects the Maritime Ports of Entry negatively. An assessment of the threats, vulnerabilities, and security risks is important to the security of Maritime Ports of Entry worldwide.

CHAPTER 2: RESEARCH METHODOLOGY

2.1 Introduction

A successful study necessitates a careful selection of a research strategy that includes qualitative, quantitative and mixed method techniques. A qualitative approach entails describing, interpreting, contextualising, and acquiring a deep understanding of the concepts or phenomena under study. To examine security measures at Maritime Ports of Entry, the researcher took a qualitative approach. The goal was to create descriptive knowledge regarding maritime security officials' behaviours, social structures and shared views. Because qualitative research methods are less controlled and more interpretive, the researcher's participation and observation influenced the study's outcomes.

The researcher chose a case study design for in-depth, multifaceted explorations of difficult issues in their natural settings. In social science research, thematically linked questions are used to look into current events in their natural settings. The research paradigm, interview schedule, observation checklist, and documentary study checklist were employed to collect data. The data were analysed thematically.

This chapter discusses the methodological framework, which includes the research strategy, approach, philosophical assumptions, data collection methods, sample selection, processes, and data analysis for the study. It also describes the study's reliability before concluding with ethical difficulties, limitations, and the value of the study.

2.2 Research approach

The nature of the research problem, issues to be addressed, and study participants all influence the choice of a research approach (Creswell, 2014:31). The qualitative approach helps in the understanding of complex situations by utilising real-life experiences, meanings, and perspectives of participants. In order to test objective theories, the quantitative approach investigates the relationship between variables. A mixed method approach is one in which researchers combines both quantitative and qualitative methodologies to better comprehend the phenomena being studied

(Fouchė, 2021:41).

The researcher employed a qualitative approach to collect data through one-on-one online telephonic and email semi-structured interviews, purposive observation, and secondary data. The present security measures at Maritime Ports of Entry were assessed using a qualitative technique, in which the researcher engaged with participants through observation and dialogue, allowing them to relate their personal experiences with the subject. The researcher began by formulating the research questions using an inductive approach (Fouchė, 2021:42). The inductive method helped the researcher extract meaning from the collected data set, identify patterns and linkages, formulate generalised theories and draw research conclusions. Because it can handle small samples and offer qualitative data analysis, the inductive technique was the best choice for this study. After finding themes, the researcher used a deductive technique to create interpretative narratives from the data to represent the intricacy of the phenomena under study (Fouchė, 2021:41).

2.3 Research design

The how, what, and why questions are crucial to this research, hence a case study methodology was used. Researchers utilise case study research as a method, design, methodology, and strategy to learn how people interpret their life experiences (Schurink, Schurink and Fouchė, 2021:302). The researcher conducted a case study to understand the day-to-day work of maritime security officials (Ponelis, 2015:537).

Face-to-face interviews, on-site observations, and the analysis of incident reports were the three data gathering methods planned for this research to investigate the perspectives of participants in order to find commonalities (Schurink et al, 2021:303). Due to the social distancing restrictions of the Covid-19 pandemic, the researcher collected data for this study by online-telephonic and email interviews, purposive observations, and secondary data because gaining permission to conduct on-site observation was not granted by the responsible gatekeepers. Purposive sampling was used to target specific maritime security officials with relevant experience and knowledge of the inner and outer layers of security needed for site observation. Purposive interviews were conducted to obtain data on the observation checklist in

place of on-site observation (Strydom, 2021a:337). Since permission was not granted by the South African Police Service to conduct case docket analyses (documentary study), the researcher used similar studies relating to Maritime Ports of Entry to obtain secondary data in support of the documentary study (Strydom, 2021a:348).

The case study design helped the researcher to collect information from maritime security officials on threats, vulnerabilities and security risks from the participants' personal work experience (Leedy and Ormrod, 2013:141). This helped the researcher to identify gaps in security measures for future improvements (Ponelis, 2015:537). The online-telephonic and email interview transcripts, observation checklists and data from the documentary study were analysed using thematic analysis in which data were coded and clustered under themes and categories (Leedy and Ormrod, 2013:141).

2.3.1 Research paradigm

Qualitative research starts with a new set of assumptions. This is the researcher's statement of beliefs about the nature of reality, what can be learned about it, and how to learn more about it (Rehman and Alharthi, 2016:51). The interpretative research paradigm influenced the way the researcher organised this study, chose the population and target sample, collected data, and analysed and interpreted the results (Sefotho, 2021:4).

A paradigmatic framework prompted the researcher to consider the broader philosophical implications of her viewpoints (Ponelis, 2015:537). As discussed below, the research design procedure for this study included a philosophical set of common ideas and assumptions concerning ontology, epistemology, and axiology, as well as methodological views (O'Gorman and Macintosh, 2015:54).

Ontology

The philosophical study of the nature of reality is known as ontology (Sefotho, 2021:7). The ontology framework determines the reality of the phenomenon under study (Sefotho, 2021:6). To construct reality and learn more about the participants' ordinary work experiences, the researcher used one-on-one online-telephonic and email interviews, purposive observation, and secondary data. The approaches employed allowed the researcher to comprehend the threats, vulnerabilities, and security risks

that Maritime Ports of Entry face on a daily basis. The researcher transcribed the data collected for analysis and interpretation of the findings (Sefotho, 2021:8).

Epistemology

The study of knowledge is known as epistemology. Its goal is to describe the nature of knowledge (Rehman and Alharthi, 2016:52). Threats, vulnerabilities, and security risks affecting Maritime Ports of Entry were identified using the participants' knowledge. The data regarding the level of risks posed by the current security measures were obtained from the participants' experiences (Sefotho, 2021:8).

Axiology

Axiology is a philosophical study of value and principles that reveals a unique viewpoint. Ethics and aesthetics are the two main categories of values. Ethics was chosen above aesthetics in this study because ethics is a classification of scientific morals in research (Sefotho, 2021:10). Before starting the study, the researcher sought approval from the Unisa ethics committee because the study involved conducting interviews and gathering data through interactions with maritime security officials. The ethical clearance guidelines from Unisa included anonymity, confidentiality, and informed consent. The researcher respected the confidentiality of the participants in this study.

2.3.2 Methodological choice

Methodology is a framework that contains the plan, process, design and methods chosen to achieve the desired outcomes (Moon and Blackman, 2014:1). As advised by Sefotho (2021:11), the researcher used online-telephonic and email interviews, purposive observations and documentary study (secondary data) to investigate the complexity of Maritime Ports of Entry in real settings. An interview schedule was utilised to record participants' replies during online-telephonic and email interviews with different maritime security role players working at Durban and Cape Town Maritime Ports of Entry (Yushan, Oksavik and Hildre, 2020:661). Purposive interviews were conducted to collect observation data. The observation checklist was completed during the purposive interviews. A documentary study checklist was used to collect documentary study data from secondary data sources (Strydom, 2021c:347).

The interpretive approach was employed to give context to the data that were gathered for this study. The researcher chose the interpretative approach because the study was complex and required in-depth knowledge of a participant's social world to answer the research question (Sefotho, 2021:11).

2.4 Population and sampling

The population and sampling table indicate the unit of analysis of the population and the sample groups used in this study.

Table 2.1: Population and sampling table

UNIT OF ANALYSIS	POPULATION	SAMPLE
Ports of Entry	Eight	Two (2): Durban and Cape Town ports of entry
Security officers	200	10
Customs officials	120	10
South African Police Service (SAPS)	120	10
South African National Defence Force (SANDF) officials	100	10
South African Maritime Safety Authority (SAMSA)	60	10

Source: Prepared by Researcher (2019)

2.4.1 Population

The population refers to all potential subjects whose characteristics are of interest to the researcher (Strydom, 2021a:228). It involves people, groups, organisations, and the products of people and events or situations in which they appeared. Population restricts the extent of the research and provides environmental and textual signals. Such constraints allow the researcher to focus on the collection of relevant data (Casteel and Bridier, 2021:343).

The unit of analysis for the study comprised Maritime Ports of Entry security officials, customs officials, South African National Defence Force officials (SANDF), South

African Maritime Safety Authority officials (SAMSA) and South African Police Service (SAPS) officers. Proposed population size included eight Maritime Ports of Entry, 200 security officers, 120 customs officials, 100 SANDF officials, 60 SAMSA officials, and 120 SAPS officers working at Durban and Cape Town Maritime Ports of Entry. The researcher used the population sample groups for this study as depicted in Table 2.1. The participants in this research were chosen because they are directly involved in maintaining the day-to-day security of Maritime Ports of Entry.

2.4.2 Sampling

The method employed to choose a sample has an influence on the reliability of the study findings (Creswell, 2014:42). In sampling, the researcher selects individuals from the study population to serve as representatives. The technique of data collection and the objective of the study dictate the sample size in qualitative research (Bertram and Christiansen, 2014:63). According to Strydom (2021b:382), selecting a sample minimises sampling errors and achieves maximum precision for a given outlay of resources. Furthermore, the researcher used her own discretion in selecting the study's sample of participants. Strydom (2021b:382) believes that, by selecting a sample population, the researcher is able to collect data that are representative of the population under study.

Sampling designs are classified into two types: probability and non-probability (Creswell, 2014:42). This study's participants were chosen using non-probability sampling that cannot predict the possibility of participants being included in the sample (Strydom, 2021b:382).

The purposive sampling technique was used to target a sample of people who are knowledgeable and experienced about the focus of the study in order to capture a variety of perspectives on the study's objectives (Strydom, 2021b:381). Purposive sampling is a non-probability sampling strategy in which the researchers use their own expertise to select the sample that best fits the study's criteria and interests (Strydom, 2021b:382). The researcher selected maritime security officials from the relevant departments as representatives because of their work experience in the maritime security and Ports of Entry. According to Creswell (2014:42), participants in qualitative

studies are chosen because they possess characteristics that could provide insight into the research.

2.4.2.1 Sampling of the Maritime Ports of Entry

The researcher used purposeful sampling to select study sites. The population sites consisted of eight Maritime Ports of Entry in South Africa, namely, Saldanha Bay, Cape Town, Mossel Bay, Port Elizabeth, East London, Ngqura (Eastern Cape), Durban and Richards Bay. The researcher used ports of Durban and Cape Town as a sampling site. The researcher concentrated on these two ports because they are the busiest and largest in terms of container capacity. According to the researcher, the busier a port of entry is, the greater the security risks it faces due to a variety of factors such as porous physical protection systems, poorly trained security officials, corruption, and inadequate security measures. As a result, the security assessment was carried out at the Ports of Entry in Durban and Cape Town.

2.4.2.2 Sampling of interview participants

The initial interview sample group included 30 maritime security officials from the Durban and Cape Ports of Entry. These were permanent employees who worked at the Maritime Ports of Entry from January 1 to December 31, 2018. They were security officers and SAMSA officials working for Transnet National Ports Authority (TNPA), as well as SARS, DHA, SAPS, and SANDF officials. These participants were chosen because their work is a collective responsibility and they were able to provide richly textured information relevant to the phenomenon under investigation (Strydom, 2021b:382). To collect data during online-telephonic and email interviews, an interview schedule instrument was used.

Purposive sampling, as a non-probability sampling approach, was used to target potential maritime security officials positioned at the Maritime Ports of Entry in Durban and Cape Town. Participants' background knowledge and experience in Maritime Ports of Entry were used as selection criteria.

2.4.2.3 Sampling of on-site observation points

The researcher intended to use the ports of Durban and Cape Town to conduct

observation to assess the current security control measures in terms of physical security, access control, Closed Circuit Television (CCTV) cameras, perimeter fence, and x-ray baggage scanners.

Due to the Covid-19 pandemic restrictions imposed in terms of National State of Disaster, the researcher could not conduct on-site observation with the sample Maritime Ports of Entry (see paragraph 2.11 below). The researcher used purposive sampling to conduct observation on the two sample Maritime Ports of Entry. Two officials working at Transport National Port Authority (TNPA), Security and Compliance Division, deployed at Durban and Cape Town Maritime Ports of Entry, assisted the researcher to complete observation checklist. These two officials were the ports security officers responsible for day-to-day supervision of security at Durban and Cape Town Maritime Ports of Entry.

2.4.2.4 Sampling of documentary study (incident report analysis)

The initial plan was to analyse criminals' methods of operation in cases of illegal movements and smuggling using incident reports. Purposive sampling was planned by the researcher to select cases for incident report analysis. The case study's sampling frame consisted of 30 criminal case docket reports of illegal movements and smuggling investigated by SAPS between 1 January 2018 and 31 December 2018. Because of the limitations discussed in paragraph 2.11 below, the process of selecting specific cases, such as guilty, not guilty, withdrawn, undetected, and pending investigation cases, from a population of 200 did not go as planned.

The SAPS did not grant permission to access the incident reports (see paragraph 2.11 below). To increase the study's overall effectiveness, the researcher decided to collect secondary data from similar research conducted by previous researchers using the documentary study checklist. Secondary data included four articles and one dissertation (see paragraph 2.6.6 below) with related information on threats, vulnerabilities and security risks affecting Maritime Ports of Entry worldwide. Collectively, both methods resulted in a complete sample needed.

2.5 Data collection methods and instruments

Researchers are typically from the social environment being studied and are regarded to be part of the data collecting instrument as they employ their observational skills, trust with participants, and capacity to extract information. Furthermore, researchers are expected to draw on a variety of sources of evidence to employ a variety of data sources and methodologies to achieve convergence and verification. Multiple sources test the trustworthiness (validity) and confirm the reliability of data collected using various methods (Bell and Waters, 2018:140).

An interview schedule was used to collect data from online-telephone and email interviews and an observation checklist was used to collect data from purposeful observation. Because of the limitations outlined above, the researcher used a documentary study checklist to collect secondary data in place of the case dockets analysis.

2.5.1 Design and development of data collection instruments

Data collection instruments are an inquiry tool to investigate issues related to a research question or problem in a qualitative study (Leedy and Ormrod, 2013:1). The discussions below illustrate how the researcher designed and developed the study data collection instruments.

2.5.1.1 Semi-structured interview schedule

An interview schedule is a research instrument that consists of a sequence of questions meant to collect data from participants. Creating an interview schedule allows researchers to plan an interview (Geyer, 2021:358). The researcher compiled a set of open-ended questions to ask participants for their opinions about the security measures at Maritime Ports of Entry based on their prior experience and knowledge of the topic (Bairagi and Munot, 2019:37). A qualitative study has the advantage of allowing the researcher to ask participants to elaborate further on their experiences and knowledge on topics that came up during the interview (Geyer, 2021:358).

Semi-structured interviews were conducted using online-telephonic and email interviews considering the Covid-19 pandemic. Participants were required to sign an

informed consent form before the interviews began. Telephone interaction was formed to establish a relationship and to follow up before, during, and after the interview process.

The researcher developed semi-structured questions that were used during the interviews to assess threats, vulnerabilities, and risks at Maritime Ports of Entry. The interview schedule contained thirty-one (31) semi-structured questions, all of which were asked to each participant.

The researcher used a literature review to construct the interview questions (Geyer, 2021:358). Mind mapping was used to formulate sub-questions for each principal question to gain a better understanding of the threats, vulnerabilities, and security measures from the perspective of maritime security officials. To encourage probing, elaboration, and follow-up questions, the topics and questions were presented thematically in a semi-structured manner. The sub-questions followed a logical sequence as guided by an interview schedule.

Semi-structured interview schedule contained the following sections:

Section A: Biographical data

Section B: Threats, vulnerabilities and security risks confronting Maritime Ports of Entry in Durban and Cape Town, South Africa

Section C: Roles and responsibilities of maritime security officials in ensuring security at Maritime Ports of Entry in Durban and Cape Town, South Africa

Section D: Security measures at Maritime Ports of Entry in Durban and Cape Town, South Africa

The South African Police Service, South African Revenue Service, South African National Defence Force, Transnet National Port Authority, Department of Home Affairs and South African Maritime Safety Authority were included in the sample for the online telephonic and email interviews.

2.5.1.2 Observation checklist

The observation checklist was designed and developed taking into account different layers of security, starting from the outer perimeter to the inner perimeter of the Maritime Ports of Entry. The observation checklist contained a list of items formulated by the researcher to record behaviour and situational features during observation (Roestenburg, 2021:207).

The researcher used Durban and Cape Town Maritime Ports of Entry as a research sites to collect data on the security control measures and their suitability to counter threats. The following variables were incorporated into the observation checklist of the selected Maritime Ports of Entry to measure the outer layers of protection: asset removal permits; access control standards; internal controls; perimeter fencing; beams; building access points; motion sensors; alarm systems; detection of explosives; egress control standards; parking areas; seal and tamper indicative devices; barriers; biometric identity verification systems; windows; illumination (lux units); doors; and security patrols.

The following variables were used to measure inner layers of protection: security personnel; employee vetting; system operation; network monitoring; storage areas; closed camera circuit television; finance office; glass breaker; locks and key controls; card readers; fire and smoke detection; alerts and notifications; warning signs; communication devices; search systems; security lighting; document register; security patrols; policies and procedures; security awareness; and emergency evacuation. An observation checklist helped the researcher to identify and monitor threats, vulnerabilities and security risks in the identified variables.

Purposive interviews were conducted online using telephonic and email interviews to address the variables on the observation checklist. Two TNPA officials from the Security and Compliance Division were the fieldworkers requested to assist the researcher to record observational data on the observation checklist. The officials were knowledgeable about the phenomenon being observed (Roestenburg, 2021:208). Permission to conduct purposive interviews to complete the observation checklist was obtained from the TNPA Head of Security and Compliance (attached as Annexure R).

2.5.1.3 Documentary study checklist

Incident report analysis was not conducted at Durban and Cape Town Maritime Ports of Entry because of study limitations. The initial plan was to conduct a documentary study on incidents that were registered on illegal movements and smuggling crimes at Durban and Cape Town Maritime Ports of Entry. The purpose of the study was to identify threats, vulnerabilities and security risks at Maritime Ports of Entry and the modus operandi of the criminals, illegal movements and smuggling at Durban and Cape Town Maritime Ports of Entry and to determine the trends of these crimes in terms of days, weeks and weekends.

The researcher planned to use purposive sampling to select cases such as guilty, not guilty, withdrawn, undetected, and pending investigation cases from the population of 200. The planned sampling frame comprised 30 cases of illegal movements and smuggling crimes documented and investigated by SAPS at the Maritime Ports of Entry for 12 months (1 January to 31 December 2018). A documentary study checklist was designed and developed to gather relevant information during incident report analysis. The checklist contained the following variables: date; time; place; method of operation; and case outcome.

As mentioned under paragraph 2.4.2.4, the researcher used secondary data from four articles and one dissertation (see paragraph 2.6.6 below) with the documentary study checklist to generate information for the documentary study analysis. According to Strydom (2021c:347), researchers can employ secondary data to add value to data already collected by the researcher.

2.6 Collection of data

2.6.1 The role of the researcher

According to Kabir (2016:215), researcher's responsibilities include locating participants, informing them of the study's benefits, and clarifying any unexpected concerns raised by participants. Initially, the researcher intended to employ semi-structured face-to-face interviews, on-site observation and documentary study analysis of case dockets to gather data for the study. However, as a result of the Covid-

19 pandemic and other limitations, the research design had to be changed.

The researcher only used online telephonic and email purposive interviews to collect data for the observation checklist and secondary data sources to complete the documentary study checklist. Due to the Covid-19 pandemic, only ten online-interviews were conducted during data collection.

2.6.2 Protocols in obtaining ethical clearance

Before data collection began, the first stage was to get research ethical clearance from the University of South Africa (Unisa) Ethics Committee. Ethical clearance is required to preserve participants' privacy and gain consent to conduct research according to the methods outlined in the Unisa Ethical Policy (Stuckey, 2014:6). The researcher first received approval from Unisa ethics committee before conducting the study (attached as Annexure A). The researcher maintained ethical research principles to protect the anonymity and confidentiality of data obtained from maritime security officials (Strydom and Roestenburg, 2021:118).

2.6.3 Obtaining gatekeepers' permission

Kabir (2016:2018) states that the researcher should first obtain permission to access the field from the appropriate authorities before beginning the study. Often, researchers must pass via a gatekeeper or someone who can help them to gain access to a population or a site (Leedy and Ormrod, 2015:273). After receiving ethical approval from Unisa, the researcher explored pertinent public domain websites for specific addresses for the gatekeepers' contact information (Kabir, 2016:2015).

After the contact details were established, requests for permission letters were made that included: permission letter to conduct research at TNPA, attached as annexure B; permission letter to conduct research at SAMSA, as annexure C; permission letter to conduct research at SARS, as annexure D; permission letter to conduct research at DHA, as annexure E; permission letter to conduct research at SAPS, as annexure F; and permission letter to conduct research at SANDF, as annexure G, together with informed consent form, attached as Annexure H, interview schedule, as Annexure I, observation checklist, as Annexure J and documentary study checklist, as Annexure

K, were sent by email to the respective heads of the unit of analysis before securing permission for their participation. This included: Transnet National Ports Authority (TNPA)/security officers; South African Maritime Safety Authority (SAMSA); South African Revenue Services (SARS); Department of Transport (DHA); South African Police Services (SAPS); and South African National Defence Force (SANDF). According to Leedy and Ormrod (2015:278), gaining informed consent provides the participants time to exchange information, ask questions and consent or deny their participation.

The subject email stated, “Request for permission to conduct research at Maritime Ports of Entry in Durban and Cape Town South Africa”. The permission letter stated the study's purpose and stressed the study's voluntary nature and anonymity. The letter also stated that the privacy and confidentiality of the information obtained would be respected.

The researcher received both approval and non-approval responses from the gatekeepers. Below is the detailed explanation of the gatekeepers’ responses obtained by the researcher:

Approval letters were obtained from SAPS (attached as Annexure L) and SARS (attached as Annexure M) head offices.

According to the email copied to the researcher by SAMSA training and development manager, approval to conduct the study at Maritime Ports of Entry as well as to conduct interviews with SAMSA officials and Transnet security officers was granted by National Department of Transport (NDoT). For this reason, SAMSA forwarded the same request for permission letter that was emailed to them by the researcher to NDoT head office for their approval (see SAMSA email to NDoT attached as Annexure N). After reviewing the request for permission, the NDoT contacted the researcher by email to inform her that they had authorised TNPA to approve the study (see NDoT email to grant permission attached as Annexure O). The TNPA authorities also called the researcher telephonically to inform the researcher that they had received permission to participate in the study from NDoT. They also said that a secretariat had been appointed to draft the approval letter. They provided the contact details of the secretariat to make follow-ups and to receive updates.

A series of emails and telephonic calls were made by the researcher to follow up with the secretariat and the TNPA authorities on the matter but to no avail. The approval letter to conduct the study has not, at the time of writing, been received by the researcher. This has limited the researcher's ability to conduct interviews with SAMSA officials, TNPA security officers as well as to conduct on-site observation and incidents report analysis at the Maritime Ports of Entry (see study limitation in paragraph 2.11 below).

Two non-approval letters were obtained from the Department of Home Affairs (DHA) (attached as Annexure P) and the South African National Defence Force (SANDF) (attached as Annexure Q). According to DHA, the permission was not granted because the study requires sharing of classified or sensitive information and could expose the existing security measures at the Ports of Entry. On the other hand, SANDF stated that they cannot participate in the study because they are no longer responsible for port security; according to them, the responsibility of port security lies with the Department of Transport (DoT).

2.6.4 Interviews

Semi-structured online-telephonic and email interviews were used to interview participants. Online interviews allowed participants to take part in the study and to answer interview questions in their own time and space. The use of the online telephonic and email interview method was consistent with the Covid-19 protocols and the Unisa ethical conduct for qualitative researchers (Leedy and Ormrod, 2015:278). The researcher chose this method to ensure safety of maritime security officials and to adhere to all Covid-19 restrictions (Geyer, 2021:358).

During the online-telephonic and email interviews, responses were recorded using an interview schedule. The researcher mailed the whole interview schedule to the participants before obtaining consent for the interviews. The interview schedule included a list of open-ended questions and variables that needed to be addressed in a specific order during the conversation (Kabir, 2016:212). The semi-structured interview schedule gave the researcher a clear set of instructions and provided trustworthy, comparable qualitative data. Open-ended questions encouraged

participants to provide rich information that provided new perspectives and understandings on the subject. Open-ended questions were used to encourage the participants to give clarity on problematic areas (Geyer, 2021:358). All participants were asked the same questions to ensure reliability and consistency (Kabir, 2016:212).

Owing to the Covid-19 pandemic, interviews for this study were limited to officials with access to telephones and emails. These were permanent maritime security officials who were employed at the Maritime Ports of Entry during the period of 1 January 2018 to 31 December 2018. All officials who agreed to participate in these interviews signed an informed consent form and then couriered the completed consent form to the researcher (Geyer, 2021:359).

The researcher used telephones and emails to conduct the interviews and to interact with all participants during the process of interviews. The researcher started by reading the interview questions to all of the participants before giving them time to ask questions. This technique helped the researcher to identify participants' prior knowledge of the subject. Participant-initiated questions also helped them to obtain clarity before responding to the set questions and follow-up questions were used to clarify participant replies that were unclear, lacked sufficient depth or detail, or were ambiguous. The questions were written in a language that the participants understood.

The researcher kept participants engaged during the interview by the participants remained active online at a set time for completing the interview. The researcher monitored personal emails regularly for communications from participants, both to keep track of their progress and to issue reminders when responses were not received by the deadline.

The researcher followed the ethical processes outlined in the ethical approval to preserve participants' privacy and obtained consent to conduct research in accordance with the protocol's specified procedures (Stuckey, 2014:6). The researcher also reminded participants that their identity was protected, their participation was valued and their answers were treated with confidentiality (Geyer, 2021:359).

In total, ten interviews were conducted with maritime security officials. All interviews

were handwritten transcripts. This method was chosen by participants themselves to allow them more time to complete the interview questions in their own space and time considering the Covid-19 work-from-home orders. Most participants raised concerns that they did not have laptops or data for internet at home, hence, printing the interview schedule and completing it at home was recommended.

Eight hand-written copies of interview transcripts were collected from the participants' places of work using a professional courier. The remaining two handwritten copies were sent to the researcher's email address by the participants. After receiving the interview transcripts, the researcher stored the collected data in a safe place to avoid tampering and loss of data (Leedy and Ormrod, 2015:278).

2.6.5 On-site observation

The most basic method for data collection is observation. According to Strydom (2021a:336), observation can be defined as a qualitative research method that explores the natural and daily structure of a certain community or setting.

The researcher could not conduct on-site observation because of the study limitation outlined above. The researcher decided therefore to use purposive interviews to ask questions pertaining to the observation checklist at Durban and Cape Town Maritime Ports of Entry. Permission to conduct purposive interviews was requested and obtained from TNPA Security and Compliance division (see attached cell phone message to permit purposive interviews as Annexure R). The TNPA appointed two officials from Security and Compliance Division to help the researcher to complete observation checklists.

The purpose of purposive observation was to assess the current Physical Protection Systems (PPS) at Durban and Cape Town Maritime Ports of Entry. The observation checklist was a guideline used to capture data on the site. The variables included in the observation checklist were the outer layers and the inner layers of protection discussed under paragraph 2.5.3. This process helped the researcher to gather information that was not disclosed during interviews for security reasons. The researcher was also able to uncover the activities of marine security officers in terms of overall preventive security measures.

2.6.6 Documentary study (case docket) analysis

Case docket documentary study analysis was not conducted because permission was not granted by the SAPS as discussed above. Secondary data from similar research conducted by other researchers were used to complete the documentary study checklist. Secondary data were collected from research journal articles and theses/dissertations (Leedy and Ormrod, 2015:71). Many sources were consulted but, after examining them, four articles and one dissertation were selected and were used in this study. The selection of these four articles and one dissertation was based on their content's relevancy to the objectives and research questions of this study (Strydom, 2021a:348). A documentary study checklist was used to collect information from the secondary data sources.

The selected four articles and one dissertation used as secondary data sources are outlined below:

1. United Nations Office on Drugs and Crime. 2011. *Smuggling of migrants by sea*.

2. Moodley, M.M. 2014. *An investigation into the illegal movement of goods from seaports-of-entry: A case study at Durban Harbour*. Unpublished MTech dissertation. University of South Africa, Pretoria

3. Ekwall, E.D. and Lantz, B. 2018.*Theft of goods in ports: A review of TAPA EMEA IIS statistics*. Turku, Finland: Hazard Project.

4. Justus, M., Ceccato, V., Moreira, G. and Kahn, T. 2018. *Crime against trading: The case of cargo theft in São Paulo*.

5. Organized Crime Research Brief. 2018. *Marine ports and organized crime*.

2.7 Data analysis and interpretation

2.7.1 Transcribing of the data

The researcher began transcribing the data soon after they were collected (Ponelis, 2015:542). Once the data were transcribed, the researcher checked the data for

spelling and other errors. The transcribed data was anonymised to hide the participants' personal details (Stuckey, 2014:7). The transcribed data were typed and saved into Microsoft Word or an Excel spreadsheet file.

2.7.2 Data analysis

The data were thematically analysed and interpreted (Schurink et al, 2021).

2.7.2.1 Data familiarisation

Data familiarisation allows for an understanding of data (Schurink et al, 2021:404). The researcher read the transcribed data several times to familiarise herself with the content and to interpret its meaning. Data familiarisation allowed the researcher to learn from participants' experiences of the phenomenon (Javadi and Zaera, 2016:35). Writing memos allowed the researcher to tell the participants stories using patterns from their own narratives (Ngulube, 2015:9). Analytical memos were used because the study's credibility and trustworthiness was grounded on participants' experiences (Schurink et al, 2021:407).

2.7.2.2 Coding

A code is a first step in the analysis process that involves labelling the texts and noting concerns, relationships, and variances that emerge from participants' accounts (Akinyode and Khan, 2018). According to Schurink et al (2021:406), the words and sentences in the transcripts should be labelled with pencil, paper, and coloured markers. The researcher coded the full dataset by writing notes in the margins, underlining key words or sentences, naming the section of the text that had relevant points and repeated concepts from the participant's narratives. After coding, the coded data were grouped into themes and categories based on their similarities and contrasts (Schurink et al, 2021:406).

2.7.2.3 Theme development and categorisation

Themes describe the ideas and experiences of study participants that the researcher believes are important to the research question (Schurink et al, 2021:407). To find similar themes in the datasets, the researcher employed thematic analysis. After

identifying themes, the researcher checked and/or modified them with new information to make them more accurate. The researcher constructed interpretative narratives from the data that were related to threats, vulnerabilities, security risks and inadequate security measures. The researcher opened a file in Microsoft Word and an Excel spreadsheet for each theoretical concept and used it to capture all information related to the concepts or themes. Each theme was given a name and a page number in the data transcripts so that they could be compared to the original transcription. The software system made it simple for the researcher to connect the themes that were related to one another (Schurink et al, 2021:403). Threats, vulnerabilities, security risks, roles and responsibilities, and security measures were used to categorise the themes.

2.7.2.4 Data presentation

The researcher used specific themes to illustrate the emergent explanations as narratives related to the research questions in Chapter 4, leading to the main findings and recommendations in Chapter 5.

2.8 Trustworthiness

The trustworthiness of qualitative studies is determined by four factors: transferability, credibility, dependability, and conformability (Elo, Kääriäinen, Kanste, Pölkki, Utriainen and Kyngäs, 2014:1). According to Gunawan (2015:10), to achieve trustworthiness, the researcher describes the study's data collection processes. Trustworthiness and reliability is discussed in detail below.

2.8.1 Credibility

Credibility is the degree to which participants' impressions and the researcher's presentation of them are consistent (Ponelis, 2015:538). Credibility was attained through the accuracy, honesty and transparency of the data collected from the interviews, observations and documentary studies.

2.8.2 Transferability

The term "transferability" describes how the results of a research may be applied to a

comparable situation to solve the research problem (Korstjens and Moser, 2017:121). The researcher used one-on-one online telephonic and email interviews to access the knowledge and skills of maritime security officials. Each research question was phrased in such a way that respondents could respond in their own unique way. The consistency of data collected from maritime security officials assisted the researcher in making an accurate comparison of the findings. Transferability was confirmed by comparing the results of online-telephonic interviews, purposeful interviews, and secondary data to determine commonality and establish codes and themes.

2.8.3 Dependability

Dependability indicates the quality of the data that were gathered (Ponelis, 2015:538). The researcher explained the processes, including the selection of study participants, data collection, analysis, interpretation of the findings, and reporting of the findings. A professional statistician was also appointed to verify the data collected, the process, methods used, and data analysis procedures to ensure the research's credibility. The data collection methods and management techniques used in the study provided enough information to assist the researcher in generating the findings of the study.

2.8.4 Confirmability

Confirmability implies that the data correctly represent the information supplied by the participants and that the researcher did not fabricate the interpretation of those data (Elo et al, 2014:5). The designs and phrasing of questions in the data collection instruments were reliable in terms of providing the necessary information to answer the research questions. The questions in the interview schedule, the variables in the observation checklist and the variables in the documentary study checklist all measured what they were supposed to measure. Furthermore, the researcher was able to maintain confirmability by preserving documentation and the audit trail of the data collected throughout the research process. Microsoft Word or Excel spreadsheet files were used to keep track of the documents, interview transcripts, the thoughts about the research, ideas, and biases that impacted the objectivity of this research

2.8.5 Reliability

According to Roestenburg (2021:207), reliability is when an instrument measures the same thing multiple times and produces similar results. It has to do with a measurement's stability and consistency of the findings.

Case study methodology was used to improve reliability through interviews, observations and secondary data. The interview schedule, observation checklist, and documentary study checklist assisted the researcher in producing accurate and consistent results. This is because the same questions/variables in the instruments were used for all of the Durban and Cape Town maritime security officials. The data gathered from the three instruments mentioned above led to the answering of research questions and the establishment of findings and recommendations for this study.

2.9 Ethical considerations

The researcher adhered to ethical principles for the research design, data collection, analysis and presentation of research results (Leedy and Ormrod, 2013:104). The participants in this study received relevant information on the purpose and methods of data collection. To ensure voluntary participation, informed consent was employed, and participants were informed that they may withdraw from the study at any time (Strydom and Roestenburg, 2021:121).

The study's purpose was defined in more detail on the participants' information sheets that contained the contact details of the participant, the researcher's supervisor and those of Unisa research ethics committee should participants wish to enquire about the research findings or report any unethical behaviour. Participants had the right and the time to ask questions and voice their concerns (Arifin, 2018:30).

The anonymity and confidentiality of participants' information was also maintained during the data collection, analysis and reporting of study findings (Arifin, 2018:30). Hard copies of participants' interview transcripts were kept in a lockable steel cabinet. Anonymity of participants was protected using numbers to hide the names in the interview transcripts.

2.10 Value of the study

The value to the private security industry

This study will allow the private security sector to provide better maritime security services at sea.

The value to law enforcement agencies (SARS, SANDF, SAPS and DHA)

The findings of the research will aid government stakeholders and role-players to combat local and worldwide maritime threats. The research will convey new risk identification and mitigation methods.

The value to Transnet and SAMSA

The information gathered will aid Transnet in determining the current state of Maritime Ports of Entry, including physical security systems, infrastructure, training of security officials and raising security awareness to reduce the risks associated with the port.

The value to Unisa and other academic institutions

The dissertation will add value to Department of Security Management at Unisa. The completed dissertation will be available and accessible through the Unisa Library and on the related departmental website for future researchers.

The value to South African citizens

The outcomes of this study can inform South African communities of the security risks challenging Maritime Ports of Entry in terms of illegal sailing and smuggling. After being informed of the security challenges, the community may volunteer to offer assistance to the law enforcement agencies with regard to the organised criminal activities that will lead to successful arrests.

2.11 Limitations

The research study was carefully planned during the proposal phase; however, the process was disrupted due to the limitations discussed below:

Covid-19 caused poor participation

The Covid-19 crisis affected this research. With the sudden spread of Covid-19 all over the world, South Africa issued obligatory shelter-in-place orders. As a result of social distancing initiatives and movement restrictions to slow the transmission of the pandemic, the University of South Africa banned all face-to-face interactions between researchers and study participants from 2019. All active researchers and those working on research proposals had to reconsider their study designs to account for social-distancing measures (Jowet, 2020). For this study, face-to-face semi-structured interviews were replaced by online-telephonic and email interviews. The researcher chose this method to ensure safety protocols and adhere to all Covid-19 restrictions.

Most participants were not interested in participating in the study because it was conducted online and not face to face. Some participants consented to take part in the study but later declined because of their rotational work and work-from-home conditions.

Sensitive information

Gatekeepers from key departments had difficulties approving the study due to the sensitivity and security of information in their possession. Many participants who were able to discuss threats, vulnerabilities and security risks at Maritime Ports of Entry were inaccessible or unreachable to form part of the study. This was the case especially in the data to be collected from semi-structured interviews and incidents reports analysis. The key maritime institutions/departments, such as TNPA, DHA and SARS, turned down the study because they felt that most information they had to share was sensitive so they feared that they would compromise or expose the security measures currently in place at Maritime Ports of Entry. Compromising this information was a high risk when compared to the potential benefits of the study.

2.12 Conclusion

Too little is known about security risk challenges at the Maritime Ports of Entry worldwide. The researcher used online telephonic and email, purposive interviews to complete the observation checklist and secondary sources for the documentary study

to identify threats, vulnerabilities and security risks at Maritime Ports of Entry. The researcher supported these methods with a literature study.

CHAPTER 3: SECURITY AT THE MARITIME PORTS OF ENTRY

3.1 Introduction

Maritime Ports of Entry are responsible for regulating the legal flow and preventing illegal entry of people and goods into the country. Society, industry and governments depend on port security for the continued freedom of a democratic society and the growth of a market economy. Threats, vulnerabilities and security risks should be identified by maritime security officials to ensure effective responses. Security control of Maritime Ports of Entry is primarily a multi-departmental obligation that includes robust maritime transport communication and coordination.

The marine environment covers the Ports of Entry, the harbour, coastlines and the Exclusive Economic Zone (EEZ) in the sea. Maritime Ports are inherently at risk of maritime threats because of their geographical areas. They store large quantities of valuable goods and provide many border destinations with efficient links and nodes (Elago, 2020:23). The identified threats, vulnerabilities and risks found at Maritime Ports of Entry include, inter alia, internal conspiracies such as organised criminals, stowaways and smuggling illegal aliens, illegal exports, and drug smuggling. The reduction of threats, the removal of vulnerabilities and the avoidance of risks has been challenging, owing to weak security control at Maritime Ports of Entry. Addressing security at Ports of Entry requires highly knowledgeable and skilled human resources, a wide variety of information sources, surveillance cameras, communication infrastructures and a centre for gathering, analysing and disseminating information (Moodley, 2014:31). A lack of careful monitoring can both expose maritime assets to risk factors and jeopardise the credibility of maritime security. This chapter provides a theoretical framework which can be used effectively and efficiently to enhance security measures at Maritime Ports of Entry.

3.2 The impact of theories on maritime security

The researcher identified three classical theories to support the study. They include the Theory of Probability, Rational Choice Theory and Routine Activity Theory.

3.2.1 Theory of probability

Probability theory maintains that whatever we do always involves risk (Athreya, 2015:292). The theory postulates reasonable thinking to find the most suitable solution to mitigate the risk (Bernstein, 1996:48). The theory of probability uses the frequency of events as the result of an experience to mitigate the risk (Hansen, 2010:iv). In this study, the theory of probability allowed maritime security officials to consider the probabilities of specific risks occurring at Maritime Ports of Entry and to take the most effective measures to mitigate these risks (Bernstein, 1996:101).

The probability theory uses the ISO 31000:2009 Security Risk Management Model that is used globally to handle all forms of risks identified by the theory of probability (Govender, 2018:88). Risk analysis allows an organisation to gain an understanding of each risk, its effects and its consequences. This includes the operational aspects of the acquisition, implementation and ongoing maintenance of physical protection systems (PPS), such as alarm systems, barriers, guards and the installation and maintenance of technological solutions, which incur substantial costs (Govender, 2018:54).

The ISO 31000:2009 describes risk as a consequence (Purdy, 2010:882). Organisational risks may include terrorism, drug smuggling and human trafficking being triggered by security risk factors, including internal and external security systems, corruption and bribes (Govender, 2018:54). Risk identification requires a systematic way of assessing what could happen, when and why (Purdy, 2010:884). It involves defining the risk source, incidents and the cause and possible consequences (Sangathan and Nehru, 2011:4). Historical statistical evidence, analytical research, expert opinions and stakeholders are used to define possible threats to an organisation (Sangathan and Nehru, 2011:4). The main part of the risk management process is to recognise opportunities, analyse them and evaluate whether risk management should be adjusted as well as monitoring and communicating the risk management systems to verify that they meet their risk criteria (Sangathan and Nehru, 2011:i). According to Govender (2018:88), the security risk management model allows organisations to gather, analyse and assess security information and offer guidance on how to handle particular risks that could have a negative impact on the entity being protected. Risk

evaluation is used to compare the effects of the risk assessment process with particular circumstances in order to determine if the risk and its progress are acceptable or tolerable. Risk evaluation aids organisations in decision making processes (Sangathan and Nehru, 2011:6). Risk treatment reinforces the company's new or existing controls. It analyses the cost-benefit and also examines the new risks that each opinion would produce and prioritises the treatment chosen through a scheduled process (Purdy, 2010:885).

Maritime ports are critical components of global supply chains. Ports of Entry threats, such as terrorists, smugglers, drug traffickers and migrants, may result in service delays or port closures, as well as harm to people, property and the environment. Risk management in Maritime Ports is critical in controlling risks and eliminating these possible threats (Nagi, Indorf and Kersten, 2017:491). As in e other organisation, the ISO 31000 offers guidelines, rules and procedures for Maritime Ports of Entry to neutralise or remove potential sources of risks. This involves balancing the principle of protection against organisational constraints such as restricting access, safeguarding trade and integrating the physical plant with screening areas, buffer zones and protection zones (Bernard, 2015:36). The ISPS Code that was established by the IMO contains regulations that define security assessments, annual exercises and drills (Nagi et al, 2017:496).

3.2.2 Rational choice theory

Rational Choice Theory is a theoretical framework developed by Cornish and Clark to describe individuals' actions when committing a crime (Hechter and Kanazawa, 1997:201). According to this theory, people make reasonable choices to avoid punishment for the crimes they commit. They see illegal acts as a measure of expected reward and punishment, measured against anticipated disco risk (Hechter and Kanazawa, 1997:201).

According to Akers (1990:663), criminals see crime as a rational, measured and deliberate. Offenders behave rationally when making criminal decisions; they use their reasoning abilities to weigh the consequences, the cost, and the benefits before acting. The rewards of committing the crime far outweigh the costs of committing a crime for

the offenders. Shariati and Guerette (2017:6) argue that the higher the commitment and risk rewards of the crime, the lower the possibility of prosecution and criminal punishment. Hollman (2013:1) stresses that human rationality is a concept of pleasure-pain. According to Hollman (2013:1), all human's actions are performed with the purpose of maximising pleasure and minimising pain therefore criminality is a rational free will choice (Hollman, 2013:1).

Comte and Lombroso (2010:76) argue that rational choice theory is a classical integrated theory that blends classical and positivist ideas on crime and crime prevention. It helps law enforcement to discourage crime and concentrate on situational variables that influence multiple types of criminal activity. According to Davis and Cragin (2009:170) police and law enforcement need to be informed about an offender's beliefs and motivations to prevent them from committing crime.

The purpose of rational choice theory is to offer an integrated framework on aspects that influence the decisions and behaviour of maritime terrorists and criminal acts. The vulnerability of the Port of Entry, the ship, the goods and the supply chain play an important role in the subjective perception of the risks and the rational decisions of the offenders. Moreover, revenue from terrorist and cross-border activities is linked to the use of drugs, illegal activity and the punishment costs, while calculating legal and illegal way of earnings.

3.2.3 Routine Activity Theory

Routine activity theory was first proposed in the United States by Lawrence Cohen and Marcus Felson from 1947 to 1974 to describe the reasons for committing crimes (Hsieh and Wang, 2018:335). The theory is increasingly applied by many organisations, for example, law enforcement agencies that use the theory to determine, identify and prevent crime (Miro, 2014:1). Cohen and Felson describe three main essentials that are prevalent for a crime to happen, namely, a potential offender who is motivated to commit a crime, a suitable target or victim to which the crime is directed, and the absence of a capable guardian to protect or stop the victim or target (Hsieh and Wang, 2018:335). According to the routine activity theory, the three basic elements listed above have to be in place for illegal activities to take place. The

emphasis of routine activity theory is primarily on crime characteristics rather than criminal characteristics. Hsieh and Wang (2018:338) contend that the absence of law enforcement agencies and the lack of punishment mechanisms give offenders opportunities to commit crimes.

A potential offender is someone with the motive and the desire to commit crime. The offender's motivation is difficult to quantify, hence the routine activity theory of Cohen and Felson struggles to account for it (Miro, 2014:2).

A suitable target is an individual, an object or location. An assessment of the target depends on cumulative weighted variables (e.g. visibility, inertia, value and accessibility) that encourage the perpetrator to commit a crime (Argun and Daglar, 2016:1188). Suitable organisations are extremely vulnerable to a greater probability of "hit rate" in terms of lucrative rewards, financial incentives and other malicious factors (Hsieh and Wang, 2018:337). A successful motive increases the possibility of rewards, such as income, profits, interest, ego gratification and achievement, and the potential motivation of criminal behaviour outweighs the potential punishment and consequences (Hsieh and Wang, 2018:337).

A capable guardian serves as a key agent in this theory as they may interrupt the link between a motivated offender and a successful target, directly or indirectly (Hollis-Peel, Reynald, Bavel and Welsh, 2011:2). The presence of access control measures, CCTV cameras, high tech fences and alarm systems may also be barriers that block criminals (Hollis-Peel et al, 2011:4). Hsieh and Wang (2018:338) argue that the absence of guardianship increases the certainty, speed, and interest of unlawful actions that lead to more crime. Argun and Daglar (2016:1190) contend that the presence of technological guardianship cannot be effective to detect and prevent the offender if the guardian is ineffectual.

The illegal movements and smuggling crimes at the Ports of Entry could increase due to economic, political and social development. The changes in the socioeconomic structure of society and the geographical design of the Ports of Entry make it a potential target for crime (Farrell, Clark, Ellingworth and Pease, 2005:7). Maritime Ports of Entry without effective access control or advanced security methods become targets for criminality. Crime is higher at Maritime Ports of Entry because of the size

and complexity of the maritime commons. The easy access and largely uncontrolled extension of the maritime domain is perceived by criminals to conceal and encourage their illegal activities (Phelps, 2014:156). In routine activity theory, detecting and prevention tools such as cameras, scanners and sensors, act as guardians to strengthen security at the Ports of Entry (Givens, Busch and Bersin, 2018:8). These technological advancements are tools designed to ease the workload of the human guardians (Anagnostakis, 2015:15).).

It may be difficult to define the motivation of criminals at the Ports of Entry, but countering terrorists and other criminal activities or unauthorised access to the port facilities should be carried out. Routine activity theory recommends the use of advanced technologies, such as CCTV cameras for monitoring, restricting access, and target hardening with the use of locks, scanners and sensors, to minimise criminal and terrorist activities (Chetty, 2018:33).

3.3 The nature and extent of security threats, vulnerabilities and risks confronting Maritime Ports of Entry globally

Security at Maritime Ports of Entry has generated discussion, with large cargo obviously being a major target for a wide range of terrorist attacks (Hill, 2015).

Maritime Ports of Entry is seen as a one size fit all location where prospective offenders are deterred; illegal persons and goods transportation are interrupted; lawful trade and travel are facilitated; and operations and outcomes are consistent (Gerstein and Alter, 2018:6). Maritime Ports of Entry involve multiple players that have an interest in port security such as owners, officials, crews, port employees, passengers and the community (Nagi et al, 2017:492). As such, maritime security officials have to follow strict laws to produce and maintain a sound enterprise and a vibrant economy to draw investment both from within and outside the country (Irandu, 2016:130).

Maritime transportation today is facing the difficult task of tightening the security of the ports, especially after the terrorist attacks of 9/11 in the United States. The main port security duties are protecting the people, goods, and facilities through which dangerous materials travel or are stored (Young, Gordon and Plant, 2018:105). The cost of inspecting cargo arriving at ports is high as is the delay caused by checking all

cargo (Hill, 2015).

In the past, Maritime Ports of Entry experienced criminal activities because of a lack of security and also because they were designed to make access easy for shipping to land markets (Leonard, Gallo and Veronneau, 2015:42). Maritime security that included restricted access controls, cargo inspections, identity checks and personnel searches were regarded as slowing down trade (Leonard et al, 2015:42).

Vulnerabilities in Maritime Ports stem from a lack of cross border relationships between country states and maritime personnel giving access to the ports' containers and ships carrying illegal goods and unauthorised people (Gerstein and Alter, 2018:6). In-depth understanding of port operations and geography, including knowledge of security systems, guards and access control procedures, can be established by those who access the port most frequently undermining national security services (Gerstein and Alter, 2018:9).

The reputation of global maritime crime suggests that the port's economic activities are vulnerable to terrorists and other illegal activities (Leonard et al, 2015:42). A break in security has been created by a combination of security and commerce into a single framework that supports the country's national goals as well as political, economic and cultural needs (Gerstein and Alter, 2018:8). The national policies regarding security and commerce define the type of systems and operational capabilities that are in place to enforce control and track terrorist and criminal activities but the reality is that it has been difficult to protect major ports from terrorism (Gerstein and Alter, 2018:8; Moodley, 2014:31).

Ports of Entry comprise highly specialised physical structures and facilities, run in compliance with demanding protocols and procedures (Nagi et al, 2017:492). In many cases, the security of both the outer and inner perimeters of the port facility and its infrastructure are compromised by criminal activities that take place within the Maritime Port premises (Ofosu-Boateng, 2017:21). Moreover, each port has its own rules and security measures with respect to vessel movements, activities, cargos, intentions and ownership that are unique and often difficult to discern (Irandu, 2016:137). The provision of high-tech security solutions, access control measures, lighting, patrols, identification and credentials provide a safe and secure environment, considering the

widely distributed presence of different locations involved (Young et al, 2018:106).

Securing Maritime Ports needs joint efforts on a national and global scale. Sharing maritime information can provide a basis for coordinating maritime security activities conducted with foreign governments and other international bodies (Phelps, 2014:161). Guidelines for maritime protection have been established by the International Maritime Organisation (IMO) and the International Ship and Port Security (ISPS) Code has been adopted (Leonard et al, 2015:45). The ISPS Code offers global maritime authorities a set of guidelines on how to safeguard ships against terrorists or other maritime violators. It also specifies security standards that may be shared among the ships and the port facility to protect the restricted areas of the port. This includes central funding for port security, background checks for port workers and the implementation of advanced technologies and resources (Herout, 2017:50). The Code refers to foreign passenger ships, cargo vessels of 500 gross tonnage or more, international ports of call, offshore drilling facilities and port facilities (Pearl, 2019:27).

Shipments, Maritime Ports, law enforcement and others who are at sea are vulnerable to terrorist and other criminal attacks. Maritime Ports without proper access control or advanced security measures are easy targets for smuggling drugs and illegal weapons. Many Maritime Ports lack police or security personnel to ensure accountability for criminal conduct (United Nations Office on Drugs and Crime, 2017:4). Because some countries have no system in place to detect and prevent prohibited people and goods from entering their countries, this increases the amount of illegal imports being concealed within the legal deli methods (Phelps, 2014:177).

United States of America (USA)

A wide variety of crimes such as drugs trafficking, contraband and counterfeited goods, human trafficking, trade fraud, bribery, extortion, environmental crime and cargo theft are related to illegal activities and Maritime Ports in the USA (Moodley, 2014:38). The USA has more than 143 Maritime Ports of Entry that function as vital gateways to commercial trade. More than 62,000 vessels enter USA ports per year (Pearl, 2019:3). In view of the steady rise in trade in the USA due to the rising population, security in major USA ports needs upgrading (Leonard et al, 2015:42). The top three Maritime Ports in the USA include Los Angeles, Long Beach and New York. Closing one of

these major USA ports because of terrorist attacks is expected to cost the economy $1 billion a day for the first five days which will rise dramatically after that period (Leonard et al, 2015:42).

The USA national security should therefore take all necessary steps to minimise potential risks to Maritime Ports (Phelps, 2014:138). The National Strategy for Maritime Security (NSMS) is the cornerstone of the federal government to protect the Maritime Ports of the nation (Christopher, 2009:72). It drives port security agencies to incorporate both natural and man-made threats into their security planning (Christopher, 2009:72).

Although maintaining the freedom of seas remains the top priority of USA, it is also a challenging task to protect the USA Maritime Ports of Entry. This means that there is an inadequate supply of federal resources and technologies for the nation's maritime defence strategies (Leonard et al, 2015:45). These security lapses are open to terrorists and other criminals (Herout, 2017:76) who are aware of the immense quantity of cargo passing through USA ports that has never been inspected (Leonard et al, 2015:45).

Supply chain makes the Maritime Ports of the USA prone to different types of terrorist attacks. It hinders free flow of goods and services by impacting cross-border trade along the transit routes (Leonard et al, 2015:42). Inspecting e container has been difficult for the USA because of an ever growing number of containers arriving daily (Leonard et al, 2015:45).

The USA has implemented many security initiatives that include technology, training and collaborations with foreign allies that provide an aggressive, in-depth, layered defence (Phelps, 2014:143). They include: the Maritime Transportation Security Act (MTSA) programme; the Container Security Initiative (CSI), the 24-Hour rule and customs x-ray scanners and radiation detection gates (Phelps, 2014:151).

The Security and Accountability for Every Safe Port Act (SAFE) of 2006 was implemented to complement the Transport Workers Identity Card (TWIC), while the Customs-Trade Partnership Against Terrorism (C-TPAT) programme codified the CSI. The SAFE port Act mandated additional requirements to be made available to the

Customs and Border Protection (CBP) in order to enable port security officials to properly execute their duties to identify and prevent high risk containers and to secure container shipments (Pearl, 2019:11). Additionally, the USA is one of the most active supporters of the ISPS Code that has been implemented to protect USA interests from possible maritime abuse (Herout, 2017:74). Furthermore, the MTSA has set up the TWIC to monitor and control the access of personnel (Pearl, 2019:10).

European Union (EU)

European Union Ports of Entry are critical infrastructures and the main service providers to the entire economy (Kallas, 2014:6). Based on a gross weight, 1,723.4 tons of cargo were handled in Europe's top 20 cargo ports in 2015. In addition, 395.4 million seaborne passengers entered and exited through the Ports of Europe in 2015 (Nagi et al, 2017:492).

Drones that can bypass security controls around the port security perimeter, compromise port security in the EU (Confederation of European Security Services, 2017:20). Furthermore, the shortage of security facilities for inspecting goods affects port security and supply chain operations (Carpenter, 2013:62). There are no security requirements for the training and recruitment of maritime security personnel, and no coordination between security management teams that make up the first line of defence (Confederation of European Security Services, 2017:17).

There is also a shortage of organised operations in the Ports of Entry between security personnel, immigration, customs, and general law enforcement that are responsible for daily port operations leading to port attacks (Confederation of European Security Services, 2017:29). The EU has established a situational awareness strategy to guide it on how to resolve Maritime Port problems (Hofmeister and Rueppel, 2014:40) that includes motivating security staff. Furthermore, there is a minimum standard criterion for recruiting, vetting, training and screening of private companies operating in EU ports. The European Handbook of Maritime Security Exercises and Drills contains guidelines to assist EU Maritime Ports in training their staff (Confederation of European Security Services, 2017:24).

Young et al (2018:31) believe that the implementation of the ISPS Code into the

European Union Maritime Ports has improved the security of their ships and port facilities by establishing risk mitigation measures. The ISPS Code requires a 96-hour pre-arrival notification from all foreign ships visiting the EU ports that is used to assess the ship security level and the effectiveness of security measures that guarantee the security level of the ship (Ramsaroop, 2016:12).

Brazil

Brazil is an emerging regional and global leader with both complex challenges and great potential. It is well aware that there is a need for improvements in transport infrastructure and port security (Williams, 2016:172). Rivers that flow into Brazil from others countries through the dense rainforest make up almost 6,000 miles of Brazil's borders. Narcotics and arms smuggling are Brazil's biggest crime problems as drugs, illegal goods and people flow across these poorly managed borders (Rhoades, 2016:285). Brazil is bordered by Bolivia, Peru and Colombia. Due to a lack of administrative capability and a regional security policy, these regions are recognised as the major entry points for cocaine in Brazil (Pinto, 2018:59). Brazil's progress in improving its borders and port security is connected to sustainable growth, collaboration between agencies, technological advancement and international relations (John and Parks, 2016:1). Brazil's port security involves man-made barriers, such as fences, walls and other barricades, to support technical equipment, guard patrols, and access control restriction (John and Parks, 2016:4).

Even though Brazil is among the most dangerous nations in terms of cargo crime, because of the friendly relationship with USA, Brazil is able to mitigate these threats through USA C-TPAT programme (Williams, 2016:171). On June 2011, Brazil released Degree No. 7,496, a developing strategic Border Plan to strengthen cross-border crime prevention, monitoring, inspection, and repression in the Brazilian borders and Ports of Entry (The Law Library of Congress, 2013:38).

India

India's maritime domain is characterised by its multiple maritime facilities within their respective maritime zones, such as economic interests and assets around the borders and Ports of Entry (Narvenkar, 2018:49). The maritime state of India is home to 16

busy main ports and 227 minor ports, which contribute to their economic development (Singh, 2019:20). The lack of adequate security controls at borders and Ports of Entry is the primary cause of ports' vulnerabilities and terrorism attempts to use weapons of mass destruction in India. Such risks are the basis of increased threats that makes the India's ports unsafe for foreign ships (Narvenkar, 2018:50). Kshirsagar and Kumar (2016:295) also note that India's limited investment in human and technological resources increases the threats to its maritime domain.

There is a lack of comprehensive maritime infrastructure and a stable supply chain at the Maritime Ports of India. A new Merchant Shipping Bill signed in 2016 does not resolve India's Maritime Ports' issues (Singh, 2019:15). According to Indian intelligence agencies' 2017 security audit report, India's major ports, including the Blair port trust and Cochin shipyard, lacked radiation detection facilities, while only 54 minor ports comply with ISPS, and about 75 of the 187 minor ports have no security coverage (Singh, 2019:20).

According to Kumar (2016:238), India has porous, vulnerable and poorly guarded costal stretches which are open to abuse by organised criminal gangs (Kshirsagar and Kumar, 2016:238). India's cross border challenges are forests, rivers and mountains along the borders of Bangladesh, Myanmar, and Bhutan. Most goods moved through these borders are not ISPS Compliant (The Law Library of Congress, 2013:74).

India uses both human intelligence and technical developments to safeguard its Maritime Ports. This includes the installation of fencing, floodlighting and the construction of Integrated of Check Posts (The Law Library of Congress, 2013:72).

Indian authorities have mounted radiation sensors in India's premier shipping hubs to screen cargo. The level of India's Maritime Port security has been increased by frequent coastal drills and increased cooperation between agencies (Singh, 2019:21). India has a transponder system installed to allow operators to control the movements of vessels. They also use biometric cards to monitor the operation of ports and harbours and to improve the ability to recognise and trace container movement (Singh, 2019:19).

India has also improved its maritime domain awareness and information sharing. An

information fusion centre set up in Gurugram is an aide to the Information Management and Analysis Centre of the Indian Navy to collect, analyse and exchange information with neighbouring states (Singh, 2019:19). The establishment of a maritime security committee to strengthen Maritime Port security was another step taken by Indian stakeholders and role-players to find collaborative solutions to fight coastal security challenges. These programmes also resolve inter-agency concerns and strengthen cooperation between the Indian Navy, Coast Guard, Marine Police and private maritime entities (Singh, 2019:20).

China

China has a total of 31,862 shipping berths in service, 5,623 of which are in coastal ports, 517 that can accommodate ships of 10 000 tons and more. China has seven of the world's top ten container ports. China's Maritime Ports include a complex range of operations, highly fragmented infrastructure, very diverse tenants, numerous modes of transport and a large volume of people, equipment, vehicles, cargo and vast lands, making ports vulnerable to illegal activities and terrorist attacks (Irandu, 2016:146).

China is trying to make its Maritime Ports free from terrorism and other criminal attacks. Procedures and technologies have been introduced in the ports of China to ensure the security of goods and people. Several security steps have been enforced at the port of Shanghai, the largest port in China and in the world (Irandu, 2016:155). These include 24 hour security guards and reinforced berth patrols, as well as surveillance cameras around the port. To strengthen security of the port of Rizhao, an intelligence security system has been introduced with Global Positioning System (GPS) location monitor, electronic eye target surveillance, motion detector alarms, digital imaging and facial recognition. At the Shanghai ports, electronic locks with Radio-frequency identification (RFID) technology have been introduced (Irandu, 2016:155). Lastly, the use of x-ray systems, human life detectors, micro vibration sensors, and perimeter security systems for infrared intrusion have made it harder for criminals to smuggle their contraband at Shengzhen port (Irandu, 2016:155).

Australia

It is estimated that four million people are smuggled through Australian borders and

Ports of Entry each year (Moodley, 2014:35). The Australian government is strengthening border controls and collaboration with international law enforcement to jointly counter smuggling, illegal migration and transnational crime. Australia also takes part in international maritime conferences, exercises, capacity building activities and knowledge sharing forums (The Law Library of Congress, 2013:24).

Australia's border agency detects and stops the high rate of illegal transportation of drugs, arms and goods at their Ports of Entry each year. In 2015, Australian border controls discovered 32,880 contrabands, of which 14,899 were major illicit drugs and precursors, weighing a total of around 7,309 kilograms. Moreover, the total revenue estimated for illegal tobacco has been $103 million, comprising 150 tons of loose tobacco and 40 million tobacco sticks detected in the sea cargo environment (Australian Customs and Border Protection Service, 2015:19).

Asia

Within its main ports, Asia has seen a major increase in freight traffic, transforming it into a global trading centre. Safeguarding the Maritime Ports of Asia revolves around information, threat analysis, risk assessments and technological protection measures (Singh, 2019:21). The lack of advanced technologies for credentials and verification, screening and monitoring, tracking, and inspection suggests that Asia is an attractive target for terrorism (Singh, 2019:21).

Public bodies, such as law enforcement, naval forces, and the private sector, are the agencies responsible for the security in Asian ports. The ISPS Code standard, the shipping security and naval patrols have contributed to the enhancement of maritime security (Hofmeister and Rueppel, 2014:30). Asia is also working to increase the number of guards, gates and surveillance cameras, and has developed identification card systems to monitor and manage those with access to critical port infrastructure. Radiation detectors were also mounted to screen critical cargo and identify suspicious shipments (Singh, 2019:13).

Kenya

In recent years, Kenya has seen a number of terrorist attacks in the capital city of

Nairobi, including the bombing of the USA Embassy in 1998 and the Westgate Mall attack on 21 September 2013. Such terrorist attacks pose a substantial threat to the security of containers, passengers and equipment at Kenya's Maritime Ports, in particular, at the port of Mombasa and along the Northern Corridor (Irandu, 2016:130).

Kenya is expected to have the most stable ports in the East African region after completely implementing the Integrated Security System (ISS) project. The ISS conducts security automation in accordance with the specifications of the ISPS Code (Irandu, 2016:133). Furthermore, the use of alarms, cameras, intelligence gathering and physical monitoring challenges the problems of terrorism, counterfeits and substandard goods getting into the local markets (Busiega, 2016:77).

The port of Mombasa has a technological system designed to control the entry and exit of cargo through the doors of the port. The system comprises mechanisms for the detection of optical characters and License Plate Recognition to identify containers and trucks simultaneously for documentation purposes. Moreover, the port of Mombasa is preparing to add hundreds of strategical cameras around the port to operate 24 hours a day (Irandu, 2016:133).

South Africa

The economy of South Africa remains the largest on the continent, and hence considers its national interest as integrally linked to the Maritime Ports' efficiency (Department of Transport, 2017:4). The preservation of Maritime Ports' security is a key component of achieving sustainable economic growth not only in South Africa but across the continent (Manig, 2017:10). Every year, 13 000 vessels carrying 500 million tons of cargo pass through South African ports (Botha, 2019). Durban and Cape Town are Southern Africa's busiest ports. Durban's port handles the most sea-going trade of most ports in Southern Africa (Moodley, 2014:37) and the total cargo handled at the port of Cape Town in 2015 was 4.226 million tons (Ridgway, 2020).

Pre-1994 border and Ports of Entry security was heavily securitised and militarised under apartheid military and police. The post-1994 democratic government demilitarised border security to the roles of immigration, customs and the inspection of goods (Department of Home Affairs, 2016a:14) that are primarily focused on

strengthening restrictions at all Ports of Entry, but fail to improve cooperation among interdepartmental agencies (Moodley, 2014:38). Historically, South African politics has made it difficult for collaborative efforts within government departments as the departments pursue control, supremacy and respect. A tradition of silos has existed psychologically and therefore it has proven difficult to get government agencies at borders and Ports of Entry to work together for a common purpose (Manig, 2017:37).

South Africa's eight commercial Ports of Entry lack proper management, are understaffed, under-facilitated, lack security training facilities and are controlled by government authorities unwilling to choose the right security for the Maritime Ports (Department of Home Affairs, 2015:7). South African ports and borders are faced with the illegal movement of drugs, contraband, vehicles, arms and people. In addition, the unauthorised entry of people and goods at the Maritime Ports of South Africa is caused by corrupt officials willing to admit them in exchange for bribes. The most troublesome areas in the port of Durban are access and egress control due to inadequate control systems for monitoring, securing perimeter fences, scanners and security personnel. The current security measures have proved to be ineffective and unsuccessful in limiting the illegal movement of people and goods and other related crimes in the ports (Moodley, 2014:31).

Other major problems facing South Africa's Maritime Ports are the fact that real estate in the ports is in high demand and that cross border threats have spread throughout the port's geographical area. The Maritime Ports of South Africa need advanced technologies to monitor the movement of people and goods at the entry and exit points of borders and Ports of Entry, as well as to protect the maritime economy from illegal activities (South African Government News Agency, 2014).

Neglecting port security makes Maritime Ports vulnerable to changes in the global economy and trade which can lead to the loss of economic opportunities. The security of the Maritime Ports of South Africa has experienced structural changes with the adoption of various new maritime security and legislative initiatives. Consequently, South Africa has identified marine protection and governance as one of the priorities under Operational Phakisa, the country's ocean economic policy (South African Government News Agency, 2019). A port of entry control centre at the port of Cape

Town was opened by the government to link government stakeholders and role-players, such as immigration, customs, health, agriculture, security and intelligence, to solve problems related to border and Maritime Port security (South African Government News Agency, 2014).

Transnet National Ports Authority (TNPA), with the assistance of other players such as the South African Revenue Services (SARS), customs, South African Police Services (SAPS), provide security at the Maritime Ports of Entry (Moodley, 2014:31). The TNPA is committed to enhancing global port security and supply chain standards through the IMO and the ratifying of the ISPS Code. The Code, which became compliant with the South African TNPA through the Merchant Shipping (Maritime Security) Regulation in June 2004, includes steps to prepare ports and ships for the risk of crime and terrorist attacks, such as retraining security staff and re-enforcing port borders. The National Department of Transport is the custodian for the implementation of the ISPS Code as per the National Ports Act 12 of 2005 (Ramsaroop, 2016:6).

Strict access control measures have been enforced within designated port limits to rectify insufficient protection measures and to deal with non-compliance at South African Maritime Ports of Entry. All port users are inspected at the port of entry. Daily port visitors are provided with visitor's identification card (Ramsaroop, 2016:40). Furthermore, at the port of Cape Town, 72 hours advanced notice is provided to the port, indicating arrival time, final port of call and ship security level (Panargo Shipping, 2011:4).

South Africa has also pursued many projects with foreign maritime allies to overcome transnational problems faced by Maritime Ports. South Africa, Mozambique, and Tanzania have entered into a trilateral agreement to tackle drug trafficking on maritime routes in the Indian Ocean. This is in collaboration with the United Nations Office on Drugs and Crime. This agreement aims to increase the capacity of maritime surveillance, the identification of drugs trafficking and the enhancement of security at Ports of Entry (South African Government News Agency, 2019). South Africa maritime foreign policy is influenced by partnering with international members and organisations from various countries such as India Ocean Rim Association (IORA), Brazil, Russia,

India and South Africa (BRICS), and Joint-India-Brazil-South Africa (IBSA). The IBSA has been maintaining diplomatic partnerships and co-operation within the states that is also a priority of South Africa (Walker, 2020:14).

Security of Maritime Ports of the world are increasingly under threat because of cargo theft, drug smugglers, stowaways, terrorists acts and piracy, weapons and people trafficking (Carpenter, 2013:2) that result in the costs of damages, loss of incomes and disruption of product flows. The negative results affect both partners in transport or supply chains (Young et al, 2018:30). In South Africa, inadequate security has led to the country's ports failing to provide security measures to prevent the smuggling of goods, weapons, people and drugs (Moodley, 2014:42).

The following types of threats are recognised:

Cargo theft

Cargo theft is a security problem that affects all forms of transportation. Syndicates are actively involved in cross-border crimes, chains, and sourcing goods and materials for resale (Institute for Security Studies, 2018:19). Cargo thefts are a burden on the economy as the cost of stolen goods disrupts the credibility of business process in the price of the commodity delivered daily (Van Marle, 2019). Cargo theft presents threats to supply chain of cargo that could adversely affect port operations, such as loss of customer's satisfaction, trustworthiness of port facilities and loss of financial value (Elago, 2019:86).

As of 2015, South Africa's average cargo theft loss was approximately 201,423 Euros derived from the 34,5 percent of recorded cargo theft by the Transported Asset Protection Association (TAPA) and Incident Information Services (IIS) (Elago, 2019:17). The 2019 cargo theft figures from South Africa are the highest number reported in TAPA's 23 years' history (Neumann, 2020). The amount of global cargo theft is estimated to be $50 billion or more per year (Elago, 2019:17). Cargo theft usually takes place through the coastal cargo movement. Unreported incidents of cargo theft are estimated to cost $100 billion a year. Another part of the cargo theft technique is cargo robbery and hijacking (Bernard, 2015:21).

Goods are usually stolen from the warehouse during the loading and transiting process (Young et al, 2018:32). Protecting and preventing shipments from pilferage and theft during transit through Maritime Ports is a major security issue. Access control measures, such as locks, identification cards and container seals, can prevent threats to goods being shipped and stored (Christopher, 2009:58).

Illegal or undocumented immigrants

According to Busiega (2016:66), illegal immigration is a problem that threatens regional stability and affects Maritime Ports of Entry. Rosenblum and Hipsman (2016:7) note that since Congress first tried to counter widespread illegal immigration by passing the Immigration Reform and Control Act (IRCA) of 1986, the USA has spent more than $250 billion on border security and immigration enforcement. The lack of tools for measuring immigration is the biggest challenge for the USA (Rosenblum and Hipsman, 2016:7).

South Africa has wide borders, giving rise to difficulties with cross-border regulations. The rise in the number of refugees and asylum seekers provides terrorist groups with a suitable opportunity to hide and plant combatants. An estimated five million undocumented immigrants live in South Africa, plus approximately three million Zimbabweans (The Law of Library Congress, 2013:119; Mollema, 2018:25).

Seda (2015:55) defines illegal immigrants in South Africa as those who use illegal means to get into South Africa. The complexities of migration to South Africa are due to the fragmented nature of the state's borders, seas and the presence of unregulated modes of transport by land, rail and sea (Mollema, 2018:25).

In an effort to resolve the multi-dimensional warfare against illegal trafficking of people, South Africa signed the Trafficking Protocol in 2000 which was ratified in 2004. As a result, the nation has been subjected to international obligations under which the government is granted exclusive responsibility to detect and prosecute crime efficiently to protect the victims' rights and the interests of the country. Anti-trafficking legislation, the Prevention and Combating of Trafficking in person Act 7 of 2013 (Trafficking Act), was passed into law on 9 August 2015 (Mollema, 2018:25).

Stowaways

According to Bernard (2015:23), a stowaway is someone who hides on a ship or cargo or in a container until the ship leaves the port without the ship-owner's permission. Stowaways pose a threat to global shipping, disrupt freight schedules and delay shipments. They put cargo at risk and jeopardise the operational safety of ships, put their lives at risk and threaten maritime security. Apart from disturbing the vessel's patterns of trade, stowaways breach the global provisions of the ISPS Code intended to minimise unauthorised entry to ships, port facilities and the port's high-risk areas (Aguocha, 2018:1).

Stowaways are threats for shipping companies especially those visiting the commercial ports of South Africa. P and I Associates (Pty) Ltd reported overwhelming numbers of incidents of stowaways in the port of Durban in 2016 (Heads, 2016:1). Meanwhile, the Durban media have reported incidents involving people entering ships illegally. Most of these stowaways are illegal immigrants working as informal workers in South Africa (Gard Alert, 2016).

According to Aguocha (2018:17), most stowaway incidents are carried out by organised human smuggling operations from local and transnational human, and drug trafficking networks. In this criminal operation, port security officers may be receiving bribes from the stowaways or the criminal organisations (Aguocha, 2018:17). Blaine and Nel (2020:112) believe that the harbour, containers and the geographical dispersion that leads to a lack of resources exacerbate various types of illegal activities at the borders and Ports of Entry.

In South Africa, any person illegally boarding the ship is automatically considered a stowaway and the ship-owners are responsible for repatriation costs unless they can provide evidence (such as photos, videos) confirming that the stowaway got into the ship in South Africa (Gard Alert, 2016). The stowaway repatriation costs levied by custom authorities on ship owners also put the life of the stowaways at risk of being killed on board by shipmasters to prevent fines (Aguocha, 2018:21).

Drug trafficking

Drug trafficking is the second-most lucrative criminal market, accounting for over a third of the general income of transnational crime. The global drug trafficking industry had a volume of US$426 billion in 2014 (May, 2017:3).

Container shipments are used to transport cocaine. Container ships have been exploited by drug trafficking groups because it is a cost-effective and easy route for transportation of drugs. South America, Europe and Western Africa are affected by the illegal trafficking of drugs arriving by ships (Carpenter, 2013:4). Nearly two percent of containers are inspected globally; making it easy for drug smugglers to use containers that import cargo to African or European countries for illegal drugs (Akar, 2019:16).

Trends in South Africa show that drug related crime is on the rise, putting pressure on law enforcement to detect and combat these crimes. The large number of containers that move every day through the port of Durban and the ineffectiveness of Port of Entry security inspections increase the number of smuggled goods and contraband into the country (Moodley, 2014:44). Haysom, Gastrow, and Shaw (2018:13) point out that law enforcement in the port of Durban does not search in-transit cargo upon arrival and departure. The proximity of the port of Durban to a network of trains and truck terminals makes it attractive to smugglers. Furthermore, the lack of Port of Entry control measures, corruption and poor management have allowed a wide number of criminal networks to be active in the port of Durban (Haysom et al, 2018:32).

Illegal drug trafficking, drug addiction and gangsterism continue to affect the physical, emotional and mental health of Cape flats residents in the Western Cape Province (Ramson and Chetty, 2016:67). The port of Cape Town is used as the main route for importing illegal drugs. In June 2017, law enforcement authorities discovered 963 kg of heroin, in the farming town of Villiersdorp, one of the largest seizures in the country and the first heroin seizure made in five years. The heroin was divided into 253 packets hidden within wine cases intended for sale. The investigators traced the origin of the drugs to the port of Cape Town (Haysom et al, 2018:15).

The port of Cape Town is not commonly known for corruption, giving smugglers an

advantage of using the port to transport illegal supplies into and out of the country. Traffickers use commercial containers carrying export goods that are not carefully inspected, such as wine and fruit, because containers transporting these items are considered low risk in the country of destination, rendering them less likely to be searched (Haysom et al, 2018:15).

Trade fraud (such as under-valuations and sale of counterfeit goods)

Trade fraud is becoming a more complex and diversified through the use of the latest technologies. The illicit trade of goods is the most profitable illegal trade and is worth between US$923 billion and $1.13 trillion per annum (May, 2017:xii). Counterfeit goods are expected to cost the USA economy $600 billion a year (Schlesinger and Day, 2019).

China struggles with negative image as one of the world's most dangerous countries for crimes involving counterfeited goods (Reniers, Rhoades, Szyliowicz and Zamparini, 2016:294). According to Osimen, Anegbode, Akande and Oyewole 2017:24), smuggling of contraband goods usually takes place in Maritime Ports with the help of maritime port officials to escape customs and exercise duties. This is supported by Moodley (2014:8) who claims that the port of Durban is South Africa's largest port with corrupt customs and police officers. These officers are alleged to allow smuggled goods to pass through the port un-scanned in exchange for money (Moodley, 2014:8).

Regardless of various programmes initiated by IMO and government agencies to achieve maritime security by identifying threats and initiating maritime programmes, Ports of Entry challenges and realities continue to escalate. Ports of Entry are targeted by criminal groups because of their vulnerability (Bernard, 2015:30). The Ports of Entry act as a bridge between land and maritime roads for commercial purposes and have become an important route for illegal trade and criminal groups. The features, its geographical positions, and the nature of cargo make ports vulnerable to all forms of crime for financial gain (Bernard, 2015:30). On a global scale, the channels for non-compliance and customs fraud point to the falsification of goods, misappropriation of the country of origin, round tripping and counterfeit goods (United Nations Office on Drugs and Crime, 2013:46). Customs evasion provides organised criminals with an

opportunity to fund other crimes by under-declaring imported goods passing through the ports or harbours (May, 2017:xii).

Globalisation has intensified the insecurity of state sovereignty and of border security. The growth of freedom of cross-border movements in people, goods and money (presented as a means of obtaining political, economic and social freedom) greatly led to the transportation of dangerous weapons, drugs and people at land border or maritime ports. Trends in international migration from 2000 to 2013 show that the vulnerabilities of Ports of Entry, such as physical structures, personnel protection systems, and processes, connect to other modes of transportation and other commercial and governmental facilities whose security is co-dependent with that of maritime industry (Young et al, 2018:8; Department of Home Affairs, 2016a:21).

Every year, over 400 million people cross the borders of the United States through Ports of Entry, with hundreds of thousands of them doing so illegally (Moodley, 2014:39). South Africa has a vast coastal and marine environment that has significant economic value, covering over 4 340 000 square kilometres (km), of which 474 000 square km are situated 1 920km southeast of the South African coastline It is difficult to maintain a clear and effective police presence and authority over such a huge and isolated territory but a disorganised state capacity and limited maritime resources to screen goods and people to ensure secure operations have border and ports control implications (Manig, 2017:17).

In South Africa, the number of uncoordinated multi-departmental stakeholders at the Ports of Entry is considered to be the most fundamental of all threats. A lack of collective approach or a clear direction is caused by maladministration and poor service delivery as prescribed by the Constitution (Van Nieuwkerk and Manganyi, 2019:10).

A high rate of untrained and unmotivated border police officials to identify and prevent cross-border crimes is a challenge. Maritime Ports run the risk of increased criminal activity and internal intrusion if the personnel in charge have no knowledge of detecting and preventing illegal activities (Department of Transport, 2017:15). To date, the training of Maritime Port stakeholders is minimal or conducted disjointedly with different Maritime Ports' stakeholders (Manig, 2017:4).

South Africa lacks a national maritime security strategy for evaluating security control equipment to protect the Ports of Entry (Van Nieuwkerk and Manganyi, 2019:10). A maritime strategy is the overall direction of domestic power relevant to the interest of a nation at sea. It contains the role of state powers, such as diplomacy, the safety and security of oceanic maritime trade, the control and defence of the maritime exclusive economic zone, the security of national borders and the Maritime Ports, and the collaboration and co-operation with regional and foreign allies on matters related to the exploitation of the oceans (Manig, 2017:20).

The lack of a national strategy in South Africa makes it difficult for maritime security officials to organise maritime interests (Manig, 2017:21). There is very little coordination and operational procedures between agencies that defines how to use the equipment available and this often contradicts the roles and responsibilities of the various departments within the maritime domain (Van Nieuwkerk and Manganyi, 2019:10). Moreover, the lack of strategic direction from decision-making authorities hinders the ability of maritime security officials to rapidly and effectively respond to threats, vulnerabilities and maritime security risks (Moodley, 2014:43).

According to Manig (2017:11), the South African Maritime Ports lack monitoring equipment such as vehicle patrols, land-based sensors, access control systems, maritime intelligence networks, surveillance technology and Automated Identification Systems (AIS). The absence of these systems leaves maritime operations with an insufficient information base for controlling illegal movements of goods, people and weapons (Moodley, 2014:43). As a result, the port security is unable to combat unauthorised access (Chetty, 2018:55).

Haysom et al (2018:34) indicate that criminal group networks operating in South African Ports of Entry often rely on corrupt officials and maladministration to prevent international crimes and transitional criminal activity (including both South African and international foreign-run groups) (Democratic Alliance, 2019:72). The most common way to remove goods from the port of Durban is through the use of fraudulent documents. Corruption of maritime security officials is a well-known method for unlawfully transporting cargo from South African ports (Moodley, 2014:50; Reniers et al, 2016:294). The Danish Institute for International Studies Policy Briefing of 2016

points out that regular traders, trans-shipments and passengers pay bribes to law enforcement agencies to avoid paying goods tax or administrative measures imposed by state agents (Hahonou, 2016:3).

The Department of Home Affairs, immigration and customs officers within the maritime port environment execute their duties without proper technical tools (Parliamentary Monitoring Group, 2013). Some border posts lack the necessary equipment, such as storage spaces, appropriate search locations, vehicles and facsimile machines, to carry out adequate port security (Moodley, 2014:50). The ratio of available sea resources against the size of the maritime domain areas is unbalanced and distorted (Department of Home Affairs, 2016a:10). The practice of inspecting containers at random is responsible for high volumes of contraband passing through South African Maritime Ports without being detected (Moodley, 2014:50). The current biometrics systems launched by the Department of Home Affairs at the Ports of Entry is fully functioning at only ten out of 71 Ports of Entry and certain counters at the port of Cape Town (Department of Home Affairs, 2020:19).

South Africa has no dedicated and singular maritime border post that is fully functioning and in operation for 24 hours with a manned control centre (Manig, 2017:42). According to Khumalo (2015:844), customs agencies' operational hours were between 8h00 and 16h00, affecting traffic flow at the border posts by reducing the hours for freight clearance services. According to the Department of Home Affairs (2016a:21), Maritime Ports of Entry are understaffed and under-facilitated and this affects the efficiency of on-going inspection and screening of container cargo to combat cargo crime and theft at the Ports of Entry.

3.4 The roles and responsibilities of security officials at Maritime Ports of Entry

Maritime security is a responsibility that has no clear definition. It is a legislative obligation, but sovereign decisions of various choices rest with the government authorities that have an impact on maritime collaborations (Feldt, Roell and Thiele, 2013:2). Elements that are within the scope of maritime security include protecting a territory and ensuring political and economic independence on the sea (Feldt et al, 2013:2).

The CBP and Coast Guard are agents in the USA that are responsible for securing the Maritime Ports of the country. The USA Coast Guard is responsible for port security, waterways and USA coastal territories. They prohibit unauthorised migrants from entering the USA illegally or smuggling goods by sea route into the country (The "PEW" Charitable Trusts, 2015:3). They also carry out risk analyses to ascertain the level of risk and training needed to meet the ISPS Code designated measures (Pearl, 2019:26). In addition, the CBP is the police and security department responsible for guarding and upholding regulations at the borders and Ports of Entry (The "PEW" Charitable Trusts, 2015:3). They are also responsible for container security, including screening entrants at the ports for contraband, prohibited items, illegal immigrants, dangerous insects and produce that exceeds tariff restrictions. The CBP also maintains offices worldwide from which it detects, inspects, and loads shipment containers bound for the US. Documentation is pre-screened and the process is in place to speed up the delivery of goods to USA ports (Phelps, 2014:128).

South Africa has a separate body to oversee its land and sea borders. The Border Control Operational Coordinating Committee (BCOCC) system established in 2005 is supported by Justice, Crime Prevention and Security Structures to enhance the South African border environment (Dailey, 2014:102). South African Revenue Services (SARS); the South African Police Service (SAPS); the Department of Home Affairs (DHA); the Department of Transport (DoT); and the Department of Agriculture and Fisheries are the key government institutions in maritime borders and Ports of Entry security of South Africa (Moodley, 2014:40). The roles and responsibilities of these entities are discussed below in terms of their constitutional mandate:

Customs - South African Revenue Services (SARS)

Customs officers are in charge of monitoring the transportation of commodities entering and leaving the Ports of Entry and national borders. Their main objective is to prevent all declared contraband from importation into the country (Department of Home Affairs, 2016b:48).

South African Police Services (SAPS)

Maritime borderline controls are the primary responsibility of the South African

National Defence Force (SANDF), but South African Police Services (SAPS) remain accountable until SANDF is able to perform this role completely on its own (Manig, 2017:39). The objectives of SAPS include preventing and investigating illegal or concealed cross-border movement of persons and goods and implementing the necessary safeguarding measures in accordance with South African law (Moodley, 2014:39). The SAPS functions complement other law enforcement agencies in their efforts to enforce law and control the sea trade route to prevent cross-border crimes such as smuggling, human trafficking and piracy (Manig, 2017:39).

Department of Home Affairs

The DHA is essential for the promotion of legal movement for people entering and leaving the country as well as detecting and monitoring the irregular movement of people while retaining the security of the Ports of Entry (Department of Home Affairs, 2016b:48).

Department of Agriculture, Fisheries and Forestry (DAFF).

The DAFF has been mandated with the responsibility of protecting the environment from pollution and illegal, unreported and unregulated (IUU) fishing. The DAFF also performs routine inspections of containers at sea and maintains ongoing monitoring of maritime policy compliance, both nationally and regionally, by ratifying a Memorandum of Understanding with the appropriate border control agencies (Manig, 2017:38).

Department of Transport (DoT)

Port security's role is retained by the national Department of Transport. The DoT, in partnership with government stakeholders such as South African Maritime Safety Authority (SAMSA), Transnet National Ports Authority (TNPA), Transnet Port Terminal (TPT) and the South African Ports Regulator, promotes the South African government's policy and legislation to promote economic growth within the maritime industry in order to create jobs. The legislative steps to achieve maritime security at Maritime Ports of South Africa include the South African Maritime Security Regulations (ISPS Code) in terms of section 3(1) of the National Ports Act, 2005; the South African Port Legislative Arrangements; and the South African Maritime Security Regulations

(Act No. 12 of 2005) (Ramsaroop, 2016:7).

The South African Maritime Safety Authority (SAMSA) is the nominated authority in South Africa for the overall management of marine safety and security in all eight maritime commercial ports. They are accountable for authorising ship security plans; checking security plan compliance; issuing the International Ship Security Certificate (ISSC); as well as the Continuous Synopsis Record (CSR) (Ramsaroop, 2016:39).

3.5 Security measures to improve security at Maritime Ports of Entry

Pinto (2018:1) shows that transnational threats and vulnerabilities at Ports of Entry pose constant challenges to national and international security. Understanding the fundamental origins of threats and employing the right technologies would strengthen Ports of Entry security and provide law enforcement with the power to control the movement of people and goods across their national borders (Dailey, 2014:269).

Traditional security is a vital element in the disruption of illegal activities from the Ports of Entry into the seaport. The first line of defence for ports includes the implementation of efficient access control to know who is accessing the port and for what reason. This includes drawing up an effective access control strategy and protocols, and increasing the number of access/egress control point tools (Moodley, 2014:59). This includes the close scrutiny of identification credential information and the verification of the intentions of people, ships and goods arriving at the port (Andritsos, 2013:7). Proper inspection of visitors and vehicles arriving at the port of Durban and Cape Town is another way of detecting and preventing terrorist or criminal activities (Moodley, 2014:59).

According to Borchert (2014:24), conducting a security review of proper technological aids can increase security for maritime transport. The following categories can be applied to provide solutions to improve port security globally (Young et al, 2018:52):

Infrastructure protection

Protecting infrastructure deters and prevents terrorist or criminal activities from obtaining entry to a structure or facility and minimises the effectiveness of an attack if access is obtained. This needs a standoff distance, access control and CCTV

surveillance, intrusion detection and lighting as well as human security (Aamilid, 2019:43).

Access management

Access control is significant in the security of Maritime Ports of Entry. Biometric security in a form of identification/access cards is a value-added access control for the security of foreign vessels (Moodley, 2014:59). The iconic access control measure is the Transportation Workers Identification Credential (TWIC) programme that facilitates economic productivity, mobile personnel and resilience when port disruption occurs. The TWIC programme mandates that all maritime personnel have a biometric ID card, and pass a security background check. Only personnel who possess the ID card or a temporary ID are permitted to enter security facilities and vessels at the port level (Herout, 2017:47).

Intrusion detection

Intrusion detection is a software technology with video recording that gives security personnel total visibility of the port infrastructure to provide evidence to remediate the threat (Young et al, 2018:52-54). It includes lighting, perimeter, video surveillance, biometrics, ID card, metal detectors and scanners that detect the tampering of containers or devices set by terrorists. These sophisticated systems thus control and deter criminal activities at port facilities, vessels and port assets (Aamilid, 2019:41, 43).

Situational awareness

Situational awareness is being aware of the most vulnerable parts of the maritime port facility and assessing the possibility that the security would be compromised. Maritime Ports have vast areas to monitor; some are bordered by water and other by natural barriers. By understanding the threats and vulnerabilities, maritime security officials have the ability to establish risk reduction strategies (Young et al, 2018:55).

Various forms of technology have an impact on transportation security. Basic technologies to protect infrastructure include the surveillance and restriction of entry (Dailey, 2014:268). The CCTV systems and intrusion sensors provide port facilities

with advanced surveillance capabilities to track movement, observe the actions of employees and visitors, inspect cargo transfer processes and rapidly identify security breaches and take action. High-tech is one of the most advanced electronic fence technologies that protect the boundary by limiting access. It secures the Ports of Entry against unnoticed escapes, infiltration and smuggling (Busiega, 2016:77).

Alarm systems and electric key cards provide human patrol ability. Aircraft are also helpful for surveying wide expanses of remote areas. The United States uses drones to patrol wide expanses of open space along their right of way (Young et al, 2018:178). These systems provide a strong method of detection and prevention and are a proactive method to identify and respond to potential threats even though it is not possible to eliminate vulnerabilities completely (Segovia, Cavalli, Curppens and Garcia-Alfaro, 2019:258).

The port of Durban consists of an intelligent command and control system which transforms a CCTV camera network into an intelligent sensor for detection, tracking and recording. There are over 120 cameras in operation around the Durban harbour perimeter. Any security breach or suspicious behaviour observed by cameras through the command centre programme activates an alarm in the control room, allowing security personnel to respond appropriately (Moodley, 2014:111). Protecting the Cape Town maritime port includes 24-hour operational security which includes access control, CCTV and intruder detection systems (TheSAMag, 2018).

Non-intrusive imaging technologies, such x-ray and gamma-ray security scanners, are recommended scanning systems capable of scanning containers and other cargo for illegal narcotics, radioactive materials and terrorist weapons (Morris, George, Haseley, Parker and Sherman, 2020:12).

The International Ships and Ports Facilities Security Code (ISPS)

The United Nations International Maritime Organization (IMO) adopted the ISPS Code for the protection of Life at Sea (SOLAS) Convention of 2002 to strengthen regional and international ships and ports facilities (Feldt et al, 2013:9). The goal of the ISPS Code is to outline minimum security criteria for ships and ports (Haelterman, 2013:45). It covers port facilities and vessels of countries that are signatories to the IMO

(Carpenter, 2013:9). The Code offers structured risk assessment systems that allow governments to set adequate security levels and measures to account for changes in the threats and vulnerabilities of ships and port infrastructure (Haelterman, 2013:45). It serves as an international mechanism for collaboration between countries, government agencies and the shipping companies (Monacelli, 2018:5).

Security and Accountability for Every (SAFE) Port Act

The Security and Accountability for Every (SAFE) Port Act is another initiative initiated by the USA in 2006. The act is used to ensure that member states are committed to improving their port security to detect and deter criminal attacks on cargo (Leonard et al, 2015:44).

Customs-Trade Partnership against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) is an additional USA initiative that is an independent government-business programme to develop relationships of cooperation that improve security of international supply chains and USA ports (Haelterman, 2013:46). The C-TPAT programme guarantees that high security measures are maintained by these role players and that these measures and security procedures are shared across the supply chains (Herout, 2017:48).

Maritime Transportation Security Act (MTSA)

The Maritime Transportation Security Act (MTSA) was passed by the USA security services in 2002. The MTSA addresses the problem of port and waterway security in terms of mitigating maritime trade threats through the evaluation of all maritime vulnerabilities, the preparation of effective and cooperative security plans and the production of transport security response plans. The programme mandates that all passengers and their belongings be checked by passenger vessel operators using x-ray machines and metal detectors (Herout, 2017:49).

Container Security Initiative (CSI)

The Container Security Initiative (CSI) is a successful multinational initiative that has improved the security of the ports (McClain, Thomas, McAleenan, Sadler and Kamoie, 2014:6). The CSI aims to identify high-risk containers carrying weapons of mass destruction or hazardous nuclear substances that terrorists could use (Feldt et al,

2013:8). The programme allows the USA Coast Guard and CBP to use intelligence and automated information systems to classify and inspect all containers posing possible terrorist dangers to foreign ports. They also use evidence to recognise tampered cargo before it arrives at USA ports (Carpenter, 2013:12).

The CSI operations are a critical layer of security for world trade that is potentially threatened by terrorism and piracy, especially in Asia and Europe (Feldt et al, 2013:8). A joint anti-piracy mission to reinforce the EU Maritime Ports and to provide accurate information was signed in April 2004 between the USA and the EU customs (Carpenter, 2013:12).

Physical search

According to Morris et al (2020:12), a physical search is another method for screening and inspecting containerised cargo. It addresses concerns about a container initially checked by other means of inspection systems that cannot be addressed through technology and radiation sensors, especially when these methods raise suspicions. The container then needs to be unpacked and searched physically again (Morris et al, 2020:12).

Co-operation and communication

Collaboration between the government and the private sector raises awareness and information sharing on maritime security. Energy, insurance, and commercial shipping companies are the main actors in the private sector (Manig, 2017:33). Effective communication is crucial since crimes, particularly those considered cybercrimes or those that involve terrorism, must be fought by maritime security officials in more than one nation (Phelps, 2014:238).

Strong public-private partnerships are also critical to boost trade and travel flows across borders and Ports of Entry. This includes closed cooperation between nations using a number of forums, committees and organisations (Young et al, 2018:44). The advice of the IMO is that cooperation be formed by countries with shared maritime interests to enhance their joint targeting efforts (Asiamah, 2018:36).

Technology has enabled the USA to broaden cooperation beyond their facilities and

to be involved in areas of concern far from their soil (Herout, 2017:55). The protection of USA ports depends on the knowledge of the contents of each freight container before it enters their Maritime Ports from abroad (Givens et al, 2018:2). The USA also collaborates closely with its foreign counterparts, law enforcement, and counterterrorism to track the location and security of transit containers (McClain et al, 2014:14). Moreover, the USA provides maritime financial assistance to developing countries to improve maritime prosperity (Herout, 2017:55).

According to Duarte (2019:189), the International Coordination Centre (ICO) for maritime security cooperation in the Gulf of Guinea, based in Cameroon, is the best model for cooperation between Brazil, the United States and the European Union to help Western African countries cope with piracy and transnational challenges. These collaborations avoid the duplication of efforts and increase prospects in other marine locations (Feldt et al, 2013:13).

Australia has expanded its risk-based border control systems to strengthen cooperation with international allies to jointly tackle smuggling, illegal migration and transnational crime. Additionally, Australia participates in international maritime conferences, exercises, events for capacity building and forums for information exchange (The Law Library of Congress, 2013:24).

India has already taken steps towards interagency coordination to protect itself against potential risks in the Indian Ocean. India has embedded agents with foreign law enforcement partners in Sri Lanka, the Maldives, the Seychelles, Mauritius, Madagascar, Myanmar and Vietnam at strategic levels to improve Indian maritime diplomacy's capacity (Van Nieuwkerk and Manganyi, 2016:5).

The African Union (AU) has established the AIM (African Integrated Maritime) Strategy for 2050. The AIM collaboration is a joint maritime strategy focusing on African maritime states to share information on maritime security risks and mitigating measures. Other initiatives have been undertaken by the IMO to coordinate a comprehensive maritime security strategy to strengthen the efforts of Western and Central African countries to tackle maritime piracy and organised crime by cargo carriers (Asiamah, 2018:3). In particular, the IMO and AU have signed the African Union Agenda 2063 transportation cooperation programme (International Maritime

Organisations, 2015:2).

A memorandum of understanding on cooperation in Maritime Security between South Africa, Mozambique and Tanzania was signed in 2012 to improve control over trafficking and illegal fishing. It has created joint activities such as exchanging information, surveillance, joint military exercises, patrolling, arrest, search and seizure (Blaine and Nel, 2020:115).

Information sharing

For security purposes, the sharing of information is necessary for the Maritime Ports of Entry. Maritime security officials want to be informed as early as possible of the contents of the intermodal loading units. Furthermore, shippers who own the goods are kept updated about the position of the goods (Nieuwenhuis, 2016:33). The high incidences of maritime related threats indicate the need for comprehensive vessel movement databases and cargo information. The aim of the database expansion is to cover all potential threats relating to the marine sphere and to provide measures to safeguard naval forces against such threats. Increasing information exchange allows intelligence services to use comprehensive databases to search for maritime domain threats and develop advanced reactive measures based on the findings of such databases (Herout, 2017:56). The opening of a Port of Entry control centre at the Port of Cape Town brings together government departments and state agencies to share maritime threat trends and to prepare preventive measures on the control of the Maritime Ports (South African Government News Agency, 2014).

Enforcement of law on criminal activities

Cyber, trans-border and transnational criminal activities have increased since 11 September 2001. This has caused law enforcement and government agencies to change their perspectives and work together with their allies to counter traditional and cybercrimes that threaten the safety and security of maritime navigation (Phelps, 2014:237). The United Nations Convention Against Transnational Organized Crime and the Council of Europe's Convention on Cybercrime are legal frameworks that provide accountability for prohibited conduct regardless of where it happens (Phelps, 2014:239). The Suppression of Unlawful Actions (SUA) Convention against the safety

of maritime navigation is a cooperative agreement explicitly dealing with certain types of criminal activities concerning ships and navigation. On request, it grants another state the right to extradition or prosecution of suspects apprehended by the states that have ratified it. Furthermore, the SUA Convention of 2005 criminalises the shipment of terrorists, drugs and weapons. It also facilitates cooperation between states and offers a comprehensive framework for the transportation of high-risk cargo (United Nations Office on Drugs and Crime, 2017:4).

3.6 Conclusion

The Maritime Ports of Entry have always been perceived as an outsider in which permanent human presence and demarcation of boundaries seemed impossible**.** It appears that handling the complexities of maritime security is a major responsibility affecting international, local and private sectors.

There are two facets of maritime security risks. The first element is the framework of vulnerability, which represents the probability of carrying out illegal actions successfully. The second aspect is the effects of a legal act that has been successfully carried out. These effects are related to two measurable magnitudes, the amount of potential damage and the economic impact of these incidents.

The role of Maritime Ports of Entry is to promote lawful trade and travel while, at the same time, identifying and preventing entry to those individuals and goods that pose a risk of violating the security of the Ports of Entry.

Maritime security threats have been effectively addressed by initiating various measures such as technology, collaboration and information sharing within the contracting states. The security of the Maritime Ports of Entry can be enhanced through the application of various authorities' initiatives and expertise gained in the maritime area.

CHAPTER 4: ANALYSIS AND INTERPRETATION OF DATA

4.1 Introduction

This study was aimed at assessing security measures at Maritime Ports of Entry in Durban and Cape Town, South Africa. Data collection was focused on the following objectives:

- To identify threats, vulnerabilities and security risks confronting Maritime Ports of Entry in Durban and Cape Town, South Africa;
- To establish the roles and responsibilities of maritime security officials in ensuring security at Maritime Ports of Entry in Durban and Cape Town, South Africa; and
- To identify security measures to improve security at the Maritime Ports of Entry in Durban and Cape Town, South Africa.

Data were obtained from ten online telephonic and email interviews and from observations conducted at the two different Ports of Entry. Secondary data were also collected from similar studies in accordance with the documentary study checklist. The data were transcribed, processed, and analysed using thematic analysis and an Excel spreadsheet to show that it had been thoroughly examined. To collect data, the researcher employed an interview schedule, an observation checklist, and a documentary study checklist (secondary data).

This chapter discusses the data management process, the analysis and interpretation of the data.

4.2 Data management

As a result of the Covid-19 pandemic, no face-to-face interviews were permitted by the Research Ethics Committee (See Ethical clearance attached as Annexure A). The research design had to be changed to accommodate the prevailing situation. Instead of face-to-face interviews, interviews with all the sampled participants were conducted by telephone and email. The data for on-site observations were also changed and replaced with purposive interviews with two experts from the Security and Compliance

divisions at Durban and Cape Town Maritime Ports of Entry. The data for documentary study were collected using secondary data of previous articles and dissertation with related information on Maritime Ports of Entry. The data were transcribed, analysed, and interpreted in the manner described below:

4.3 Analysis and interpretation of the data

4.3.1 Interview data analysis

The researcher collected the study data using one-on-one telephonic and email interviews with maritime security officials at Durban and Cape Town Maritime Ports of Entry. All interviews were recorded in writing guided by the interview schedule. The analysis below describes the interview data of all ten participants who were interviewed for this study.

SECTION A: BIOGRAPHIC DATA

4.3.1.1 Gender (see Annexure I question 1)

The table and chart below reflect several respondents who participated in the study as grouped per gender.

Table 4.1: Participants' gender

Gender	Number of participants
Male	8
Female	2
Total	**10**

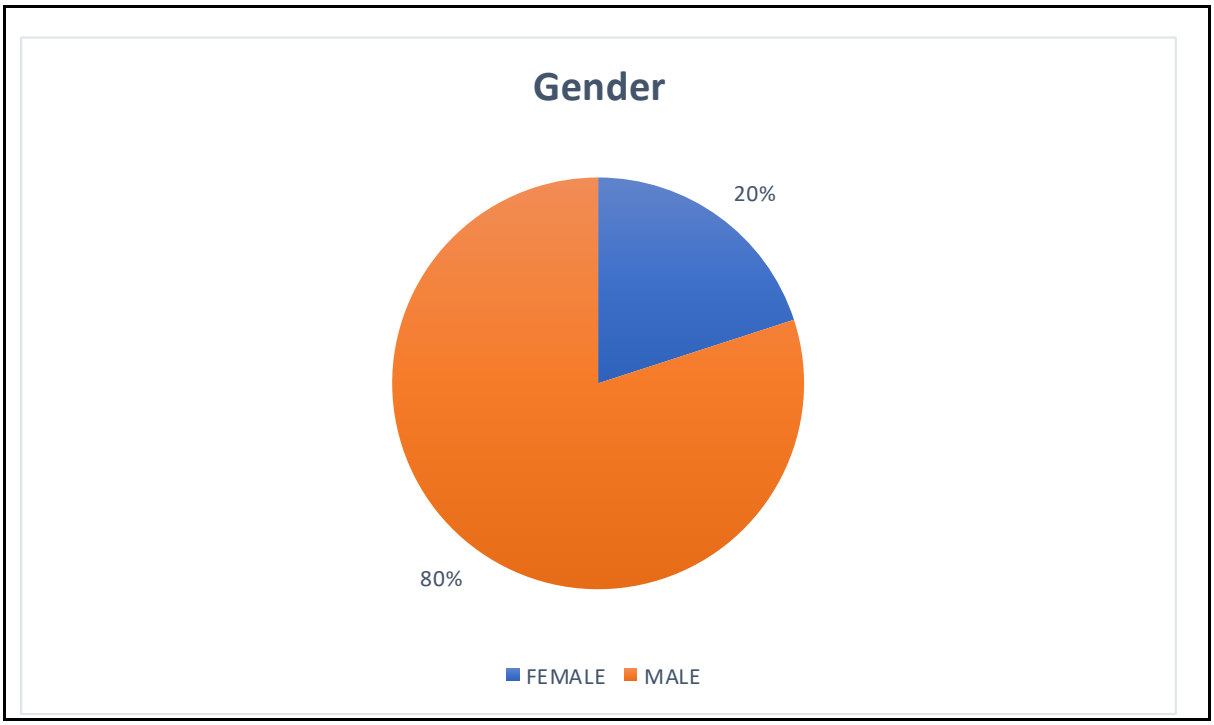


Figure 4.1: Participants' gender

The data analysis revealed that the eight participants who took part in the study are males and two participants are females.

4.3.1.2 Age (see Annexure I question 2)

These are the participants' age range categorised in age brackets.

Table 4.2: Participants' Age

Age Range	Number of participants
36 to 45	2
46- and above	8
Total	**10**

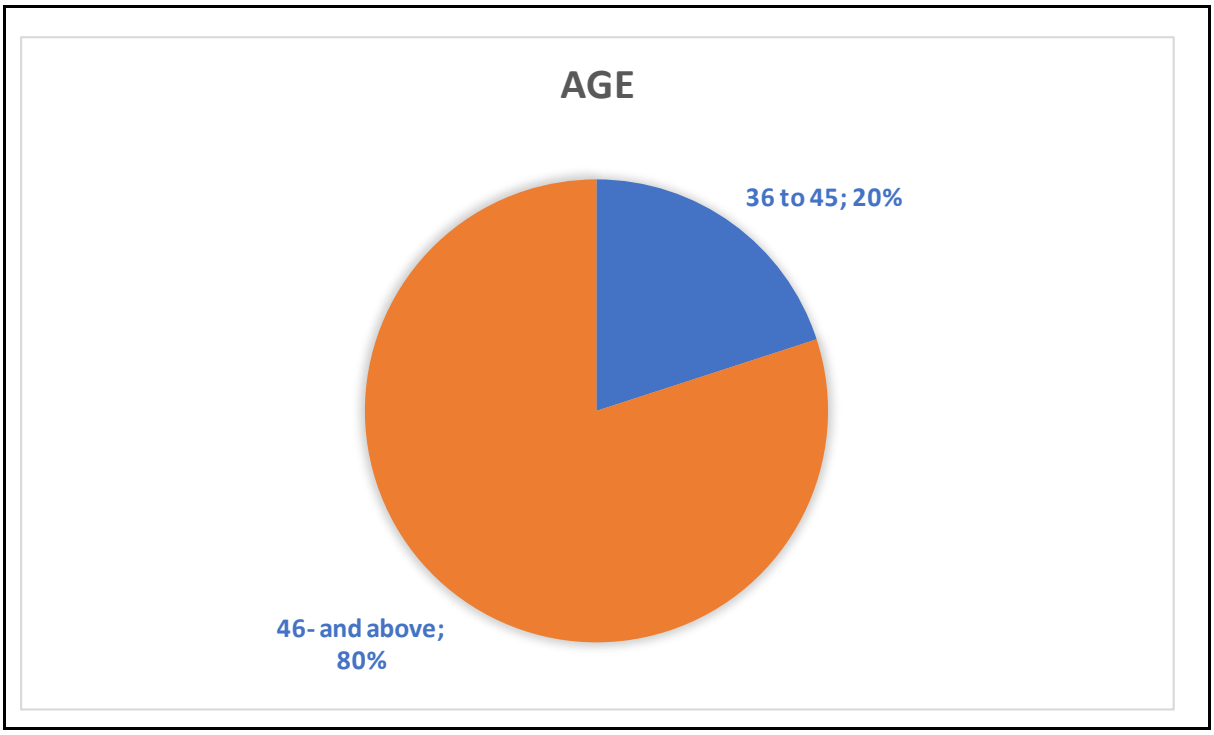


Figure 4.2: Participants' Age

The data analysis revealed that eight of the participants were over the age of 46 and the other two were between the ages of 36 and 45.

4.3.1.3 Educational levels (see Annexure I question 3)

These are the participants' educational levels categorised in level brackets.

Table 4.3 Participants educational level

Educational level	Number of participants
Undergraduate	6
Grade 12	2
Non-responded	2
Total	**10**

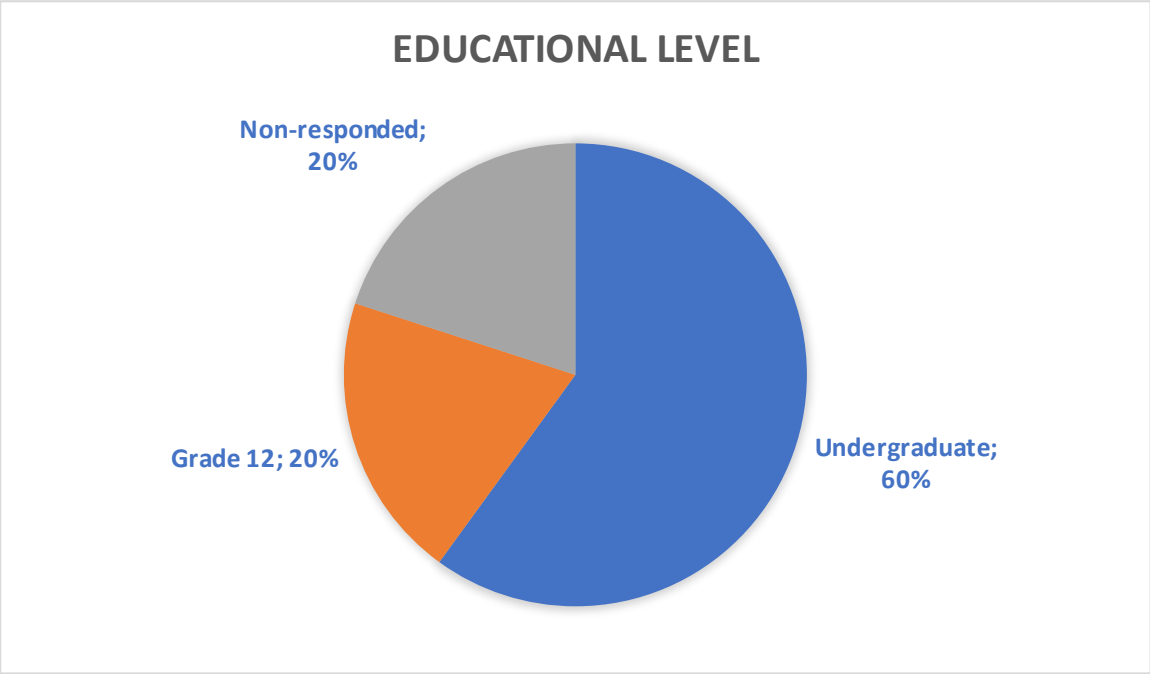


Figure 4.3: Participants' Educational Level

The data analysis revealed that the majority of participants held undergraduate qualifications. Two participants had grade 12 and the remaining two participants did not answer the question about qualification.

4.3.1.4 Port of Entry (see Annexure I question 4)

These are the Ports of Entry where participants originated.

Table 4.4: Participants' Ports of Entry

Port of Entry	Number of participants
Durban	9
Cape Town	1
Total	**10**

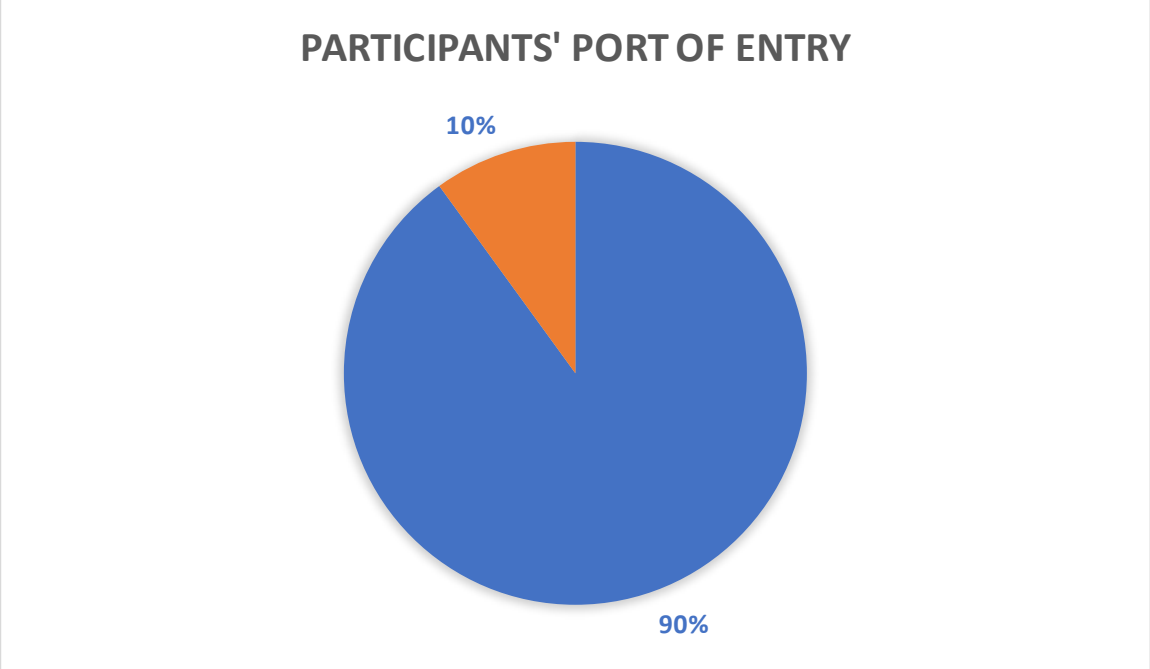


Figure 4.4: Participants' Ports of Entry

The data analysis revealed that the majority of participants came from the Port of Durban, as opposed to the minority who were from the Port of Cape Town.

Interpretation

The fact that more men responded to this study than women may be due to the fact that men are less fearful. Studies show that people over the age of 46 are more

resilient in their lives and more concerned about protecting their communities. According to the educational level of participants, the majority had undergraduate degrees. This may be the result of mature people realising that they need more than a matric qualification to succeed. It should be noted that participants from Durban were more interested in the study than the participants from Cape Town. This indicates that the majority of the analysis of data was from the participants from the Durban Maritime Ports of Entry.

4.3.1.5 Employer (see Annexure I question 5)

Table 4.5: Sector of employment

Sector of employment	Number of participants
SAPS	10
Total	**10**

The data analysis reveals that this study's participants came from the South African Police Service.

Interpretation

The fact that all of the participants were SAPS officers suggests that they were interested in the study. Because of their enthusiasm, the responses they offered were precise and dependable, resulting in strong recommendations. It may also suggest that their superiors gave them permission to participate.

4.3.1.6 How long have you been working for your current company/employer? (see Annexure I question 6)

Table 4.6: Number of years with current employer

Number of years	Number of participants
More than five years	10
Total	**10**

All participants for this study had more than five years working at Maritime Ports of Entry.

Interpretation

All participants in this study had been at Maritime Ports of Entry for more than five years. This may indicate that the maritime security officials are older and have relevant marine experience, which does not have to be limited to those of a certain age. It is once again assumed that the responses of maritime security officials are accurate and reliable, considering the fact that they all have more than five years of experience.

4.3.1.7 Have you undergone security-related training on Maritime Ports of Entry? (see Annexure I question 7)

The table and the graph reflect the security-related training that participants have undergone on Maritime Ports of Entry.

Table 4.7 Security-related training

Security-related training	Number of participants
Trained	9
Not trained	1
Total	**10**

Figure 4.5 Security-related training

This question was posed to see whether participants had received any training in security in relation to security risks at Maritime Ports of Entry. A majority of participants stated that they had undergone some type of security training, only one person did not receive security-related training on Maritime Ports of Entry.

Interpretation

This demonstrates that the majority of participants in this study are competent to perform security related duties at Maritime Ports of Entry.

SECTION B: STAKEHOLDER PERCEPTIONS ON THREATS, VULNERABILITIES AND SECURITY RISKS CONFRONTING MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

4.3.1.8 The Participants' understanding of threats, vulnerabilities and security risks (see Annexure I question 8)

4.3.1.8.1 Threats

Threats (Question 8.1)

Conceptual analysis of threats:

Participant 1: Occurrences that can take place in the maritime environment/ports which can result in harming a country, its economy or citizens/environment, e.g., terrorism, piracy, trafficking, narcotics people/ firearms, and illegal fishing.

Participant 2: Attack of the port that will impact negatively on the functioning of the port.

Participant 3: A statement of intention to illicit pain, injury, damage or other hostile action on someone in retribution for something done or not done.

Participant 4: Hostile action with the intent to damage, inflict pain or injury or something that can cause danger to a person or a particular environment.

Participant 5: Where crime threat analysis and crime pattern analysis is indicative, the port is faced with crime threats and the SAPS has to be proactive in conducting operations jointly with the various role players in order to eliminate the threats.

Participant 6: The port of Durban is constantly under threats of daily crimes, counterfeits, transportation and stowaways and trespasses in facility.

Participant 7: Terrorism/piracy. Smuggling. Statement of intention to inflict pain/injury damages on other, hostile action.

Participant 8: private security colluding with criminals. Legislation/boundaries. Corruption collusion and insider threats. Service tunnels leading to the port.

Participant 9: Bomb threats. Sabotage of the port of entry. Viruses.

Participant 10: It is all about harm or damage in the port or country. The security threats that I have identified at Durban Port of Entry are: cargo theft, stowaways, and counterfeit goods. Trade fraud and organised crime syndicates, drug smuggling, firearm smuggling, etc.

Interpretation

According to a majority of the participants, a threat is a harm or damage caused in the port by organised crime syndicates. Other participants related threats, corruption, stowaways, trafficking, cargo theft, sabotage, terrorists/piracy, smuggling, illegal fishing, criminal activities and hostile actions not on behalf of the port or a country.

Bernard (2015:20) describes maritime security threats as potentially dangerous or harmful activities carried out by terrorists and criminal groups or by port personnel or nations. Aamilid (2019:63) cites cyber-attacks as the most important threat in the modern world. Cyber-attacks can cause serious damage by blocking activity in the whole terminal. Maritime security officials should be educated on the new technology used by criminals to attack the port systems.

4.3.1.8.2 Vulnerabilities

Vulnerabilities (Question 8.2)

Conceptual analysis of vulnerability:

Participant 1: It's the assessment in the maritime port to evaluate where there are vulnerabilities or weak areas open for attack either physically or emotionally.

Participant 2: Poorly secured facilities makes it vulnerable.

Participant 3: It is the quality of being easily hurt or attacked. Some seniors think it's funny to pick on the ninth graders because of their vulnerabilities; it's the state of being open to injury or appearing as if you are.

Participant 4: Quality of being exposed or being attacked or harmed.

Participant 5: Where inadequate security renders the port vulnerable to criminals and criminal activity within the port or outside the port .

Participant 6: The port is vulnerable due to its size and layout and a weakness that has been created or overlooked. The systems that are in place are sometimes too easy to flout e.g. entry in to certain terminal/business units.

Participant 7: Possibility of being attacked or harmed. Easy access into port.

Participant 8: Infrastructure challenges at perimeter point/perimeter fencing. Lack of intelligence. Bad lighting in Durban Harbour on ports. Lack of training in ISPS Code with Government officials.

Participant 9: Access control points. Surveillance methods and lack of private security.

Participant 10: Port of entry is a receiving and distribution of goods; these services create vulnerabilities to organised criminal groups. Taxes need to be collected by Customs; this creates vulnerabilities to corruptions as traders need to save time and money.

Interpretation

In terms of vulnerabilities, a majority of participants indicated that vulnerability constitutes weakness within the port of entry, while others cited problems at perimeter fencing and access control areas. Another participant indicated an overlooked port size layout as a vulnerability. A lack of surveillance methods and of human resources creates vulnerabilities to organised criminal groups. These responses show that there are different types of vulnerabilities facing Durban and Cape Town Maritime Ports of Entry that need to be examined. Vulnerability areas that can be spotted by criminal groups at Durban and Cape Town Maritime Ports of Entry include the receiving and distribution of goods areas as well as the ship or container to move illegal goods and drugs.

4.3.1.8.3 Security risks

Security Risks (Question 8.3)

Conceptual analysis of security risks:

Participant 1: Evaluate the threats and vulnerabilities in an area/environment. The risk factor should occur or take place and the impact thereof on an area/country or environment.

Participant 2: Attack on the port that could impact negatively on the functionality of the port.

Participant 3: Someone or something that is a risk to safety or could damage an organisation by giving information to an enemy of competitor.

Participant 4: Threats to security or a particular environment.

Participant 5: Where breach of security or corruption by any role-players at the port creates a security risk to the port in its operations thus creating an economic problem for South Africa.

Participant 6: The risk will always be there; we have to constantly change our ways of doing business to mitigate the risks. Security needs to be more advanced and changed with time in relation to the criminal activity encountered.

Participant 7: National key points, pollution/poaching, human trafficking, drugs, arms.

Participant 8: It is a transnational crime. CCTV cameras visuals at night [are] not clear. Foreigners employed as truck drivers as well as workers in the port.

Participant 9: Lack of intelligence. Unlawful access. Stowaways into the port or national key points.

Participant 10: It is the danger maritime can be facing like … weaknesses in port security. Is a criminal activity like cargo theft distribution to trade flow, attacking the ship to provoke human casualties and the use of the ship to launder illicit funds for terrorist organisation.

Interpretation

A majority of participants' answers to this question indicated that a security risk is the weakness in port security emanating from threats and vulnerabilities of the South African Maritime Ports of Entry's current security measures. Other participants described security risks as unlawful access, cargo theft distribution to trade flow, terrorist organisations exploiting ships to launder illicit funds, corrupt maritime security officials, stowaways boarding the ship, a lack of intelligence gathering to provide a real time and actionable intelligence and attacks on the ship by criminal syndicates. Moodley (2014:84) indicates that a security risk is any condition of the physical protection system to secure the port against internal and external threats.

Manig (2017:34-35) reveals that a lack of monitoring, control and surveillance measures exposes South Africa's Maritime Ports of Entry to risks of illegal crossing. Trafficking in human beings, drugs and illegal weapons through Maritime Ports of Entry are linked to insufficient road maintenance making the sea a popular destination for international trade. The security risks at South Africa's Maritime Ports are very similar and the challenges are very common to international challenges. The current security risks compel the South African government to look for solutions that meet international standards to address this issue. This will include introducing proper physical protection systems, developing multi-agency working relationships and utilising integrated resources, regional collaboration, and intelligence sharing.

4.3.1.9 The participants were asked the question: "Did you ever encounter drug smuggling, theft, human trafficking, vandalism, or any other criminal conduct while working at the Maritime Ports of Entry?" (see Annexure I question 9)

Interpretation

This was a yes/no question to see if any of the participants had encountered drug smuggling, theft, human trafficking, vandalism, or any other criminal conduct while working at the Maritime Ports of Entry. All participants indicated that they had encountered criminal conduct at Maritime Ports of Entry. This indicates that there are criminal activities at Durban and Cape Town Maritime Ports of Entry.

4.3.1.10 Crimes encountered at the Maritime Port of Entry (see Annexure I question 10)

Conceptual analysis of crimes encountered at the Maritime Port of Entry:

Participant 1: Smuggling of narcotics/endangered species, poaching, such as contraventions regarding Maritime Living Resources Act (MLRA), illegal immigrants/stowaways on vessels, theft/vandalism/foreigners working illegally in the country, corruption.

Participant 2: Some vessel called into port searched and found with endangered species, i.e., cobras, scorpions. Stowaway found. Crew member found with cocaine hidden in bag under his bunk in his cabin. Cocaine found in container loaded with chickens.

Participant 3: Counterfeit goods illegal goods container, illegal immigrants without permits.

Participant 4: Drugs, illegal fishing of abalone, unlicensed firearms, counterfeit goods.

Participant 5: Contraventions of drugs and drug trafficking, marine living resources, national road traffic act, stowaways, theft of motor vehicle with cargo, fraud and contraventions to the immigration.

Participant 6: I was working specifically with drug importation into and through the Port of Durban, so I was able to intercept with my team various shipments of narcotics substances, mainly cocaine, hashish Mandrax tablets, the biggest seizure the eleven tons of hashish.

Participant 7: Illegal importation of second hand motor vehicles, stowaways, drugs smuggling.

Participant 8: Transnational crime, CCTV cameras visuals at night not clear, foreigners employed as truck drivers as well as workers in the port.

Participant 9: Theft of containers/goods. Counterfeit goods smuggled into the port. Smuggling of drugs using containers. Illegal movement of stowaways through the port.

Participant 10: Drug smuggling prior to 2010 World cup. We stopped a container with electrical equipment and conducted a full offload and we recovered drugs. Mis-declaration. Counterfeit goods.

Interpretation

A majority of participants in this question indicated that smuggling of drugs that includes cocaine, and narcotics, unlicensed firearms, counterfeit goods and endangered species, such as cobras, scorpions and poaching of MLRA, are the majority of the crimes encountered at Durban and Cape Town Maritime Ports of Entry. Other participants mentioned illegal immigrants, stowaways, theft of cargo from containers and out of motor vehicles, corruption, illegal fishing of abalone, fraud and illegal importation of second hand motor vehicles.

According to the participants, many threats find their way into the ports of South Africa because of porous port access, corruption and weak port control systems.

Many participants mentioned causes of crimes at Maritime Ports of Entry in South Africa as the shortage of personnel and resources to search the goods and people at entry and exit points. The participants believed that all persons and goods should be checked at every entry and exit point to prevent smuggling goods without a manifest.

4.3.1.10.1 Method used by perpetrators to commit crimes at Maritime Ports of Entry (see Annexure I question 10.1)

Conceptual analysis of the method used by perpetrators to commit crimes at Maritime Ports of Entry:

- Concealment;
- False documentation;
- Corruption by port officials (including assistance by officials);
- Counterfeit goods; and
- Undeclared goods

Interpretation

Participants were provided with a list of methods used by perpetrators to commit crimes at Maritime Ports of Entry. The participants were free to choose from six variables. Eight participants indicated concealment as the primary method of committing crimes at Durban and Cape Town Maritime Ports of Entry, followed by seven participants who indicated false documentation. Six participants indicated corruption by port officials, while five participants indicated counterfeit goods as the methods used by criminals to commit crimes. Only one participant indicated undeclared goods as the least common method used by perpetrators committing crimes at Maritime Ports of Entry. According to the participants, the wave of crimes committed in South African Maritime Ports of Entry is worsened by false documentation, corruption, poor port infrastructure design and layout, poor training of personnel and a lack of physical protection systems such as CCTV cameras, scanners, surveillance equipment and biometrics.

According to Moodley (2014:83), concealment refers to tampering and counterfeiting of container seals and emptying the contents while the container is in the port of its destination. Participants said concealment meant that cargo could be disrupted or replaced while on its way to the next Port of Entry. Participants expressed concern that container searches were conducted on an occasional basis because Maritime Ports of Entry did not have sufficient personnel or resources to do so regularly. Aamilid (2019:69) found that Custom officials and SAPS officers opening suspected containers reduces the chances of trafficking, smuggling and stowaways. Meanwhile, false documents and corruption, including assistance by security personnel, are the most popular means of removing goods from the Durban Maritime Port (Moodley, 2014:50).

Given the high level of corruption in South Africa's Maritime Ports of Entry, participants suspected that the current security system is weak and leaky. Although maritime security officials are screened and vetted before being employed, participants said that the integrity of maritime security officials should be checked more often to prevent corruption at Maritime Ports of Entry. Maritime Ports of Entry require consistent transparency and co-operation from all stakeholders to protect the port from internal threats.

The participants revealed that counterfeit goods are detected by Custom officials and SAPS officers hidden inside containers during search and inspection processes. Other participants reported that undeclared goods were used by perpetrators to commit crimes because Maritime Ports of Entry do not have the capacity to physically open and check the contents of every consignment. This hole will only be closed if a physical examination of all goods in the warehouse is an ongoing procedure. However, a shortage of personnel and resource prevented this at all South African Ports of Entry.

4.3.1.11 Resources used to detect security risks at Maritime Ports of Entry (see Annexure I question 11)

Conceptual analysis of resource used to detect security risks the Maritime Ports of Entry:

- Detector dogs;
- Non-intrusive examination through the use of technology;
- Trace particle detection;
- Physical examination of cargo or ship;
- Rummage of ship;
- Stop and search operations; and
- Profiling of ship

Interpretation

Participants were provided with a list of resources used to detect security risks at Maritime Ports of Entry. The participants were free to choose from seven variables. Nine participants cited physical examination of cargo ships for identifying and detecting illicit substances and goods hidden in vehicles, trucks, vessels and containers. Eight participants indicated detector dogs as the primary methods used to detect security risks. Two participants selected non-intrusive examinations through the use of technology and profiling of ships. One participant mentioned the rummage of ships and stop and search operations.

The analysis indicated that the Durban and Cape Town Maritime Ports had various

resources to detect security risks. These are security measures used to protect the supply chain risks of cargo theft, drug smuggling and contraband. The lack of physical and technological resources to examine and screen cargo, as indicated by a majority of participants, could be the reason for the smuggling of goods, theft, stowaways and contraband. In the past, full containers were stolen from Durban port terminals and illegal items, including counterfeit cigarettes, clothing, drugs as well electronic items, were in high demand (Moodley, 2014:82). Equipping Maritime Ports of Entry with advanced inspection tools to screen shipments rapidly for illegal weapons, drugs and other contraband will assist maritime security officials to perform their work effectively.

4.3.1.12 Do you think that the resources used by Maritime Ports of Entry to detect security risks are effective? (see Annexure I question 12)

This was a yes/no question designed to determine if all participants believed the resources employed by Maritime Ports of Entry to detect security risks were effective. Six participants stated that Maritime Ports of Entry resources were ineffective. The other four participants indicated that the resources employed by Maritime Ports of Entry were effective to detect security risks. According to the responses provided above, the resources available at Maritime Ports of Entry do not assist maritime security officials from stopping people, weapons, narcotics, and contraband from entering the country illegally.

4.3.1.12.1 Other resources recommended to detect security risks at Maritime Ports of Entry (see Annexure I question 12.1)

Conceptual analysis of other resources recommended to detect security risks at Maritime Ports of Entry:

Participant 1: Proper intelligence and technology. Interlinking with other countries for intelligence information. Inter linking working relationships with role-players within port/border maritime environment. Proper operated modernised equipment.

Participant 2: Upgraded and up-to-date technology to be used to profile vessels/route and crew. Interaction with Interpol/other law enforcement agencies. To profile vessels /route and crew.

Participant 3: Searches.

Participant 4: Dog unit, profiling, investigation Unit and proper equipment.

Participant 5: Due to the infrastructure and design of the port, in my own opinion, the port needs to be re-designed since much of the cargo is transported by road and not rail. Further, the port must not be accessible by the public except role-players only.

Participant 6: More can be done with regards to interception of containerised cargo shipments; better inter-departmental cooperation; better long-term task teams; permanent Anti-Drug Team set up; better co-ordination with port terminals, i.e., Transnet.

Participant 7: Searching and inspection equipment needed.

Participant 8: The entrances to some parts of the port are opened. More scanners needed to scan containers entering and leaving the port. Government resources/personal in some departments are minimum.

Participant 9: Upgrades on our current surveillance methods. More effective technology used in the tracking and tracing of containers. Effective scanning equipment to control the access of people within the port.

Participant 10: Even though I said yes, but they are conducting random searches. Resources need to be improved by installing scanners so no container will drive through without being searched.

Interpretation

Regarding resources to detect security risks at Maritime Ports of Entry, a majority of participants proposed sharing intelligence information and coordination among regional and global stake-holders. Some participants cited proper resources and equipment to scan and search containers, goods and people entering and leaving the ports while others added the need for training detector dogs and anti-drug team units as well as re-designing port infrastructure to prevent public access. One participant indicated upgraded surveillance technologies for tracing and tracking containers.

The responses above show that maritime security officials need dedicated resources to make it more difficult for criminals to commit crimes in coastal areas. Increased intelligence sharing and gathering combined with closer working relationships with maritime contractors and companies operating in the coastal areas, can lead to better intelligence and generate better results.

The South African security sector has a tendency to withhold information from other stakeholders because government authorities protect their interests and resources. However, much of South Africa's intelligence is inaccessible in comparison to other nations' intelligence that can be found on open source networks (Manig, 2017:51). This requires supporting and empowering maritime security officials with advanced technological systems for investigating and profiling criminal syndicates, detecting illegal goods and drugs.

4.3.1.13 Areas vulnerable at the Maritime Ports of Entry? (see Annexure I question 13)

Conceptual analysis of areas vulnerable at the Maritime Ports of Entry:

Participant 1: Sea borders in South Africa coastlines not policed and patrolled as it should be. Environment fishing industry/pollution/illegal immigrants flooding our ports/crossing borders entering our country.

Participant 2: The entire quay side can be easily accessed by a person using a small craft (small boat). The port of Durban is an easy port to infiltrate. The security measures that are in place are inadequate.

Participant 3: Anywhere in the port.

Participant 4: Perimeter fence, entry to port from the sea.

Participant 5: Security guards at access points need to be more security conscious and trained in terms of the port environment possessing knowledge on crimes, persons and goods.

Participant 6: Maritime smuggling of goods in containers is the biggest threat to any country. Simply, if we can establish what the content of any container has by physical

examination or x-ray. This is an enormous task, considering the elements against law enforcement, cargo volumes, trust, corruption [and] other tasking.

Participant 7: No public slipways. Launch site in the port area.

Participant 8: Entrance points in Langeberg Road/Bayhead Road entrance/Maydon Wharf.

Participant 9: Access points at port of entry. Trucks' and containers' screening point.

Participant 10: Inner and out perimeters. Illegal movement of goods. Contraband smuggling and stolen vehicles. Stowaways, cargo theft.

Interpretation

Regarding vulnerable areas at the Maritime Ports of Entry, the responses cited access control. Two participants indicated that the port perimeter fencing is vulnerable, another participant said that there is easy access to the entire quay side of Durban Port by small craft. One mentioned problems at the launch site or the area near the sea water and one participant mentioned the entrance points at Langeberg Road/Bayhead Road/Maydon Wharf of Durban Maritime Port of Entry. The other participant added unregulated and unpatrolled port areas, followed by one participant who complained of unscreened trucks and containers arriving at the Port of Entry with cargo. According to this participant, trucks and containers are used by criminals to smuggle goods, drugs and contraband. Bernard (2015:16) points out that computers and communication systems used by maritime security officials to share sensitive information about their international maritime trade activities could be compromised. Criminals can use a computer information system in the port to detect hazardous goods for destruction. Therefore, the lack of measures to protect the port, ships and crews puts the entire facility at risk from criminals and terrorists.

4.3.1.14 What level of security risks do the under mentioned crimes pose at Durban and Cape Town Maritime Ports of Entry? 0=No risk; 1=low risk, 2=medium risk and 3=high risk (see Annexure I question 14).

Conceptual analysis of crime:

- Illegal immigration;
- Container crimes;
- Drug trafficking;
- Stowaways;
- Armed robberies;
- Human trafficking; and
- Vandalism

Interpretation

Participants were provided with a list of crimes that pose security risks at Durban and Cape Town Maritime Ports of Entry. The question had seven variables that participants were free to choose from. Nine participants cited illegal immigration and container crimes as high risk crimes. The participants said that South African Ports of Entry were neglected and complex to manage. Six participants indicated drug trafficking and stowaways as the main crime risks. This was followed by corruption of maritime security officials while armed robbery, human trafficking and vandalism were the lowest crime risks at Durban and Cape Town Maritime Ports of Entry.

The South African maritime industry suffers from violations of ethics such as bribery and corruption by maritime security officials and the presence of criminal groups in the maritime industry. Any intrusion damages the integrity and dignity, and compromises the security of the port. The challenge for the South African Maritime Ports of Entry is infrastructure that allows criminals easy access to facilitate illegal smuggling of drugs and other criminal activities.

A maritime container is a good way to transport drugs because it is difficult to tell if there are any drugs concealed inside. The study found that many containers are not checked until they reach their port of call. Furthermore, Maritime Ports of Entry in

South Africa check fewer than five percent of containers. Illegal immigration was equally mentioned by the participants and terrorism that can result in harm to the port's infrastructure, assets, and facilities.

4.3.1.15 What level of security risk do the physical protection systems listed below pose at Durban and Cape Town Maritime Ports of Entry? 0=No risk; 1=low risk, 2=medium risk and 3=high risk? (see Annexure I question 15)

Conceptual analysis of level of security risk posed by the physical protection systems:

- Access Control;
- Perimeter Fencing;
- CCTV cameras;
- X Ray Scanners;
- Metal Detectors;
- Egress Control;
- Security Lighting;
- Human Security/Guards;
- Alarm systems;
- Parking areas; and
- Storage areas

Interpretation

Regarding the level of security risks posed by physical protection systems at Durban and Cape Town Maritime Ports of Entry, a majority of participants indicated access/egress control, perimeter fencing, CCTV cameras, x-ray scanners and metal detectors as the highest risk areas at Maritime Ports of Entry. Others mentioned egress control, security lighting, human security/guards, alarm systems, parking areas and storage facilities as medium security risks areas at Durban and Cape Town Maritime Ports of Entry.

Moodley (2014:94) indicates that access and egress control are the highest risk areas

at Durban Maritime Ports of Entry, followed by monitoring systems, perimeter fencing and x-ray scanners. Participants said that a lack of proper security equipment to check and screen vessels entering the cargo terminals to deliver or to collect goods hinders maritime security officers' ability to recognise illegal activities. This increases the threat of smuggling, theft, and vandalism. Criminals know that they can pass through the Ports of Entry undetected. Other participants said that increasing security control systems, such as biometric systems, x-ray machines for searches, CCTV cameras, security barriers, perimeter fencing and lighting at Maritime Ports of Entry, can deal with these challenges. Checking documentation or access permits when the vessel enters the cargo terminal, either to deliver goods or to load goods, is another control measure.

4.3.1.16 Describe specific factors pertaining to the discipline of security officials that can be considered as human risks (see Annexure I question 16)

Conceptual analysis of specific factors pertaining to discipline of security officials that can be considered as human risks:

Participant 1: Corruption, lack of knowledge and training.

Participant 2: Not conducting proper searches, e.g., open car boot, stand back and take a peek. Not physically searching the boot. When bad weather leaves booms unmanned allowing free access (afraid of weather conditions). This practice creates an opportunity for criminals to operate.

Participant 3: Not answered.

Participant 4: Sleeping on duty, ethical conduct.

Participant 5: If a security official has no passion for his job. This alone can be considered as human risks at Maritime Ports of Entry.

Participant 6: Security personal at normal facilities or business units are not trained in maritime security, they are not too familiar with ports, how they operate, what to look out for, crew and cargo; what risks they bear, ISPS codes, etc. So I am of the opinion [that] at the conventional berth/facilities, they are merely security guards.

Participant 7: Lack of training, lack of inspection (sleeping on duty).

Participant 8: Not all security officials are trained in ISPS Code, corruption/extortion.

Participant 9: Corruption - security personnel are easily influenced. Desertion of posts. Absenteeism.

Participant 10: Corruption police officials at the Maritime Ports of Entry. Pressure from organised criminal syndicates. Discretional power that is given to SAPS. Lack of ethical standards. Poor external oversight, quality of regulations.

Interpretation

In responding this question, a majority of participants stated that maritime security officials do not conduct proper searches which the other participants suspected to be caused by a lack of proper equipment to scan goods and people. Some participants indicated that maritime security officials have negative attitude towards their work, they are careless and they sleep on duty. Others added corruption by security officials caused by discretional power given to them, a lack of good ethics and pressure from organised crime syndicates. Two participants also added a lack of ISPS Code training. Mlambo and Adetiba (2021:104) believe that South Africa's quest to strengthen its borders and Ports of Entry capabilities is being undermined by corrupt officials and organised crime syndicates. The responses received above show that the functions performed by maritime security has certain inherent risks.

Aamilid (2019:70) said that maritime security officials were known for corruption, collusion with criminals and stealing. Mlambo and Adetiba (2021:105) said criminals can enter the security system if maritime security officials become dissatisfied due to poor pay, inadequate benefits and lack of opportunity for growth Furthermore, maritime personnel are known to be overwhelmed by too many activities. These conditions, in addition to lower costs make them indifferent to pursuing maritime policies that are intended to prevent crime in the Port of Entry.

SECTION C: ROLES AND RESPONSIBILITIES OF MARITIME SECURITY

4.3.1.17 What is your understanding of the concept "Maritime Security"? (see Annexure I question 17)

Conceptual analysis of the meaning of maritime security:

Participant 1: To address vulnerable areas/threats in the maritime environment and to secure those areas/threats by means of laws/policies [and] action plans to lessen the risks.

Participant 2: Ensuring safety and security of maritime community, i.e., ocean going vessels and crew. Small crafts and safety of the port and its facilities.

Participant 3: It classifies the issues in the maritime domain that are often related to national security, marine environment, economic development and human security.

Participant 4: To safeguard and protect harbour related areas as well as sea borderline access.

Participant 5: Security and protection of international and national ships including the port facility.

Participant 6: Maritime security is security that has to do with anything pertaining to the facility, cargo, ships and crew. How they need to be safe guarded and which type of crime could be anticipated in this environment.

Participant 7: National strategy to protect the port and its interests in maritime regions. To detect and combat transnational crimes within the territorial waters of SA [to] create a crime free maritime environment.

Participant 8: Maritime security is a general term for the protection of vessels both internally and externally. The areas from which ships and maritime operations need protection include terrorism, piracy, robbery, illegal trafficking of goods and people, illegal fishing and pollution.

Participant 9: Safeguarding of all entities within the port of entry.

Participant 10: Protective measures taken to protect services at Maritime [Ports] is to prevent and limit anything that may threaten safety and security of the port. To prevent illegal movement of illegal goods, trade and people.

Interpretation

A majority of participants viewed maritime security as the protection or safe guarding of maritime entities such as containers, vessels, port, crew and people. Another participant viewed maritime security as a national strategy created to protect the ports and its interest while others viewed maritime security as the implementation of policies and laws to address threats, vulnerabilities and security risks affecting Maritime Ports of Entry. One participant said that maritime security is placing protection measures to prevent the port from terrorism, piracy, robbery, illegal trafficking of goods and people, illegal fishing and pollution.

Regarding the meaning of maritime security, all participants understood that maritime security is a dependent environment with sensitive areas which must be secured from terrorism, piracy, robbery, theft and smuggling. According to the participants, South African maritime security can be strengthened by laws, policies and action plans aimed at enhancing inter-agency and international cooperation and coordination. From a participant's view, the best way South Africa's maritime security could be achieved was to bring all stakeholders under one roof because government officials follow the standard rules of operation. Martin (2021) says that a lack of security control systems dedicated to Maritime Ports of Entry, especially on the African coast, is a challenge to the success of maritime security. Many coastal regions of Africa focus more on air protection and inland ports than on sea protection. This has created an increase in maritime crimes such cargo and vehicle theft, undocumented immigrants and stowaways, trade fraud and firearms smuggling at the Ports of Entry.

The global maritime industry thrives on the sharing of information, policies, resources and international governance to identify threats, vulnerabilities and to protect maritime interests.

4.3.1.18 Describe your role and responsibilities in ensuring security at Maritime Ports of Entry (see Annexure I question 18)

Conceptual analysis of the roles and responsibilities in ensuring security:

- Access control;
- Patrol duties;
- Guard duties;
- Inspections of goods/permit;
- Surveillance/control room; and
- Rummage on vessels

Interpretation

Participants were given a list of roles and responsibilities in ensuring security at Maritime Ports of Entry. The question had six variables participants were free to choose from. Nine participants indicated that they are responsible for patrols, followed by eight participants who is responsible for the inspection of goods/permits, five participants work at access control points, four participants perform guard and surveillance/control room duties, while one participant is responsible for rummage and inspection of vessels.

The roles and responsibilities indicated by participants above show that maritime security officials at Durban and Cape Town share their functions with other role players. This is a challenge because law enforcement and operational procedures are not the same at the South African Maritime Ports of Entry. Van Nieuwkerk and Manganyi (2017:10) explain that the major challenge at South Africa's Maritime Ports of Entry is the lack of a comprehensive maritime strategy or policy that regulates functions of the various role-players in the maritime environment. This problem results in the duplication of activities by maritime role-players. According to the Parliamentary Monitoring Group (2013), South Africa's Ports of Entry do not have the resources to deal with the production of all maritime security officials. In addition, the capacity allocated to the Ports of Entry was not scientifically determined. The Department of Home Affairs (DHA), for example, operates with a very low capacity and is not providing quality services therefore deployment at the Ports of Entry was not done or,

in some cases, was done casually. This has led to people entering the country without proper documentation (Parliamentary Monitoring Group, 2013).

4.3.1.19 What intervention/s are used by maritime security officials to address security risks at Maritime Ports of Entry? (see Annexure I question 19)

Conceptual analysis of the intervention/s used by maritime security officials to address security risks:

- Cross-border cooperation;
- Information sharing; and
- National joint operations

Interpretation

Participants were provided with a list of intervention/s used by maritime security officials to address security risks. The question had three variables for participants to select from. Eight participants mentioned national joint operations, four participants indicated information sharing, while three participants indicated cross-border cooperation.

In answering this question, participants noted national-joint operations as the most effective way to share vital maritime information of interest with other role-players. However, a majority of participants said that inter-agency coordination and collaboration amongst maritime role-players in South Africa is lacking or non-existent. Van Nieuwkerk and Manganyi (2019:11) agree that a lack of inter-agency cooperation at Maritime Ports of Entry is caused by the absence of policy that governs the conduct of the various role-players in the South African maritime domain. The participants recommended the sharing of information between maritime government stakeholders. Walker and Reva (2020:13) also maintain that South Africa supports the importance of information sharing to enforce law at sea.

Most participants complained that maritime stakeholders are not willing to share information with each other, while some suggest that governments be made aware that information sharing is necessary for building trust and combating transnational crime for collective benefit and for taking joint legal actions such as the prosecution

and sentencing of criminal syndicates. To facilitate a more accurate regional and global picture requires each country's understanding of maritime crimes to be more closely aligned so that developing crime patterns can be properly understood for better responses.

Participants showed that cross-border cooperation is a challenge in South Africa. Mlambo and Adetiba (2021:106) further state that migration and cross-border crimes jeopardise the sovereignty and security of the South African Development Community (SADC) and endanger lives and safety of those operating at sea. Participants agreed that South Africa can make a substantial contribution to regional maritime security cooperation while also benefiting from it. According to Manig (2017:34), drug trafficking in South Africa is caused by the absence of international cooperation, inconsistencies, political obstacles, and poor marine governance. Efforts to exchange information and communicate with other countries' role-players are hindered by mistrust, diversity in the law enforcement structures, the absence of communication channels, different approaches and priorities. The participants stressed that the most essential component of proactive cooperation is to adopt a uniform international legal framework, strengthen capacities, expand relationships, and encourage holistic crime prevention approaches.

4.3.1.20 What challenges do the global and regional maritime security stakeholders face at Maritime Ports of Entry? (see Annexure I question 20)

Conceptual analysis of global and regional maritime security stakeholder challenges:

Participant 1: Whatever is been shared at top level, very minimum is filtered down to ground level workers. I rely on keeping myself updated on crime/smuggling trends in the world by means of the news and web search.

Participant 2: Not all role-players are willing to share information. Most are working in silos.

Participant 3: Not answered.

Participant 4: One major challenge is working as one team.

Participant5: Challenges are vast as very little or no information is being shared with regards to vessels and its cargo, including the crew on ships.

Participant 6: Information sharing of particular action as undertaken, especially when cargo missed at a certain point. Or information profile techniques would show that a possible success is or should be achieved in a shipment. Not enough inter port communication takes place, especially along East Africa.

Participant 7: The transparency between the maritime role-players is lacking. Information sharing is limited. Lack of human resources.

Participant 8: Each department working in Port of Entries, having their own mandate and different legislation. Lack of human resources.

Participant 9: Not answered.

Participant 10: Other agencies are not transparent; this is due to trust.

Interpretation

This question was asked to determine challenges faced by global and regional maritime security stakeholders at Maritime Ports of Entry. A majority of participants indicated the lack of transparency, communication and information sharing among maritime role-players, especially in East Africa. Other participants mentioned that maritime security officials are separated from each other because stakeholders are working in silos. One participant shared that a lack of trust, separate mandates and legislation affected cooperation. Participants added that it was due to the absence of human resources and coordination between management and subordinates, while two participants did not answer the question.

The key point to emerge in considering the issue of illegal immigration and smuggling of drugs and goods by sea is that one State cannot succeed alone. Cross-departmental exercises are a technique to break down silos through educating, working, and training together.

Manig (2017:41) indicates that the National Joint Committee in Pretoria is the country's planning, reaction, and coordination hub, with security sectors from all over the country

participating. The problem with this arrangement is that it only considers land borders and ignores sea borders. Manig (2017:37) also pointed to an inadequate coordination between government agencies responsible for policing, guarding, and securing Maritime Ports of Entry. As illegal immigration and smuggling of drugs and goods are transnational crimes requiring transnational responses, a cooperative regional strategy amongst coastal governments that fosters dialogue rather than conflict, reassurance rather than deterrence, openness rather than secrecy, prevention rather than correction, and interdependence rather than unilateralism can provide significant benefits (Kumar, Dwivedi and Hussain, 2016:vii).

4.3.1.21 How many incidents of crime do you discover during a month? (see Annexure I question 21)

Conceptual analysis of incidents of crime discovered during a month:

- 1-5 incidents;
- 6-9 incidents;
- 10-14 incidents;
- 15-19 incidents; and
- 20 and more incidents

Interpretation

This question was posed to ascertain the number of incidents of crime discovered by maritime security officials during a month. Three participants reported witnessing 15-19 incidents, followed by three more who reported witnessing 6-9 incidents and the other three reported witnessing 1-5 crimes a month. There was just one participant who witnessed 20 or more incidents of crimes a month. The responses above indicate that the port needs various security measures to curb crime. Security measures that can be used to mitigate crime at Maritime Ports of Entry include the visibility of maritime security officials and the installation of CCTV cameras in every area of the port. Elago (2019:82) believes that the main solutions include technological components which are burglar alarms, CCTV camera systems, as well as electronic key cards.

4.3.1.22 What, in your opinion, are the factors that promote illegal immigration and smuggling of illegal goods through Maritime Ports of Entry? (see Annexure I question 22)

Conceptual analysis of factors that promote illegal immigration and smuggling of illegal goods through Maritime Ports of Entry:

Participant 1: Lack of proper border control and policing along SA borders. Participant 1: Smuggling. Lack of proper infrastructure, technology, training of personnel and joint intelligence sharing and working between role-players. Lack of equipment that is more modernised to detect and is not enough to cover all the ports.

Participant 2: Illegal immigrants usually use the port as access to stowaway in order to sail to the United Kingdom (mostly). It may seem easier to smuggle through a maritime port of entry than the airport.

Participant 3: Proper searching by security officials or security officials that is not well trained.

Participant 4: Corruption of officials.

Participant 5: Road transport, poor inspection of persons and goods on ships arrival due to lack or poor information sharing, this leads to promote illegal immigration and smuggling of illegal goods.

Participant 6: Illegal immigration or stowaways. These persons are always looking for a better life in Europe or America. Africa has no hope for them. Smuggling of goods: is the share profit margin, counterfeit or narcotic goods.

Participant 7: Money/greed.

Participant 8: Corruption in terms of bribery towards government's officials, criminals colluding with private security and government officials.

Participant 9: Better way of life, easy access into the country, corruptions. Lack of training of personnel in identifying and verifying counterfeit goods and documents.

Participant 10: Corruption. Burdensome processes and procedures. High tariffs. Illegal

immigration is caused by the desire to migrate away from poverty and oppression in search for better lives. This is a push factor they cannot resist.

Interpretation

Regarding factors that promote illegal immigration and smuggling of illegal goods, the majority of participants mentioned the lack of proper port security control systems to manage restricted areas and the lack of trained officials to identify and verify documents, smuggled goods, counterfeits or narcotics, followed by poor port infrastructure and road transport. Another participant spoke of easy access to the port by criminals. Three participants added corruption, bribery and greediness. Two participants also added stowaways hiding in ships to sail to America, Europe and the United Kingdom in search of a better life.

According to the analysis above, illegal immigration and smuggling of goods is a transnational crime perpetrated by organised criminal syndicates. According to Manig (2017:41), each South African government department has its own monitoring, operational, and coordination systems to ensure its own efficiency. Because of this silo approach, maritime security key stakeholders are unable to collaborate in a systematic and coordinated manner. Moodley (2014:90) says that maritime security officials at Durban Maritime Ports of Entry only search one percent of total goods and passengers. Other participants believe that a lot of illegal immigrants and smuggled goods are slipping through the present detection methods. The port is prone to smuggling of contraband due to a lack of experienced personnel in identifying counterfeit goods, fake documentation and permits, and concealment methods. Potential criminals are well informed about each country's maritime protection challenges and they can enter either the security systems meant to safeguard port infrastructure or the organisations responsible for maintaining it.

4.3.1.23 Describe the security assessment briefing given to security officials at Maritime Ports of Entry (see Annexure I question 23)

Conceptual analysis of security assessment briefing given to security officials

at Maritime Ports of Entry:

Participant 1: International Ship and Port Security (ISPS) Code.

Participant 2: Police officers are briefed daily on the Criminal Threats Analysis of the Port of Entry precinct.

Participant 3: Not answered.

Participant 4: No decent briefing.

Participant 5: Each situation experienced will entail a different security briefing in the SAPS. Crime threats and crime patterns will determine the particular briefing.

Participant 6: Most security officials are merely looking at access control duties, following rules of that facility or business unit, petty crime of thefts. Actual security officers, very little in my opinion.

Participant 7: Basic border security management course, ISPS Code.

Participant 8: Most security officials are informed about security related issues to that facility. Main focus is the theft of goods or property and illegal entry to that facility. Only national key point security officials (guard) are armed and briefed in ISPS Code.

Participant 9: Members are briefed on a daily basis. This is done at regular meetings and forums. Daily crime trends, patterns, hotspot areas outlined.

Participant 10: We know and understand our SAPS functions with police base development training but not in connection with maritime or port of entry. Employees are using their own discretion with assistance from customs members. I have never been to any training.

Interpretation

Regarding the security assessment briefing given to security officials at Maritime Ports of Entry, a majority of participants acknowledge that security assessment briefing was available at Maritime Ports of Entry. Most participants said they had been briefed on daily crime threats and patterns, hot spot areas, access control and theft of goods and

property. Three participants added the ISPS Code, but one participant said ISPS Code briefing is only provided to armed security guards deployed at national key points. Three participants said that the briefing they received was not related to maritime security functions but were to help them to perform SAPS functions. One participant stated that their authorities do not provide them with decent briefing, while one participant did not answer the question.

From the responses received above, it is evident that security briefing is an essential tool to prevent Maritime Ports of Entry threats, vulnerabilities and security risks. Regular security assessment briefings give awareness of current security concerns, detection of drugs, devices, and recognition of behavioural patterns of individuals who may pose a hazard to the port facility's functioning. The study found that no integrated assessment has been developed by South African maritime security stakeholders to provide joint briefings to address changing security needs and emerging threats as well as to improve the skills levels of maritime security officials. Manig (2017:41) also says that South Africa has no maritime security exercises that have been planned or executed involving all maritime security role players to assess the level of incompatibility and differences in policy and operational procedures. Stakeholder joint assessment conforming to the current maritime security challenges will benefit South Africa to achieve the highest level of compliance with international security measures. Engagement with various stakeholders aids policymakers in determining where new law enforcement might have the biggest positive influence in these self-reinforcing cycles.

4.3.1.24 Explain the legal framework and the policies that govern your work as a maritime security official (see Annexure I question 24)

Conceptual analysis of the legal framework and the policies that govern the work of maritime security official:

Participant 1: Police Act, Merchant Shipping Act, Marine Living Resources Act (MLRA), Immigration Act, Customs Act.

Participant 2: Section 13(6) of the Criminal Procedure Act. Search warrant and arrest. Drug and drug Trafficking Act.

Participant 3: Not answered.

Participant 4: As a border police official, our legal framework falls under the Border Police Act and mainly concentrates on Article B/6 where no Search Warrant is needed to conduct stop and search and also the MLRA.

Participant 5: All legal framework and policies are in place. As explained, a role the passion in an official would determine the success of a port both criminally and economically.

Participant 6: As border police officials will rely heavily on Section 13.6 of Police Act 68 of 1995. This allows us to search any person or vehicle, vessel, luggage or any other object that the person or truck would be carrying. It's very suitable to all border police officials.

Participant 7: SAPS Act 68 of 1995 Section 13(6), Merchant shipping Act 57 of 1951, Maritime Zone Act 15 of 1994, Firearm control Act 60 of 2000, Drugs and drug trafficking Act 140 of 1992, Human trafficking Act1957, Immigration Act 13 0f 2002, Customs and excise Act 91 of 1964, Marine living Resource Act 18 of 1982.

Participant 8: As a SAPS office, we have many laws that we can rely on or use but, from a border police perspective, Section 13.6 of the Police Act gives specific powers to search and seizure of any goods without a warrant. This section is possibly all that is required at Port of Entry and is effective.

Participant 9: SAPS Criminal Procedure Act. The United Nations Laws of the SA. The ISPS Code and the International Maritime Organisation (IMO).

Participant 10: The Constitution of South Africa Act no105 of 1996. Police Act 68 of 1995. Labour relations Act 6 1995. Criminal procedure Act 51 of 1977. Counterfeit goods Act 25 of 2001. Agricultural distiller Act 19 of 1004. Duties and power of the officer Act 34 of 1997.

Interpretation

With regards to the legal framework and the available policies that govern the work of maritime security officials, the majority of participants mentioned SAPS Act 68 of 1995

and Section 13(6) Search and Seizure without warrant. Other participants indicated MLRA, Merchant Shipping Act 57 of 1951, Maritime Zone Act 15 of 1994, Firearm Control Act 60 of 2000, Drugs trafficking Act 140 of 1992, Human trafficking Act 1957, Immigration Act 13 0f 2002 and Customs and Excise Act 94 of 1964. The same participants further added the Constitution of South Africa Act no105 of 1996. There is only one participant who added IMO regulation and ISPS Code and one who did not answer the question.

Based on the responses given above, the majority of participants are more aware of the policies that govern Maritime Ports of Entry in South Africa. A majority of participants indicated that SAPS officers rely on Section 13(6) of SAPS Act 68 of 1995 for maintaining effective and competent policing of all South Africa's Ports of Entry and borders. According to participants, Section 13 (6) is a Search and Seizure policy that allows SAPS officers to search vessels, goods and people without a search warrant (South Africa, 1995). The Anti-Trafficking Act 7 of 2013 is a regulation that helps maritime security officials to prohibit and counter trafficking of human being crimes at the Port of Entry, as well as to protect the rights of victims (South Africa, 2013). The IMO, ISPS Code and the Merchant Shipping Act 57 of 1951 spell out security measures that coastal governments might use to protect vessels, crews, and cargo in transit or at ports (South Africa, 1951; Pohlit, 2014:16). The MLRA Act 18 of 1998 safeguards the social, economic, and environment of the country (South Africa, 1998). Customs and Excise Act 91 of 1964 establishes rules for the collection of customs and excise charges, as well as the limitation and control of unauthorised importation of goods or contraband through the Port of Entry (South Africa, 1964). Home Affairs officials also use the Immigration Act 13 of 2002 to ensure that Maritime Ports of Entry are properly secured, allowing illegal immigrants to be identified, minimised, and prevented (South Africa, 2002).

A key challenge to combatting maritime criminal activities is the absence of harmonised knowledge of the phenomenon and legal definitions of maritime security among the role-players involved. When policies are not unified, different approaches may be taken in response. The flaws and the gaps in the government's regulations, as well as how those policies are perceived, can have a considerable influence on the methods utilised by criminals. To close the gap in current legal frameworks requires a

global harmonisation of understanding in accordance with the methods utilised by criminal syndicates.

4.3.1.25 Describe the type of training that should be provided to officials in your department who are employed at Maritime Ports of Entry (see Annexure I question 25)

Conceptual analysis of the type of training that should be provided to officials who are employed at Maritime Ports of Entry:

Participant 1: International training to learn more from bigger ports. Smuggling/terrorism. Human trafficking. Boarding of vessels out at sea. Narcotic detection. Fishing industries and poaching.

Participant 2: ISPS Code. Anti-terrorism/piracy. Drug and contraband identification. Counterfeit goods identification. Endangered species.

Participant 3: Officials must be trained according to their job description.

Participant 4: All maritime training courses: Swimming Pre-sink, Deck Handler courses, Skipper Courses and Vessel Rummage courses, etc.

Participant 5: Every official should be trained in policing Customs and Immigration duties.

Participant 6: Must have knowledge of what the seaport is about, how it operates, cargo, person, how goods are moved, containerised process, ISPS code. What possible crimes could occur or have occurred and how to mitigate those crimes/threats.

Participant 7: Academy to be established and situated in the maritime environment and be a theory and practical phase. Recruitment phase must be in line with the maritime environment. Specialised training to be completed within the maritime environment. The training must be accredited.

Participant 8: Maritime patrol and coastal interdiction is very important. Hence all matters relating to policing at sea, anchorage, basil shipping. Training is needed on

cargo processes, containers, profiling, inspection of these containers.

Participant 9: Maritime development programmes. All maritime related laws and functions.

Participant 10: Reading of documents, counterfeit identification.

Interpretation

Regarding the type of training that should be offered to maritime security officials, a majority of participants indicated training on contraband, counterfeit and false document identification. Some mentioned containerised and rummage vessel courses while one cited the boarding of vessels and ISPS Code training. There were participants who require international and in-house training on all maritime related functions, including customs and immigration duties and others added anti-drug and piracy training as well as training to profile suspicious vessels, containers and crew.

The responses received above show that training is needed by all maritime security officials to develop skills and competencies to perform their roles and responsibilities. According to Manig (2017:41), there has been no training and development programme for maritime security stakeholders in South Africa. This is confirmed by a study by the Parliamentary Monitoring Group (2013), which said that South Africa has a shortage of skills for detecting false documents, face recognition, monitoring asylum seekers, and checking conveyances at the Ports of Entry. With the ever present threat of piracy, smuggling, stowaways and other security related incidents at Maritime Ports of Entry, the experience of maritime security officials signifies their abilities to deter or prevent the advancement of maritime threats. The training of all maritime security officials on ISPS code, other security related courses and the use of advanced technology is essential.

4.3.1.26 Do you think that maritime security officials should be trained jointly? (see Annexure I question 26)

Conceptual analysis of joint training of maritime security officials:

This was a yes/no question to see if all participants agreed that maritime security

officials should be trained together. Seven participants agreed to joint training of maritime security officials, while three participants did not agree.

Interpretation

According to the responses above, a large majority of maritime security officials believe that collaborative training is necessary to promote collaboration in the defence of Maritime Ports of Entry against threats and weaknesses.

4.3.1.26.1 If your response to question 26 is yes, discuss your reasons for joint training (see Annexure I question 26.1)

Conceptual analysis of the reasons for joint training of maritime security officials:

Participant 1: Different role-players are working in their "own camps" so to speak, not sharing and yet we all have the same goal.

Participant 2: I think we should have all officials working under one umbrella. Have one mandate and have all policies aligned to such mandate.

Participant 3: They must have the same training with customs and immigration and Department of Agriculture Forestry and Fisheries.

Participant 4: Yes, combatting crime is a joint effort.

Participant 5: Every official should be trained in policing Customs and Immigration duties.

Participant 6: Security officials at facilities have a role to play. Border police or police are far more intrusive in their approach to maritime policing, so sharing of ideas may compromise the objective of securing Ports of Entry. Trust.

Participant 7: Different field of expertise.

Participant 8: No maritime security guards are as previously stated. [They] are looking at a specific function: safety and security of that facility. The focus is not that intrusive as police official.

Participant 9: To have a wider understanding with different entities that service this port in relation to security. To acquire knowledge for a common goal.

Participant 10: To understand their functions and responsibilities for the sake of information flow.

Interpretation

With regards to the joint-training of maritime security officials, a majority of participants agreed with joint training of all maritime security officials. According to a participant, joint training improves work performance and gives insights into the functions performed by other stakeholders, especially Customs and Immigration functions. Another participant sees joint inter-agency training as a platform to acquire knowledge for a common goal, while one added that joint training enhances integration to formulate policies, mandates and information sharing. On the other hand, two participants did not support the joint training of maritime security officials. These participants said that joint training with other role players, such as security guards, will expose and compromise their operations; they said security guard roles are not as intrusive as the functions performed by SAPS officials.

From the feedback received above, it is evident that the joint training of maritime security officials is a challenge. Maritime Ports of Entry comprise numerous stakeholders' departments with their unique training, legislation and methods of work. This implies that using a single command and sharing responsibilities is also difficult. Manig (2019:52) further reveals that no effort is being made on increasing the government's ability to work together or for joint exercises being implemented in the South African maritime environment. Joint training is crucial as it will enable stakeholders to be more vigilant, especially in vulnerable port areas. Furthermore, the training of all personnel together to deal with unforeseen situations, potential crime issues, threat deterrence and avoidance reduces misunderstanding and miscommunication among role-players.

4.3.1.27 How can the role and responsibilities of maritime security officials be improved to be more effective? (see Annexure I question 27)

Conceptual analysis of how the role and responsibilities of maritime security officials should be improved to be more effective:

Participant 1: Intelligence on smuggling/crime threats. Training. Equipment. Role-players working together on a professional basis.

Participant 2: Unit should be trained to perform in line with international standards. Technology should be upgraded regularly.

Participant 3: To join operation with immigration and customs.

Participant 4: More maritime related training courses.

Participant 5: Every official should be trained in policing Customs and Immigration duties.

Participant 6: Containerised cargo movements/policing needs to be enhanced much more; dedicated team working at this with a buy-in for Transnet and Customs who help the manifest.

Participant 7: Equipment to be upgraded for longer vessel patrols at sea.

Participant 8: Take the expertise of staff and allocate to that specific function, e.g., coastal patrol and boating crews. These members must be highly trained and skilled to work in this field. Have these members to possibly crew on ships; see how the shipping industry works. Once you have been in this position, e.g. crew member, you will know the loop holes and thus will be in a better position to police it.

Participant 9: More personnel. Training in more technology aspects and equipment. Free access to information from all security entities in the maritime industry.

Participant 10: Process and procedures of import and export of goods need to be slightly changed. Burdensome transportation rules. Weak or lack of regulation that provide ways to proceed with corruption.

Interpretation

With regard to improving the roles and responsibilities of maritime security officials, a majority of participants stressed upgrading personnel, technology and training courses. Some participants believe that the role of maritime security officials is fulfilled when there is an integration among maritime role-players such as SAPS, Immigration, Customs and Transnet officials. One participant said that maritime security officials' roles should be more in line with maritime international standards. Other participants suggested improving the processes and procedures for imports and exports as well as strengthening regulations for the prosecution of corrupt officials.

The participants understand that maritime security officials have a variety of responsibilities to protect the people, ships and ports from potential criminal intruders. A majority of participants are concerned about the lack of personnel and advanced equipment to counter dangerous and illegal movements of goods. This can result in people entering the country without being thoroughly screened. It has earlier been discovered that there is a lack of coordination and information sharing among maritime stakeholders in South Africa. According to Manig (2017:37), the country's historical politics have made collaboration difficult as departments fight for control, domination, and status. A culture of silos developed, making it impossible for government departments to collaborate on a common goal. The above responses revealed that the role and responsibility of maritime security officials will not be effective unless proper training, resources and policies are in place to address maritime crime such as corruption, terrorism, smuggling, stowaways, and piracy.

SECTION D: SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

4.3.1.28 What is your understanding of the concept "Security Measures" at Maritime Ports of Entry in South Africa? (see Annexure I question 28)

Conceptual analysis of security measures at maritime security:

Participant 1: Placing legal frameworks in place/policies Act and personnel availability with knowledge and equipment, intelligence and interworking relationships with all role-players.

Participant 2: Restrictions on easy access. Access control into facilities. Secure fencing/egress and security.

Participant 3: Refers to the steps taken to prevent or minimise criminal acts e.g. terrorism and sabotage.

Participant 4: Its level of security for foreigners and South African port users to gain entry to the port and these measures must improve constantly.

Participant 5: There are security measures that are put in place by legal provisions in terms of law and SAMSA, where each department engages operationally in order to create a safe and secure environment to prevent the illegal movement of persons and goods across our sea borders which also boosts our economy.

Participant 6: These are security standards or barriers put into place to minimise the risk of potential success of a smuggler or criminal mind. This also takes the form of permit system, fencing, lighting, patrols and booms, etc.

Participant 7: Ensure proper control and management of port, regulator and control of navigation within the approaches to ports and that of safety and security and goods order in ports and protection of the environment.

Participant 8: The essential components of port security measures and procedures are landside operations and marine patrols in harbour, anchorage and waterways of ports to control access to cargo of passengers while in the port.

Participant 9: It is the rules and regulations which are formulated to provide control of movement of goods and goods, commodities with all port of entries.

Participant 10: It is the action taken to prevent criminal proceedings.

Interpretation

The purpose of this question was to discover the meaning of security measures at Maritime Ports of Entry. A majority of participants see security measures as security policies, legal frameworks and procedures governing the Maritime Ports of Entry. The same participants added that security measures require the availability of trained personnel, adequate equipment, intelligence and inter-agency working relationships to be effective. Other participants said security measures are mechanisms the country implemented to guarantee compliance with port rules and regulations to manage the safety and security of maritime transportation. Others view security measures as a standard used for countering the risk of a smuggler or criminal mind. The same participant suggests that security measures should include the use of permit systems, fencing, lighting, patrols, and booms.

All of the above responses show that security measures mean that the maritime industry has proper human and technological resources to detect or prevent crimes in the port. Security measures are part of strategies that are meant for commanding, regulating, communicating, and exchanging intelligence to maintain compliance with international standards. Security measures can also be enhanced by employing security officers who are well trained to operate and monitor the available electronic tools.

4.3.1.29 What security controls are used at Maritime Ports of Entry? (see Annexure I question 29)

Conceptual analysis of security control:

- Immigration controls;
- Customs controls;
- Border safe guarding and surveillance;

- Inspections of goods, animals and human; and
- Border policing

Interpretation

Participants were given a list of security control measures that are used to combat crime at Maritime Ports of Entry. The question had five variables to select from, therefore participants were free to choose from many options. Nine participants indicated Customs controls, inspection of goods, animals and humans as well as border policing as the most common security control measures they use. Eight participants mentioned immigration controls. Five participants mentioned border safeguarding and surveillance.

From the responses stated above, it can be established that most participants saw security control as a collaborative effort involving many departments with similar and sometimes overlapping tasks. These security controls assist personnel to work effectively within protected areas ensuring that people and goods go through the right channels. According to one participant, customs officials inspect the cargo to confirm that the item indicated in the clearing documents is the actual content of the container, while SAPS officers are accountable for checking containers and ships for smuggled goods and contraband. Most participants complained that the access controls at Durban and Cape Town are compromised because of the lack of access control systems, such as x-ray scanners and biometrics. Some participants suspected that manipulation of the systems take place when organised criminals pay bribes to corrupt maritime security officials during the examination of goods and documentation. This is possible since Durban and Cape Town are South Africa's two main ports, implying that narcotics and contraband are constantly trafficked into these ports via containers and ships.

4.3.1.30 Describe the measures that are available for the safety and security of maritime contractors and companies operating in the coastal areas (see Annexure I question 30)

Conceptual analysis of measures available for the safety and security of maritime contractors and companies operating in the coastal areas:

- Automatic Identification System (AIS);
- Identification and Tracking of Ships (ITS);
- Ship Security Alarm System (SSAS);
- Vessel Traffic System (VTS);
- Long-Range Identification and Tracking of ships (LRIT); and
- International Ship and Port Facility Security (ISPS) Code

Interpretation

Participants were given a list of measures available for the safety and security of maritime contractors and companies operating in the coastal areas. The question had six variables to select from, whereby participants were free to choose from many options. In answering this question, eight participants indicated Vessel Traffic Systems (VTS), followed by seven participants who noted Automatic Identification Systems (AIS), Identification and Tracking of Ships (ITS) and International Ship and Port Facility Security (ISPS) Code compliant. Six participants mentioned Long Range Identification and Tracking of Ships (LRIT) and Ship Security Alarm System (SSAS).

These responses show that the Port of Durban and Cape Town made efforts to have various safety and security measures aimed at protecting maritime contractors and companies operating in the coastal areas. These systems are incorporated by International Maritime Organisation (IMO) as part of the ISPS Code legal requirement to monitor their territorial waters and the vessels of interest. The participants said that the AIS, SSAS, LRIT and VTS systems assist in monitoring the in-transit freight. Manig (2017:30) maintains that the IMO requires all eligible cargo and passenger vessels to always have an operational AIS when they are underway or on board to track their position. The AIS is a navigational and surveillance technology that provides insights

about the vessels, goods and Maritime Ports for maritime contractors and companies operating in a coastal area in case of threats and incidents.

Manig (2017:38) also highlights that the South African Maritime Safety Authority (SAMSA) has an active 24-hour search and rescue centre in Cape Town called Maritime Rescue Coordination Centre (MRCC). The centre is responsible for coordinating information with other coastal countries to curb piracy and armed robberies that pose risks on seas.

4.3.1.30.1 Effectiveness of the measures to instil safety and security

This was a follow-up question with yes or no answer where participants were asked to determine whether measures mentioned in question 30 provide safety and security for maritime contractors and companies operating in a coastal area **(see Annexure I question 30.1)**.

Interpretation

In answering this question, the majority of the participants said that the available measures are not effective; three participants said the available measures were effective. There was only one participant who indicated “not sure”, and one participant who did not answer the question.

According to the responses above, the majority of participants believe that the existing security methods are unsuccessful in safeguarding the maritime contractors and companies against piracy, armed robberies and other criminal activities taking place in the coastal areas. Despite the fact that South Africa possesses a sophisticated coastal-based radar, Walker and Reva (2020:14) claim that the country's ability to detect vessels at sea is constrained by a variety of reasons. The security gaps around South Africa's coastlines, where effective terrestrial AIS reception was not possible, demonstrate that vessels of interest cannot be fully monitored when they are within the Exclusive Economic Zone (EEZ). The participants agreed that South Africa's present monitoring capabilities should be improved by adding analysis that allows for a more selective digest of warnings, particularly in outdoor locations.

According to Pichon and Pietsch (2019:1), maritime contractors and shipping

companies operating in a coastal area are at risk of being robbed, murdered, attacked and kidnapped by piracy and armed robbery targeting the goods they are delivering. Manig (2017:33) said that South Africa's existing surveillance system, which includes satellite, radar and AIS, is lacking since the system's coverage of the mainland maritime domain as well as sea air patrolling of the coastal areas is limited. Furthermore, system operators are skilled at manipulating systems to get the desired outcomes. Because of this limitation, serious crimes and major incidents might go undiscovered if they occur when the system is being manipulated.

The majority of participants believe that the ineffectiveness of security measures in coastal regions is due to a lack of close cooperation amongst coastal nations to implement the necessary steps. The participants also said that South African maritime stakeholders are not involved in collaboration relationships, either globally or regionally, for preventing and mitigating transnational maritime security crimes and incidents.

Piracy and armed robberies are increasing on the high seas and oceans, owing to a lack of awareness, experience and training on maritime international requirements and standards among South African shipping companies. The weak criminal justice systems in South Africa that fail to punish and prosecute perpetrators, allows cross-border criminals to bring large numbers of unauthorised goods and contraband into the country.

4.3.1.31 Are the current security measures effective or not in providing access control? (see Annexure I question 31).

Interpretation

Participants were asked to determine whether existing security measures were effective in providing access control in a yes or no question. Eight of the participants replied no, the present security measures are ineffective, while the remaining two said yes, the existing security measures are effective.

Most of the participants claimed that the current security measures in improving access control were not as effective as they wanted them to be. However, some of the

participants indicated that the existing measures at access control were effective. The majority of the responses received give an indication that existing security measures and systems must be re-evaluated to ensure access control security. The participants said that access control is the responsibility of TNPA Security and Compliance division who mandated security measures to manage all access control points.

The most mentioned cause of security ineffectiveness was that the Maritime Ports of Entry have a limited number of security officers to man the entrance and exit points. This was supported by participant 8 (question 12.1): who said *"government resources/personnel in some departments are minimum"*. The shortage of personnel at Maritime Ports of Entry compromises the security at access control. Some participants mentioned the lack of control checks and equipment to scan and inspect people, goods, containers and vehicles entering and leaving the port. This was supported by participant 7 (question 12.1): who said, *"Searching and inspection equipment are needed … more scanners are needed to scan containers entering and leaving the port".* While participant 9 (question 12.1): said that there is *"ineffective scanning equipment to control the access of people within the port"*. A lack of countermeasures is another factor contributing to ineffectiveness of the access control measures. It is clear that maritime security officials at Durban and Cape Town Maritime Ports of Entry are expected to prevent maritime security risks with low levels of capacity and resources.

Participants said that the security officers at entrance and exit points lack proper training on different aspects relevant to their duties such as identifying counterfeit goods and other contrabands passing through the Maritime Ports of Entry. This was supported by participant 10 (question 25) who said maritime security officials lack knowledge on *"reading of documents and counterfeit identification"*. Participant 6, (question 16) also said that *"security personal at normal facilities or business units are not trained in maritime security; they are not too familiar with ports, how they operate, what to look out for, crew and cargo; what risk they bear".* Participant 3, (question 22) mentioned that "*searches are conducted by security officials who are not well trained".* This is believable because theft, trafficking, smuggling of drugs, dangerous weapons and other illicit activities are conducted by unauthorised personnel who are able to enter the port through unauthorised access.

4.3.1.31.1 The participants were asked to describe the security measures they suggest to improve the current system? (see Annexure I question 31.1)

Conceptual analysis of security measures suggested to improve the current system:

Participant 1: A port must be totally enclosed, no public roads running through it; it must only be accessed by means of permits at proper secured manned access/egress points.

Participant 2: Stricter biometric systems; current access permit system is non-existent. Customs and Immigration officers should be deployed at every access point. X-ray searches should be used at every point of access.

Participant 3: Did not answer.

Participant 4: In our port, we are missing some crucial measures, for example, there must be profiling and an Investigation Unit for Maritime related cases. If we want to stop contraband from going out and coming into our ports, collaboration with different departments, Department of Environment Forest and Fisheries (DEFF), Customs or South African Revenue Services (SARS), Department of Home Affairs (DHA) is crucial.

Participant 5: Due to the infrastructure and design of the port, in my own opinion, the port needs to be re-designed since much of the cargo is transported by road and not rail. Further, the port must not be accessible by the public except by role-players only.

Participant 6: Better physical security at facilities; cameras; booms; fencing; lighting; less movement of person in facilities; 8-hour work system of security; 12 hours is too long become fatigued; better control measure on who goes on board the vessels; better monitoring of crew changers and luggage of crew; better monitoring of ship suppliers.

Participant 7: Access control security officers need more training.

Participant 8: Port infrastructure in terms of perimeter fencing is not maintained and secured. Cameras and early detection warning systems are not in place or functional.

All facilities within the port, especially those ISPS Code accredited facilities, should be managed, controlled and have standards like the National Key Point facilities in the Port.

Participant 9: Did not answer.

Participant 10: As the vessels are being stopped or parked outside for inspections and others. Authorities are getting a chance to extort money or they take food from the vessel. If the master of a ship is not paying, they will not grant him entrance with the master.

Interpretation

This question was intended to determine security measures to improve the current system. In responding to this question, a few participants mentioned improving security control systems to monitor, restrict or control access at the Port of Entry. Other participants added security control systems such as CCTV cameras, booms, perimeter fencing, and security lighting. One participant advised redesigning the port infrastructure for efficient movement of goods. Another participant identified the installation of biometrics and x-ray searches at every access control point to recognise false permits and contraband, while other participants suggested the training of maritime security officials who control the entrance and exit points. There was one participant who recommended reducing the hours of work shift of maritime security officials from a 12-hour shift to an 8-hour shift, while two participants did not answer the question.

With increasing threats at Maritime Ports of Entry, access control can be improved by the implementation of electronic equipment, such as facial recognition, fingerprint scanning systems, night vision cameras, x-ray scanners, and biometric technologies, to verify and deter unlawful acts. Installation of stricter biometric systems reduces the unlawful movement of people and cargo at the port. The participants suggest that the Port of Entry must deploy Customs and Immigration officials at the control points to assist with the duties of imported and exported goods. Moodley (2014:52) also indicates that South African border posts need advanced technical tools and basic equipment such as document scanners, security patrol vehicles, binoculars, radars,

radios and devices for night vision. According to Govender (2018:79), implementing adequate access control measures aids the organisation in detecting criminals, delaying offenders, and allowing marine security officials to respond quickly. Furthermore, long work hours and irregular shifts may be stressful physically increasing the risk of sleeping on duty and a lack of concentration.

4.3.2 Observation data analysis

As a result of Covid-19 pandemic restrictions, the researcher was not allowed access to the Maritime Ports of Entry to conduct on-site observations. Purposive interviews were conducted online with two participants from TNPA Security and Compliance Division using telephonic and email at Durban and Cape Town Maritime Ports of Entry. Observation analysis was conducted to assess the current Physical Protection Systems (PPS) in terms of threats, vulnerabilities and security risks focusing on the outer and inner layers of security at Durban and Cape Town Maritime Ports of Entry. The participants informed the researcher that they observed that the Ports of Durban and Cape Town have uniform security measures in place to counter threats, vulnerabilities and security risks.

4.3.2.1 Security policies and procedures

The question was intended to check whether the Port of Durban and Cape Town has a security system in place that includes rules and procedures to govern the port. From the responses received below, the researcher discovered that security policies are in place that serve as Standard Operating Procedures for security and access for most of the security measures being assessed at Durban and Cape Town Maritime Ports of Entry.

The participant from Durban indicated that the policies at Durban include a Code of Conduct, Contract Management, Master Agreement and Service Level Agreement. The participant from Cape Town mentioned that their policies include Access Control, PSIRA Code of Conduct, TNPA Security Policy and TNPA Permit Procedure. The Cape Town participant also said that their Port of Entry policies have been established in line with the Service Level Agreement signed between Cape Town TNPA and the contracted security service provider.

Other key issues highlighted by the participant from Cape Town is that the policies are well regulated by the Maritime Port Security Plan and supported by the Ports Act 12 of 2005 (South Africa, 2005).

Interpretation

The all-inclusive policies serve as a security guideline that maritime authorities commit to implement and maintain at all times to prevent unauthorised access, smuggling and tampering of goods. Given an existing access control strategy, the security officers deployed at Durban and Cape Town Maritime Ports of Entry are able to protect port restricted areas through the combination of procedures and technical means.

4.3.2.2 Access control

Access control is a collection of requirements that define how access or egress control points at Ports of Entry are controlled to prevent unauthorised entrance. From the information provided by the participants, Security and Compliance Divisions at Durban and Cape Town provide security directions to the security officials as to how egress and access points should be properly manned for the security of the Maritime Ports of Entry. The participant from Durban mentioned that security officers that work 12-hour shifts regulate access at the main points of entrance and exit. There are 157 officials assigned to each of these entry and exit points for the day shift, 153 for the night shift, and 22 TNPA security officials including supervisors. While the participant from Cape Town indicated that the PSIRA security officers and TNPA supervisors operate on a 12-hour shift cycle, are in charge of access control at the key entry and exit points, and that access control in Cape Town is mandated by the procedure of the ISPS Code, which include maritime security levels 1, 2 and 3 (see attached ISPS Code as Annexure S).

Other issues highlighted by both participants are the use of security control systems to manage authorised access and prevent unwanted people in the port. The participant from Cape Town indicated that permit/access cards, including biometric data, identity badges/cards, and TNPA Identification cards are required from everyone accessing the port premises, including visitors, contractors, port service providers as well as stevedores and personnel. The participant from Durban said that biometric identity

verification systems are available at the Port of Durban and mostly used by TNPA employees when clocking for duty. The participant from Cape Town also said that their port access control has barriers which are controlled by boom gates, turnstiles, automated security gates and floodlights to strengthen access control into the Port of Cape Town, while the Durban participant cited the use of boom gates and cones as additional access control barriers.

Interpretation

From the responses above, it is evident that Durban and Cape Town Maritime Ports of Entry have security measures to secure the access and egress of the port. Having the right security system in place assists the Maritime Ports of Entry to protect their assets from criminals with minimum disruption. Durban and Cape Town Maritime Ports of Entry achieve access control by using a combination of security personnel, mechanical means and technical access at entry and exit points. Different levels of security at entry points prevent unauthorised access into the ports' restricted areas.

Physical security officers represent the human element of the security measures used at Maritime Ports of Entry. Positioning security personnel at entry and exist points with adequate knowledge to verify identification and documentation of all accesses is essential. Barriers are an important way to control access to only authorised people, goods and vehicles. This in turn can reduce the threat of smuggling, illegal entry, theft and potential terrorist attacks in the Ports of Entry.

4.3.2.3 Security lighting

With regard to security lighting, the participant from Durban said that the Port of Durban has security lighting operating on a 24-hours basis. The only shortcoming mentioned by this participant is the lack of security lighting at container security, but this participant defended this statement by saying that security lighting at container depots or berths where containers are offloaded and loaded is sufficient, hence they are able to carry on with those operations at night and that no accidents have occurred thus far. The participant from Cape Town only mentioned that there is floodlight security lighting at the Port of Cape Town. Floodlights are high-intensity, broad-beamed artificial lights that are powerful enough to illuminate outside perimeters. Both

Durban and Cape Town participants mentioned that the security lighting at their ports do not have motion sensors.

Interpretation

The responses receive above shows that the both Durban and Cape Town Maritime Ports of Entry are equipped with security lighting but more needs to be done. The lack of security lighting at container security poses threats to containers being used by criminals to smuggle drugs and counterfeit goods especially at night. A lack of motion detector lights is a problem since the port facilities require conventional security lights with motion detectors to be effectively safeguarded. Security lighting can enhance the physical security of the Port of Entry. It can also help security officers perform patrols, illuminate areas with CCTV cameras, deter unauthorised entry and provide visitors and personnel with safety lighting at parking and storage areas.

4.3.2.4 Closed circuit television

In terms of Closed Circuit Television (CCTV) cameras, the participant from Cape Town indicated that the entire Port of Cape Town is covered by CCTV cameras, while the participant from Durban mentioned that there are CCTV cameras installed around the port to monitor the entrances and exits; there are 332 cameras, 208 are functional while 124 are offline. The participant from Durban also added that their cameras have Pan, Tilt and Zoom (PTZ) and 145 High Density, PTZ. These cameras record quality images (allowing for number plates or facial recognition of people). The cameras at the Port of Durban are not tamper proof since their power connection is easily accessible and the cameras are connected to the Uninterruptible Power Supply (UPS) back up power battery and have backup generators which can ensure security when the power supply is disturbed.

Interpretation

It was established from the responses above that both ports of Durban and Cape Town are monitored by CCTV cameras. The 124 cameras that are offline indicates that Durban is not fully protected from intrusion. Installing CCTV cameras in every area of the port is crucial to prevent unauthorised access. Furthermore, CCTV cameras at the

port are a crime deterrent; they can provide visual recordings for a number of days for investigation purposes. Elago (2019:83) expressed that the technological components, such as security alarms systems, CCTV cameras, as well as electronic key cards, are the best access control systems to aid maritime security officials to fight crimes at Ports of Entry.

4.3.2.5 Parking areas

In terms of parking areas, the participant from Cape Town indicated that the Port of Cape Town has parking areas within the port and that each facility has a demarcated parking area for staff, visitors and port users; these parking areas are monitored by CCTV cameras. The participant from Durban said that there is parking space at the Port of Durban which is monitored by security personnel and CCTV cameras and that TNPA policy requires all drivers to park their cars in reverse to allow quick driving out of the building in emergency situations.

Moodley (2014:70) said that Durban Port of Entry used to have four defined parking areas that accommodated both workers and visitors, but these parking areas were not monitored by security officers or CCTV cameras, and that some of these parking lots were near storage facilities, which posed a security risk.

Interpretation

The responses above show that the parking areas at Durban and Cape Town have shortcomings as they do not have enough physical and electronic surveillance to monitor security risks at all time. The parking areas closer to storage facilities need to be adequately monitored by both security personnel and CCTV surveillance to prevent criminals and trespassers hiding in parking areas to steal goods in a storage area.

4.3.2.6 Perimeter fencing

Regarding perimeter fencing, the participant from Durban said that the Port of Durban has a concrete palisade perimeter fence while the participant from Cape Town indicated that the perimeter fencing at the Port of Cape Town is secured by 2.5-metre palisade fencing. The Durban participant also complained that there are no security alarms installed along the Port of Durban perimeter fence.

Interpretation

The responses above show that the perimeter fence of the Port of Durban is not properly secured by security alarms. A perimeter fence is of little use without security alarm systems to provide both visible and physical deterrence. An unalarmed perimeter fence is a risk to the port perimeter allowing criminals to smuggle unauthorised goods. Perimeter access control is achieved by using a combination of fences and walls, CCTV cameras, motion detectors, alarm systems and manned by guards who are well trained and motivated.

4.3.2.7 Other existing security measures available at Durban and Cape Town Maritime Ports of Entry

Other measures that protect the Maritime Ports of Entry mentioned by both participants include: document registers, security patrols, search systems and vetting of security personnel.

Document register: According to the participant from Cape Town, information register, clamping register, permit register, occurrence book, key register, visitors register, confiscated/expired card registers are used at Cape Town Port of Entry. The participant from Durban said that document register is available at the Security Systems Control Room and the Security sites to record incidents and Security breaches.

Interpretation

Maritime security officials at Durban and Cape Town Maritime Ports of Entry use document registers to record and document all events, such as crime incidents or suspicious behaviour, for recall to the appropriate authorities.

Security patrols: The participant from Cape Town said that TNPA security officers conduct security patrols around the Port of Cape Town using vehicles, by foot, with quad bikes and dog patrols to keep the people and assets safe and secured. This participant added that security officers at the Port of Cape Town conduct night patrols to check for windows left open, lights left on in offices and trespassers in the port facility. The participant from Durban said that security patrols at the Port of Durban are

performed by security guards on at intervals, while dog patrols are carried out during the night to minimise trespassers.

Interpretation

Random security patrols by security officers on foot, in cars, or using dogs serve to deter and prevent criminal activity. Vandalism, theft, and trespassing can happen at any time of day, therefore patrolling the whole port infrastructure, including delivery, storage, and parking areas, during normal office hours and after hours is critical.

Search system: The participant from Cape Town said that the port uses hand held scanners and walk-through metal detectors at access control points to conduct searches, while the participant from Durban mentioned that the Port of Durban has no system in place to detect explosives as well as the devices to check sealed and tampered containers except for the stowaway search dogs that are used inside the vessel before departure.

Interpretation

The responses above show that the Port of Durban lacks additional search tools to strengthen the physical security search of people, cargos, trucks or passenger vehicles for the presence of contraband. Search tools used by maritime security officials detects and prevents the flow of illegal imports and people through the Port of Entry, while facilitating and safeguarding lawful trade and travel.

Vetting of security personnel: Regarding the vetting of security personnel, the participant from Durban said that TNPA security division does not employ personnel without conducting vetting which is done again when security personnel are promoted in the same division. Re-vetting is also conducted to determine a person's security competencies. The participant from Cape Town indicated that screening and vetting of personnel is done periodically.

Interpretation

The responses above show that Durban and Cape Town Maritime Ports of Entry conduct pre-employment and post-employment screenings before employing their

security personnel to eliminate the less appropriate employees. Durban and Cape Town Maritime Ports of Entry have minimum security measures in place to secure their infrastructures. There might, however, be more that could be done. The absence of motion detection is remarkable. This is a security system that will respond in cases of unauthorised entry or trespass. None of the participants mentioned the use of detection analysis to find explosives at Durban and Cape Town Maritime Ports of Entry. Information gathered through explosive analysis might also be utilised to detect explosive-related incidents.

4.3.3 Documentary study analysis of secondary data

As a result of Covid-19 pandemic restrictions, the researcher was not allowed access to the Maritime Ports of Entry to conduct a documentary study. The researcher had therefore to use secondary data from four articles and one dissertation (see paragraph 2.6.6 above) to conduct documentary study analysis. Documentary study analysis was conducted by carefully perusing and analysing selected articles and dissertation of cases of illegal movements and smuggling crimes with related information to the documentary study checklist.

This section offers an analysis and interpretation of all secondary data analysis outcomes.

Day of the week that contraband smuggling took place

Moodley (2014:64) indicated that the majority of crimes occurred on Wednesdays, Fridays, and Saturdays. According to Ekwall and Lantz (2018:15), cargo theft at Maritime Ports of Entry is more frequent on weekdays than weekends. Justus, Ceccato, Moreira, and Kahn (2018:320) agree that most of cargo theft happens on Tuesdays, Wednesdays and Thursdays, with the least crime occurring on Mondays.

Interpretation

According to the responses given above, the number of accessible targets determines how much crime may be committed on specific days of the week. Cargo theft, illegal movements, smuggling and other cross border crimes are committed by criminals who have the ability to threaten or mislead. Criminals prefer to commit these crimes on

weekdays when there is the potential to pay corrupt maritime security officials.

Time of illegal movements and smuggling of goods incidents

A majority of illegal movements and smuggling crimes take place during the night when there is little chance of detection (United Nations Office on Drugs and Crime, 2011:31). According to Moodley (2014:65), the majority of crimes at Durban Maritime Ports of Entry took place between 12h00 and 17h00 and 06h00 and 11h00. Justus et al (2018:319) also support the above statement by adding that most cargo thefts occur between 06h00 and 16h00, which coincides with the operating hours of most retail and service operations.

Interpretation

The information above shows that most crimes take place during the night to avoid detection and that other crimes were committed during working hours of 06h00-18h00 when the enablers are available. As mentioned above, the preferred time of 06h00 to 18h00 may be because perpetrators perceived that there were enablers to assist them to commit their crimes.

Modus operandi used to commit crimes at Maritime Ports of Entry

The question was asked to establish methods used by criminals to commit crimes at Maritime Ports of Entry. According to Organized Crime Research Brief (2018:19), the most popular methods used by criminals are contraband among lawfully imported products, through the use of false shipping documents and internal collusions using corrupted law enforcement officials (Organized Crime Research Brief, 2018:19).

Criminals also target Maritime Ports of Entry where there are fewer personnel, or where there are no advanced techniques or trained personnel to verify documentation. Containers and trucks are the most cost-effective services available for poor migrants who use it to hide at their own risk (United Nations Office on Drugs and Crime, 2011:20).

Interpretation

Criminals employ different methods to commit crimes at Maritime Ports of Entry. The

study revealed that most of the perpetrators are aware of the security weaknesses at the Maritime Ports of Entry. The corruption at Maritime Ports of Entry is actively promoted by people in government departments and companies who are involved in the administration of port security and functions. While cross-border crimes take place at Maritime Ports of Entry due to a lack of effective security policies, insufficient maritime security officials, resources, and deteriorating port infrastructure make smuggling and unauthorised entry possible. Criminal syndicates are often adaptable and well-informed, and modify their routes and techniques to counter legitimate measures. They may have well-resourced intelligence networks and the ability to adapt and implement new methods.

4.4 Conclusion

This chapter discussed participant biographical data; threats, vulnerabilities, and security risks faced by Maritime Ports of Entry; the roles and responsibilities of maritime security officials, and the security measures used at Maritime Ports of Entry.

The researcher discussed the information obtained from the on-line telephonic and email interviews with participants from Durban and Cape Town Maritime Ports of Entry. This was followed by the information obtained from purposive interviews with two TNPA officials from Security and Compliance Division who answered questions from the observation checklist. Lastly, information was obtained from secondary data using four articles and one dissertation (see paragraph 2.6.6 above) to complete the documentary study checklist. The research data were transcribed, analysed and interpreted by the researcher. The research data were thematically analysed. All conclusions generated from the data analysis will be discussed as findings and recommendations in Chapter 5.

CHAPTER 5: RESEARCH FINDINGS AND RECOMMENDATIONS

5.1 Introduction

This study was conducted because Maritime Ports of Entry are faced with criminals who break the laws intended to protect the ports. The study was aimed at assessing the security measures; establishing the roles and responsibilities of maritime security officials and to improve security at Maritime Ports of Entry in Durban and Cape Town, South Africa. The data for this study were collected through interviews, observations and documentary study. The data were analysed, interpreted and presented in Chapter 4. The purpose of this chapter is to discuss the research findings and to make recommendations to improve security measures at the Ports of Entry.

5.2 Research overview

Maritime ports are complex and varied entities. They transport cargo and people from the sea to the land, connect with and service maritime vessels by offering a harbour, deliveries, repairs and, most importantly, receive large capacity ships with cargo. Threats, vulnerabilities, and security risks to the Maritime Ports have been there for as long as there have been seaports. Crime and criminal activities have long been present at Ports of Entry globally. Over the past decade, the maritime industry has had to deal with escalating threats from terrorist organisations, rebels and militants as their activities have increased.

The event prompted maritime stakeholders in both the public and private spheres to develop more potent security measures to prevent criminals and terrorists from taking advantage of the seaports' weaknesses. Although several aspects of security at Maritime Ports of Entry have been improved by contemporary security measures, other critical threats and vulnerabilities remain. If suitable security protections are not taken to check the identities and permits of persons, ships, and cargo arriving or exiting at the Ports of Entry, criminals may penetrate them.

In this study, the researcher assessed the security measures at Durban and Cape Town Maritime Ports of Entry, to identify the threats, vulnerabilities and security risks; establish the roles and responsibilities of maritime security officials; and to improve

security measures at the Maritime Ports of Entry. The researcher conducted interviews, observations and a documentary study to collect data, analyse the collected data and make findings and recommendations as discussed hereunder.

5.3 Findings

The researcher addressed the following research questions in the study:

What are the threats, vulnerabilities, and security risks confronting Maritime Ports of Entry in Durban and Cape Town?

What are the roles and responsibilities of maritime security officials in ensuring security at the Maritime Ports of Entry in Durban and Cape Town?

Which security measures need to be improved at the Durban and Cape Town Maritime Ports of Entry?

5.3.1 Research findings

The **first research question** was to establish the type of threats, vulnerabilities and security risks confronting Maritime Ports of Entry in Durban and Cape Town. The purpose of this question was for the researcher to ascertain the current state of threats, vulnerabilities and security risks at Maritime Ports of Entry that could be exploited by criminals.

In respect of the first research question, it was found that:

Maritime security threats are dangerous or harmful activities that can be carried out by terrorists and criminal groups or by port personnel. Smuggling, trespassers, cargo theft, stowaways, and counterfeit goods are among the most serious threats facing Durban and Cape Town Maritime Ports of Entry. Because of the amount of money linked with cargo containers, there is an external risk of organised criminals where maritime personnel may release containers falsely for money.

Containers are used to transport drugs and narcotics, because it is challenging to detect drugs concealed inside containers. Durban and Cape Town Ports of Entry scan fewer than five percent of imported containers. These findings suggest that a

significant amount of contraband is moving through supply chains, implying that the majority of narcotics pass through container terminals unnoticed.

Cyber-attacks on ships and ports involved in the maritime transportation industry have increased at an alarming rate. Cyber-attacks have been known to harm container ports' reputations, causing customers to shift their business elsewhere.

Poorly trained security personnel are another security concern that must be addressed. It was found that a large majority of participants only received basic training at their individual institutions and had no specialised maritime knowledge. This demonstrates that there are issues in this aspect and that a majority of participants were not properly trained in assessing threats, vulnerabilities and security risks.

The most vulnerable areas at the Port of Durban and Cape Town include the perimeter fence, access control points, as well as an overlooked port size layout.

Unauthorised personnel with easy access to Ports of Entry exposes them to high risk areas such as receiving and distributing goods which makes it easy for the smuggling of drugs, contraband and counterfeit goods.

Containers are vulnerable to tampering and theft by criminals because of inadequate monitoring technologies, such as seals and tracking devices, as well as cameras to monitor the port environment.

Poor and insufficient security measures at the Ports of Durban and Cape Town provided inadequate security protection against security risks. The absence of access control, security lighting, and a weak perimeter fence, as well as insufficient personnel, such as security officers, SAPS members, customs and immigration officials, and a maritime security strategy to oversee Maritime Ports of Entry security, are major risks. Other security issues include inadequate technological resources, such as CCTV systems designed to cover the whole port area, more especially on the outside and inner layers of security.

A lack of proper monitoring, control and surveillance measures exposes South Africa's Maritime Ports of Entry to risks of illegal crossings and smuggling. Another security risk is corruption by maritime security officials who assist criminals in gaining entry to

the port. Inadequate road maintenance, which makes the sea a popular destination for international trade, is the root cause of human, drug, and illegal weapon trafficking through Maritime Ports of Entry.

The **second research question** was aimed at identifying the roles and responsibilities of maritime security officials in ensuring security at the Maritime Ports of Entry in Durban and Cape Town. The research sought to establish where the roles and responsibilities of maritime security officials should be improved to enable them to protect and secure Maritime Ports of Entry.

In respect of the second research question, it was found that:

The roles and responsibilities of maritime security officials involve overseeing security by means of controlling access control, patrolling, guarding, inspections of goods/permit, conducting surveillance and rummage on vessels.

Transnet National Ports Authority (TNPA) is primarily responsible for asset and perimeter security at Durban and Cape Town Maritime Ports of Entry. It is supplemented by SAPS, SARS Customs, and DHA Immigration that are in charge of inspecting goods and people entering and exiting the port. These entities work in silos, resulting in a lack of communication, cooperation, and coordination when dealing with maritime security challenges.

Another issue discovered is the lack of a clear maritime strategy or policy for regulating the functions of maritime role-players. This leads to the duplication of responsibilities among maritime role-players. Command lines between role players are also an issue, causing role players to be unsure of the broader hierarchical structure, that is, who reports to whom. As a result of this, information is bypassing critical layers of management. There remains an urgent need for a single overarching role player involved in maritime security.

The personnel deployed at Maritime Ports of Entry do not have the resources needed to assist with the performance of all maritime security duties. A shortage of personnel causes Maritime Ports of Entry to operate with a very low capacity and to provide poor quality services. Maritime security officials have insufficient knowledge and skills to

identify security related threats. Training is not given to security officials in risk profiling, collecting sources, methodologies, or procedures.

The **third research question** was aimed at identifying the security measures that need to be improved at Durban and Cape Town Maritime Ports of Entry. The purpose of this question was for the researcher to identify the trends and common problems associated with the security measures that can be modified to increase the efficacy of security countermeasures or controls.

In respect of the third research question, it was found that:

There are no known methods that can totally prevent threats from occurring at Maritime Ports of Entry because maritime threats are unexpected and can arise at any moment; only effective countermeasures exist to lessen the risk of threats. Countering threats, vulnerabilities, and security risks depends on the amount of physical security in terms of perimeter fences, security lighting, rules and regulations, and access control. To reduce the crime and security risks at Maritime Ports of Entry, access control should be conducted appropriately to eliminate the problem of unauthorised entry, cargo theft, contraband smuggling, and illegal commodities moved through ports.

There is a lack of human and technology resources to deploy around every aspect of the port to reduce illegal activities. The lack of security control systems, x-ray machines, CCTV surveillance cameras, electronic key cards, and alarm systems in every area of the port, combined with understaffing and untrained personnel on maritime security functions, criminal activities, and security risks, impacts the prevention of criminal activities at the ports. This demonstrates the ineffectiveness of the existing measure in addressing the bulk of crimes and other security risks encountered at the Ports of Entry.

Container security methods, such as screening, sealing, and inspection, require upgrading. Maritime personnel scan few imported containers at Durban and Cape Town Maritime Ports of Entry. These findings suggest that a significant amount of contraband is moving through supply networks, implying that the majority of narcotics pass through container terminals unnoticed. Smuggling, trafficking, and stowaway

operations in containers can be reduced by using more technologically advanced scanning equipment.

Some of the accusations levelled against maritime security officials include corruption, accepting bribes, working with criminal syndicates, and stealing.

Findings in respect of observation:

It was found that **f**our official parking areas at Durban Port of Entry were near storage facilities, which posed a security risk. There was a shortage of security lighting at container security, which was frequently vulnerable to theft and container tampering crimes. The security lighting at the ports do not have motion sensors to warn them of any disturbance in the surrounding areas.

Most areas within ports of Durban and Cape Town were not covered by CCTV cameras. Out of 332 cameras installed at the port of Durban, only 208 cameras are functional. The cameras at the port of Durban have 145 High Density Pan, Tilt and Zoom (PTZ) to record quality images (allowing for number plates or facial recognition of people). These cameras are not tamper proof since their power connection is easily accessible, they are connected to the UPS back up power battery and have a backup generator which can ensure security when the power supply gets disturbed.

There are no security alarms on the port's perimeter fence.

Findings in respect of the documentary study:

It was found that

The majority of crimes occurred on weekdays (Fridays and Saturdays). Cargo theft at Maritime Ports of Entry is more frequent on weekdays than weekends but with Mondays being the day of the week with the lowest occurrence of crimes.

The majority of illegal movements and smuggling crimes take place during the night, while the crimes at Durban Maritime Ports of Entry took place between 12h00 and 17h00 and 06h00 and 11h00. The time occurrence of these crimes coincides with the operating hours of most retail and service operations.

The methods used by criminals to commit crimes at Maritime Ports of Entry involve: the use of containers; concealment of illegal goods with a lawful cargo; using fraudulent shipping documents; and internal collusions using corrupt law enforcement officials. Criminals often target ports that lack adequate human and technological resources or where personnel are not trained to identify false documentation. Containers and trucks are the most economical services used by stowaways to and from South Africa; they hide on container ships and trucks at their own risk knowing that they have a small chance of survival.

5.4 Recommendations

Research Question 1: What are the threats, vulnerabilities and security risks confronting Maritime Ports of Entry in Durban and Cape Town?

To prevent maritime threats requires the involvement of local, regional and international stakeholders, comprising not only government but also the maritime industry; the development of resilient, credible, and capable governance; and strong collaboration to synchronise security efforts. Countering maritime threats can also be aided by optimising the use of existing systems; being more vigilant and knowledgeable about the methods used by criminal syndicates; and establishing various forms of communication among all maritime role-players involved in coastal areas to share new information on threats. Tightening the links amongst role-players will enhance operations planning, capacity building, threat assessment, surveillance, and training and monitoring of present and future operations.

To combat cyber-attacks, the government must safeguard the port's valued data, which includes cargo information and employee details. Due diligence should be prioritised at Maritime Ports programmes when securing new businesses, systems or software to reduce threats that undermine or disrupt their essential services. A large amount of resources should go towards raising awareness on cyber risks. Moreover, the maritime industry should establish regulations related to digital risks that include standards, codes and legislation for cyber security that are mandatory to protect Maritime Ports from cyber-threats.

All role-players involved in the maritime domain should get training on search and

seizure laws, crime scene preservation, and evidence collection methods and procedures. The training of maritime security officials will assist them in being more aware of the threats they encounter on a daily basis. Drills, training, exercises, and countermeasures should be conducted regularly to enhance employee awareness and to serve as a deterrent to prospective criminals.

Government should increase capacity personnel for profiling, investigation, inspections, searches, and patrols to ensure that the standard of security is being maintained at the Maritime Ports.

Research Question 2: What are the roles and responsibilities of maritime security officials in ensuring security at the Maritime Ports of Entry in Durban and Cape Town?

Government should implement legislation or develop a maritime strategy to govern the duties of all stakeholders and ensure that they are coordinated under a single authority. The legislation should clearly define who administers the functions to minimise confusion and duplication of efforts and costs. To simplify the flow of information, command and control mechanisms should be developed to connect the systems used by the role-players. This enables real-time communication, which speeds up reaction times.

Governments should improve inter-agency collaboration and information exchange among role-players in the fight against maritime crime. Coordinated efforts at the highest levels, as well as authorised collaboration among staff, on threat issues is recommended. This may include collaborative investigations, continuous information sharing, and identification of criminal syndicates in order to bridge gaps in enforcement and intelligence. Timely information sharing should be greatly improved by effective decision making, and increased incident reaction time at the port. It should be based on correct information that is delivered on time. Better interaction between role-players will result in increased trust and knowledge which will help to reduce misconceptions between role-players.

Furthermore, the government should research training courses and educational methods for improving the performance of maritime security officials based on the

different maritime sectors. An academy should be formed to train the officials on identification and detection of illegal goods, counterfeits, and fraudulent identification. This will equip maritime security officials in terms of knowledge and abilities, with the purpose of professionalising the maritime security industry.

Security personnel should be provided with the resources they need to secure all access/egress control points. This includes enhancing the port infrastructure, adding security lights at entry and exit control points, perimeter fences, container hubs, parking spaces, and storage areas.

Government should make a budgetary commitment to address the lack of resources and equipment. It must recruit experienced personnel for deployment at high-risk areas to improve the current performance of maritime security officials to provide quality services. Money spent on enhancing resources and technology should be viewed as an investment rather than a cost, because the goal is to safeguard people, goods and, ultimately, business continuity. As a result, the aim should be to lessen the threat using available funds.

Research Question 3: Which security measures need to be improved at the Durban and Cape Town Maritime Ports of Entry?

Government should design or revise the security strategy based on identified threats, vulnerabilities and security risks in order to implement the appropriate security risk control measures at Durban and Cape Town Maritime Ports of Entry.

The current perimeter fences, security lighting, security policies and procedures, and access control should be upgraded for deterrent, detection and delaying offenders, and for improved reaction by security personnel.

To control unauthorised access, maritime authorities should adopt the ISPS Code. The port should require maritime workers and visitors to pass background checks and get a biometric identity card to gain unescorted access. Identification cards must be displayed at all times to ensure that only certified personnel have access to high risk areas of the port.

Specialised equipment should be provided at entrance and departure points. The

ports' CCTV surveillance system must be improved to cover all high-risk port locations. The CCTV surveillance systems should be deployed at all entrances, exits, parking spaces, and the surrounding port facilities. The CCTV surveillance systems should be under the constant monitoring of a trained security officer as a deterrent measure.

More container scanners must be purchased to increase the quantity of containers being scanned in order to reduce crimes of smuggling and tampering. Government should improve port and container security by working with foreign governments and companies that export goods and containers to South Africa to assess and mitigate cargo risks before the cargo enters South African ports.

Corruption at Maritime Ports of Entry requires immediate and continuing action. All government actors and private security officers should be educated on the importance of the system's integrity as the primary component for assessing security solutions. The establishment of an internal anti-corruption unit is one solution to the problem. Background checks can also be used to guarantee that current or prospective maritime security employees do not have criminal records. Setting a severe punishment would deter marine security officers from accepting bribes and engaging in illegal activities.

5.5 Recommendations for further research

The findings discussed above uncover potential areas for future research. This study focused on the assessment of security measures at two Maritime Ports of Entry, Durban and Cape Town, South Africa. Since the study was mainly focused on the two Maritime Ports of Entry in South Africa, similar studies could be extended to other Maritime Ports of Entry not covered in this study.

Human factors are a threat to the execution of port security measures. This has not been well researched and requires additional investigation to assess threats and vulnerabilities and to implement security measures at Maritime Ports of Entry. In addition, the researcher recommends more security studies to recognise digital technology for transformation and innovation in the maritime industry. The maritime industry must improve its technological efficiency in order to collect security information, particularly on cyber-attacks.

Further research would also be beneficial for Fusion Centres, which are used by maritime stakeholders and role-players at Maritime Ports of Entry. Due to the complexity of the maritime industry, obtaining information on the perspectives and experiences of local, regional, and international maritime role-players will result in a more global knowledge of the maritime security system and will lead to interactions with other countries.

Lastly, study is needed on the development of maritime capability. These initiatives are still in their infancy in comparison to their more established counterparts on land and in the air, so there is much to gain from a more systematic exchange of experience.

5.6 Conclusion

This chapter shows that there are threats, vulnerabilities and security risks that exist that are linked with criminal acts such as smuggling goods, drugs, stowaways, and contraband through seaports. This is due to security flaws or gaps in protective measures, such as untrained personnel, a shortage of protective security systems for prevention and mitigation activities, a lack of communication and coordination of efforts and resources at Durban and Cape Town Maritime Ports of Entry. The study has made recommendations to help maritime authorities to minimise threats, vulnerabilities, and security risks causing cross-border crimes at Durban and Cape Town Maritime Ports of Entry.

LIST OF REFERENCES

Aamilid, C. 2019. *Threats to container ports and preventative security measures.* Master's Thesis, University of South-Eastern Norway, Notodden, Norway. Available at: https://openarchive.usn.no/usn-xmlui/bitstream/handle/11250/2637935/Master%20Thesis%202019%20Chaiyakrit%20Aamlid.pdf?sequence=1 (accessed on: 1 April 2022).

Aguocha, N.M. 2018. *Stowaways: A threat to maritime security and the curse of shipowners.* Master's dissertation, University of KwaZulu-Natal, Durban. Available at: http://researchspace.ukzn.ac.za/xmlui/bitstream/handle/10413/18406/Aguocha_Nkechi_Miriam_2018.pdf?sequence=1&isAllowed=y (accessed on: 14 August 2020).

Akar, F. 2019. Maritime security challenges in Mediterranean Sea and how NATO respond to them. Available at: https://www.researchgate.net/publication/335820247_HOW_DID_NATO_RESPOND_TO_THE_MARITIME_SECURITY_CHALLENGES_IN_MEDITERRANEAN_SEA (accessed on: 18 August 2020).

Akers, A.L. 1990. Rational choice, deterrence and social learning theory in compare the criminology: The path not taken. *The Journal of Criminal Law and Criminology*, 81:653. Available at: https://www.semanticscholar.org/paper/Rational-Choice%2C-Deterrence%2C-and-Social-Learning-in-Akers/c1761d176999aa371eab269028233ba46d0dafe7 (accessed on: 29 September 2019).

Akinyode, B.F. and Khan, H.T. 2018. Step by step approach for qualitative data analysis. *International Journal of Built Environment and Sustainability*, 5(3):267.

Ali, K. 2014. *Maritime security cooperation in the Gulf of Guinea: Prospects and challenges*. Doctor of Philosophy thesis, Australian National Centre for Ocean Resources and Security. University of Wollongong, Wollongong.

Anagnostakis, D. 2015. *Securing the transatlantic maritime supply chains from*

counterterrorism: EU-U.S. cooperation and the emergence of a transatlantic customs security regime. Available at: https://aura.abdn.ac.uk/bitstream/handle/2164/11204/Securing_the_Transatlantic_Maritime_Supply_Chains_from_Counterterrorism_AM.pdf?sequence=1&isAllowed=y (accessed on: 14 August 2020).

Andritsos, F. 2013. *Port security & access control: A systemic approach.* Available at: DOI:10.1109/IISA.2013.6623728 (accessed on: 16 August 2022).

Argun, U. and Daglar, M. 2016. *Examination of routine activity theory by property crimes*. Available at: https://www.researchgate.net/publication/296477454_Examination_of_Routine_Activities_Theory_by_the_property_crime (accessed on: 22 June 2020).

Arifin, S.R. 2018. Ethical consideration in qualitative study*. International Journal Care of Scholars*, 1(2).

Asiamah, M.A. 2018. *Investigating the issue of maritime domain awareness: The case of Ghana.* Available at: https://commons.wmu.se/cgi/viewcontent.cgi?article=1609&context=all_dissertations (accessed on: 14 August 2020).

Athreya, K.B. 2015. *What is Probability Theory: Resonance?* 20(4):292-310. Available at: https://www.ias.ac.in/article/fulltext/reso/020/04/0292-0310 (accessed on: 30 July 2019).

Australian Customs and Border Protection Service. 2015. *Annual Report 2014-15*. Available at: https://www.homeaffairs.gov.au/reports-and-pubs/Annualreports/acbps-annual-report-2014-15.pdf (accessed on: 17 August 2020).

Bairagi, V. and Munot, M.V. 2019. *Research methodology: A practical and scientific approach.* New York: CRC Press.

Bernstein, P.L. 1996. *Against the gods: The remarkable story of risk.* New York: John Wiley & Sons. Available at:

http://hostel.ufabc.edu.br/~nelson.faustino/Ensino/IPE2016/Livros/Peter%20L.%20BernsteinAgainst%20the%20Gods_%20The%20Remarkable%20Story%20of%20RiskWiley%20(1998)%20(1).pdf (accessed on: 14 November 2019).

Bell, J. and Waters, S. 2018. *Doing a research project: A guide for first-time researchers* (7th ed.). Maidenhead: Open University Press.

Bell, C. 2018. *The U.S. and China can and should work together to improve African maritime security*. International cooperation. Available at: https://stableseas.org/international-cooperation/us-china-improve-african-maritime-security/ (accessed on: 2 April 2019).

Bernard, K. 2015. *Port security-threats and vulnerabilities case: Takoradi Port.* Unpublished master's thesis. Laurea University of Applied Sciences, Vantaa.

Bertram, C. and Christiansen, I. 2014. *Understanding Research: An Introduction to reading research*. Pretoria: Van Schaik.

Bichou, K., Szyliowicz, J.S. and Zamparini, L. 2013. *Maritime transport security: Issues, challenges, and national policies*. Cheltenham: Edward Elgar Publishing Limited.

Blaine, M. and Nel, M. 2020. *South African maritime foreign policy: Rethinking the role of the South African Navy*. Available at: file:///C:/Users/CHRIST%20FAITH/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/1286-Article%20Text-3263-1-10-20200609%20(3).pdf (accessed on: 14 July 2020).

Borchert, H. 2014. *Maritime security at risk trends, future threats vectors, and capacity requirements.* Available at: https://www.researchgate.net/publication/263674092_Maritime_Security_at_Risk_Trends_Future_Threat_Vectors_and_Capability_Requirements/link/0046353ba8b81c4321000000/download (accessed on: 23 June 2020).

Botha, S. 2019. *The ship market and maritime finance in South Africa: An overview*. 2016. Available at: https://www.golegal.co.za/shipping-law-ship-market-

maritime-finance-south-africa-overview/ (accessed on: 19 November 2020).

Brusco, M.A. 2016. *Read this note or else! Conviction under 18 U.S.C. $875 (c) for recklessly making a threat*. Available at: https://fordhamlawreview.org/wp-content/uploads/2016/04/Brusco_May.pdf (accessed on: 31 October 2019).

Busiega, J.N. 2016. *Harnessing maritime security and resource exploitation: Role of maritime diplomacy in Kenya*. Unpublished master's degree. University of Nairobi, Kenya.

Carpenter, A. 2013. *Security and Europe's sea ports: Threats and issues facing maritime gateways to Europe*. In book: New challenges for the EU security strategy, chapter 3. Cambridge scholars publishing. Available at: https://danskehavne.dk/wp-content/uploads/2015/12/Forskningsrapport-A-Carpenter-April-2013-1283_1.pdf. (accessed on: 14 July 2020).

Casteel, A. and Bridier, N.L. 2021. Describing populations and samples in doctoral student research*. International Journal of Doctoral Studies*, 16:339-362.

Chene, M. 2018. *Corruption at borders*. Available at: https://www.u4.no/publications/corruption-at-borders.pdf (accessed on: 14 August 2020).

Chetty, V.G. 2018. *The combating of unauthorised electrical connections in KwaZulu-Natal, South Africa*. Master's thesis, UNISA, Pretoria. Available at: http://uir.unisa.ac.za/bitstream/handle/10500/25009/dissertation_chetty_vg.pdf?sequence=1&isAllowed=y (accessed on: 19 November 2020).

Christopher, K. 2009. *Port security management.* New York: CRC Press.

Comte, A. and Lombroso, C. 2010. *Explanations for criminal behaviour.* Chapter 3. Available at: https://scholar.google.co.za/scholar?hl=en&as_sdt=0%2C5&q=South+Africa%3A+Country+profile+on+drugs+and+crime.+&btnG= (accessed on: 15 July 2020).

Confederation of European Security Services. 2017. *Best practice in transport security.* Available at: https://www.scribd.com/document/405404033/Pb-Coess-

Best-Practices-in-Transport-Security-2017-10 (accessed on: 19 November 2020).

Creswell, J.W. 2014. *Research designs: Qualitative, quantitative and mixed methods approach* (4th ed.). Thousand Oaks, CA: Sage.

Dailey, J. 2014. Border security agency operations. In Phelps, J.R., Dailey, J. and Koenigsberg, M. (Eds.), *Border security* (pp. 55-106). Durham, NC: Carolina Academic Press.

Davis, P.K. and Cragin, K.R. 2009. *Social science for counterterrorism*. Santa Monica, CA: Rand National Defense Research Institute.

Democratic Alliance. 2019. *The manifesto for change: The change that builds one South Africa for all.* Available at: https://www.sancda.org.za/wp-content/uploads/2019/04/DA-manifesto-19.pdf (accessed on: 16 June 2020).

Department of Home Affairs. 2015. *Border Management Agency (BMA) project*. Available at: https://static.pmg.org.za/151020BMA_Project.pdf (accessed on: 19 August 2020).

Department of Home Affairs. 2016a. *BMA overview: Aviation security seminar 2016*. Available at: http://www.caa.co.za/Safety%20Seminars%20and%20Presentations/BMA%20Overview.pdf (accessed on: 6 July 2020).

Department of Home Affairs. 2016b. *Green paper on the international migration.* Available at: https://www.gov.za/sites/default/files/gcis_document/201606/40088gon738.pdf (accessed on: 14 August 2020).

Department of Home Affairs. 2020. *Strategic plan 2020-2025.* Available at: http://www.dha.gov.za/images/FILES2/DHA_Strategic_Plan2020_25_WEB.pdf (accessed on: 19 August 2020).

Department of Homeland Security, USA. 2015. *Immigration enforcement along U.S. borders and Ports of Entry: Federal, state and local efforts*. Available at:

http://www.pewtrusts.org/~/media/Assets/2015/02/BorderEnforcement_Brief_web.pdf (accessed on: 22 May 2020).

Department of Transport. 2017. *Comprehensive maritime transport policy (CMTP) for South Africa.* Available at: https://www.transport.gov.za/documents/11623/44313/MaritimeTransportPolicyMay2017FINAL.pdf/4fc1b8b8-37d3-4ad0-8862-313a6637104c (accessed on: 16 August 2020).

Duarte, E. 2019. Drugs, piracy and sovereignty: Brazil, United States and European union's security perspectives for South Atlantic. *Security and Peace*, 34(3):185-190. Available at: https://www.bing.com/search?q=Drugs%2C+piracy+and+sovereignty%3A+Brazil%2C+United+States+and+European+union%E2%80%99s+security+perspectives+for+South+Atlantic&form=ANSPH1&refig=cfec035ba1a34a9fa389c3366976e9e5&pc=U531 (accessed on: 16 August 2020).

Einstein, S. and Philpott, D. 2011.*The intergrated physical security handbook II: 5-step process to assess and secure critical infrastructure from hazards threats* (2nd ed.). Government Training Inc. Available at: http://governmenttraininginc.com/pdfs/Excerpt-from-IPSH-II.pdf (accessed on: 07 June 2020).

Ekwall, D. and Lantz, B. 2018. Theft of goods in ports: A review of TAPA EMEA IIS statistics. Turku, Finland: Hazard Project. Available at: https://hb.diva-portal.org/smash/get/diva2:1185898/FULLTEXT01.pdf (accessed on: 15 June 2022).

Elago, E. 2019. *Investigating the effect of cargo theft on Walvis Bay port operations in Namibia.* Unpublished master's thesis. Namibia University of Science and Technology, Windhoek.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K. and Kyngäs, H. 2014. Qualitative content analysis: A focus on trustworthiness. *Sage Open*, 4(1):1-10.

Eurostat. 2018. *Handbook on the compilation of statistics on illegal economic activities*

in national accounts and balance of payment. Luxembourg: European Union. Available at: https://ec.europa.eu/eurostat/documents/3859598/8714610/KS-05-17-202-EN-N.pdf/eaf638df-17dc-47a1-9ab7-fe68476100ec (accessed on: 22 May 2020).

Fagan, C. 2011. *Evidence of illegal cross-border flow of funds, goods and services in South Asia and their impact on corruption.* Bergen, Norway: Anti-corruption resource centre. Available at: https://knowledgehub.transparency.org/assets/uploads/helpdesk/282_Illegal_cross_border_flows_in_South_Asia.pdf (accessed on: 22 May 2020).

Farrell, G., Clark, K., Ellingworth, D. and Pease, K. 2005. *Of targets and supertargets: A routine activity theory of high crime rates*. Available at: https://www.academia.edu/29412749/Of_Targets_and_Supertargets_A_Routine_Activity_Theory_of_High_Crime_Rates (accessed on: 15 July 2020).

Feldt, L., Roell, P. and Thiele, R.D. 2013. *Maritime security-perspectives for a comprehensive approach*. (Issue no. 222). Available at: https://www.files.ethz.ch/isn/162756/222_Feldt_Roell_Thiele.pdf (accessed on: 18 November 2020).

Fouchė, C.B. 2021. Introduction to the research process. In Fouchė, C.B., Strydom, H. and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 37-53). Pretoria: Van Schaik.

Fouchė, C.B. and De Vos, A.S. 2011. Formal formulations. In De Vos, A.S., Strydom, H., Fouchė, C.B. and Delport, C.S.L. (Eds.). *Research at grassroots* (4th ed., pp. 89-100). Pretoria: Van Schaik.

Fransas, A., Nieminen, E. and Salokorpi, M. 2013. *Maritime security and security measures: Mimic study in the Baltic Sea Area.* Kotka, Finland: Kymenlaakso University of Applied Sciences. Available at: https://www.theseus.fi/bitstream/handle/10024/68155/B-sarja_106.pdf?sequence=1&isAllowed=y (accessed on: 09 April 2019).

Gard Alert. 2016. *South Africa – increased risk of stowaways*. Available at:

http://www.gard.no/web/updates/content/22207278/gard-alert-south-africa-increased-risk-of-stowaways (accessed on: 30 June 2020).

Gerstein, D.M., Alter, A., Davenport, A.C., Grill, B., Kadlec, A. and Young, W. 2018. *Managing international Borders: Balancing security with the licit flow of people and goods.* Available at: https://apps.dtic.mil/sti/pdfs/AD1084816.pdf (accessed on: 14 July 2020).

Geyer, L.S. 2021. Interviews as data collection method. In Fouchė, C.B., Strydom, H., and Roestenburg, W.J.H. (eds.), *Research at grass roots* (5th ed., pp. 355-378). Pretoria: Van Schaik.

Givens, A.D., Busch, N.E. and Bersin, A.D. 2018. Going global: The international dimensions of U.S. Homeland security policy. *Journal of Strategic Security,* 11(3):1-34. Available at: https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1689&context=jss (accessed on: 18 November 2020).

Govender, D. 2018. *Managing security information: Incidents, threats & vulnerabilities: A practical approach for security practitioners serving private and government entities in South Africa.* Pretoria: University of South Africa Press.

Gunawan, J. 2015. Ensuring trustworthiness in qualitative research. *Belitung Nursing Journal*, 1(1):10-11.

Haelterman, H. 2013. *Situational crime prevention and supply chain security: Theory for best practice*. Available at: https://www.researchgate.net/publication/236163698_Situational_Crime_Prevention_and_Supply_Chain_Security_Theory_for_Best_Practice (accessed on: 18 November 2020).

Hahonou, E.K. 2016. *Security in the Sahel: Corruption, insecurity and border control in Niger.* Available at: https://www.bing.com/search?q=Security+in+the+Sahel%3A+Corruption%2C+insecurity+and+bordercontrol+in+Niger&form=ANNTH1&refig=750c8e78b9214d72b82abe032f13149a (accessed on: 15 August 2020).

Hansen, N.R. 2005. *Probability theory and statistics: With a view towards bioinformatics*. Available at: http://web.math.ku.dk/~richard/binf/notes/chap1 (accessed on: 15 July 2020).

Haysom, S., Gastrow, P. and Shaw, M. 2018. *The heroin coast: A political economy along the eastern African seaboard.* Available at: https://globalinitiative.net/analysis/the-heroin-coast-a-political-economy-along-the-eastern-african-seaboard/

Heads, M. 2016. *Loss prevention stowaway in South African ports.* Available at: https://www.nepia.com/industry-news/update-stowaways-in-south-africa/ (accessed on: 11 December 2020).

Hechter, M. and Kanazawa, S. 1997. Sociological rational choice theory. *Annual Review of Sociology*, 23:191-214. Available at: http//scholar.google.co.za (accessed on: 6 September 2019).

Herout, J. 2017. *U.S. Maritime security – Strategies and measures applied*. Master's thesis. Charles University, Prague. Available at: https://dspace.cuni.cz/bitstream/handle/20.500.11956/86543/DPTX_2015_2_11230_0_480815_0_179527.pdf?sequence=1 (accessed on: 14 July 2020).

Hill, A. 2015. *The importance of port security*. Available at: https://www.linkedin.com/pulse/importance-port-security-andrew-hill (accessed on: 20 November 2020).

Hofmeister, W. and Rueppel, P. 2014. *Maritime security and piracy: Common challenges and responses from Europe and Asia*. Available at: https://www.kas.de/c/document_library/get_file?uuid=00ca482c-6ebf-8d25-4ac9-cee4c44df207&groupId=252038 (accessed on: 22 December 2020).

Hollis-Peel, M.E., Reynald, D.M., Bavel, M. and Welsh, B.C. 2011. *Guardianship for crime prevention: Acritical review of literature.* Available at: https://www.researchgate.net/publication/226557712_Guardianship_for_Crime_Prevention_A_Critical_Review_of_the_Literature (accessed on: 22 June 2020).

Hollman, A. 2013. Theory as represented in music lyrics. *Papers and Publications: Interdisciplinary Journal of Undergraduate Research*, 2:Article 8. Available at: http://digitalcommons.northgeorgia.edu/papersandpubs/vol2/iss1/8 (accessed on: 22 June 2020).

Hsieh, M. and Wang, S.K. 2018. Routine activities in a virtual spree: A Taiwanese case of an ATM hacking space. *International Journal of Cyber Criminology*, 12(1):333-352.

Hutson, T. 2018. Ports conduits for drug smugglers. *The Mercury*. Available at: https://www.iol.co.za/mercury/network/ports-a-conduit-for-drug-smugglers-16582099/ (accessed on: 1 April 2019).

Institute for Security Studies. 2018. *Overview of Serious and Organized Crime in East Africa.* Available at: https://enact-africa.s3.amazonaws.com/site/uploads/2018-12-12-interpol-east-africa-report.pdf (accessed on: 18 August 2020).

International Maritime Organizations. 2015. *IMO's support to the new partnership for Africa's development (NEPAD).* Available at: https://www.un.org/en/africa/osaa/pdf/unsystemfolder/2015/imo2015.pdf (accessed on: 15 August 2020).

Irandu, E. 2016. Multimodal freight transport security in Kenya. In Szyliowicz, J.S., Zamparini, L., Reniers, G.L.L. and Rhoades, D.K. (Eds.), *Multimodal transport security: Frameworks and policy applications in freight and passenger transport* (pp. 124-142). Cheltenham: Edward Edgar.

James, A.P. 2011. The impact of the war on terrorism on maritime shipping. *International Business & Economics Research Journal (IBER)*, 1(8). Available at: https://www.researchgate.net/publication/267950978_The_Impacts_Of_The_War_On_Terrorism_On_Maritime_Shipping (Assessed: 2 June 2020).

Javadi, M. and Zaera, K. 2016. Understanding thematic analysis and its pitfalls. *Journal of Client Care*, 1(1):34-40.

Jenkins, B.D. 1998. *Risk analysis helps establish a good security posture; risk*

management keeps it that way. Available at: https://www.nr.no/~abie/RA_by_Jenkins.pdf (accessed on: 07 June 2020).

John, A. and Parks, A. 2016. *Frontier Security: The Case of Brazil*. Available at: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/StrategicPerspectives-20.pdf?ver=2016-08-17-103324-443 (accessed on: 16 August 2020).

Jowet, A. 2020. *Carrying out qualitative research under lockdown: Practical and ethical consideration.* Available at: https://blogs.lse.ac.uk/impactofsocialsciences/2020/04/20/carrying-out-qualitative-research-under-lockdown-practical-and-ethical-considerations/ (accessed on: 23 November 2021).

Justus, M., Ceccato, V., Moreira, G. and Kahn, T. 2018. *Crime against trading: the case of cargo theft in São Paulo.* Available at: https://www.researchgate.net/publication/325836109_Crime_Against_Trading_The_Case_of_Cargo_Theft_in_Sao_Paulo (accessed on: 16 June 2022).

Kabir, S.M.S. 2016. *Methods of data collection*. Thousand Oaks, CA: Sage.

Kallas, S. 2014. *Ports 2030 gateways for the Trans European transport network*. Available at: https://ec.europa.eu/transport/sites/transport/files/modes/maritime/ports/doc/2014-04-29-brochure-ports.pdf (accessed on: 19 November 2020).

Khumalo, S. 2015. *Unlocking South African cross-border transport challenges: A case study of Beitbridge border post*. Available at: https://repository.up.ac.za/bitstream/handle/2263/45526/Khumalo_Unlocking_2014.pdf?sequence=1 (accessed on: 18 August 2020).

Korstjens, I. and Moser, A. 2017. Series: Practical guidance to qualitative research. Part 2: Context, Research Questions and Designs*. European Journal of General Practice,* 23(1):274-279.

Kshirsagar, J.B. and Kumar, P. 2016. Multimodal passenger transportation security

in Indian cities. In Szyliowicz, J.S., Zamparini, L., Reniers, G.L.L. and Rhoades, D.K. (Eds.), *Multimodal transport security: Frameworks and policy applications in freight and passenger transport* (pp. 261-275). Cheltenham: Edward Edgar.

Kumar, S., Dwivedi, D. and Hussain, M.S. 2016. *Maritime security challenges: The changing scenario.* Available at: https://www.academia.edu/37940797/Maritime_Security_Challenges_The_Changing_Scenario (accessed on: 17 August 2020).

Leedy, P.D. and Ormrod, J.E. 2013. *Practical research: Planning and design* (10th ed.). New York: Pearson.

Leedy, P.D. and Ormrod, J.E. 2015. *Practical research: Planning and design* (11th ed.). New York: Pearson.

Leonard, T.J., Gallo, P. and Veronneau, S. 2015. *Security challenges in United States sea ports: An overview.* Available at: https://www.researchgate.net/profile/Simon_Veronneau/publication/276407591_Security_challenges_in_United_States_sea_ports_an_overview/links/561e639b08ae50795afe97d3/Security-challenges-in-United-States-sea-ports-an-overview.pdf (accessed on: 18 August 2020).

Liwång, H., Sörenson, K. and Österman, C. 2014. *Ship security challenges in high-risk areas: Manageable or insurmountable? WMU Journal of Maritime Affairs*, 14(2):201-217. Available at: https://www.researchgate.net/publication/266079904_Ship_security_challenges_in_high-risk_areas_manageable_or_insurmountable (accessed on: 07 June 2020).

Manig, C.G. 2017. *An evaluation of threats to the safeguarding of South Africa's maritime domain.* Security and defence studies programme (SDSP) 03/17. Available at: https://www.transport.gov.za/documents/11623/108426/ResearchPaper_ThreatsMaritimeSecurity.pdf/716b7d9c-45eb-42e9-bbf1-76be395718b0 (accessed on: 20 February 2021).

Maree, K. 2007.*The first steps in research.* Pretoria: Van Schaik.

Maritime Institute of Technology and Graduate Studies. 2021. *Guide to maritime security.* Available at: https://www.mitags.org/security-guide/ (accessed on: 19 August 2022).

Martin, G. 2021. *Defence intelligence lays out maritime security threats in Africa.* Available at: https://www.defenceweb.co.za/featured/defence-intelligence-lays-out-maritime-security-threats-in-africa/ (accessed on: 01 April 2022).

Mashiri, M. and Chakwizira. J. 2016. An exploratory analysis of constraints and impediments at South African land ports of entry. Available at: https://repository.up.ac.za/bitstream/handle/2263/58024/Mashiri_Exploratory_2016.p df?sequence=1&isAllowed=y (accessed on: 01 November 2019).

May, C. 2017. *Transnational crime and the developing world.* Available at: https://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf (accessed on: 16 August 2020).

McClain, E., Thomas, P., McAleenan, K.K., Sadler, S. and Kamoie, B.E. 2014. The U.S. Senate committee on Homeland security and governmental affairs on "Evaluating port security: Progress made and challenges ahead". Available at: https://www.hsgac.senate.gov/imo/media/doc/Joint%20Testimony-DHS-2014-06-04.pdf (accessed on: 19 August 2022).

McNicholas, M. 2008. *Maritime security: An introduction* (2nd ed.). Oxford: Butterworth-Heinemann.

Miro, F. 2014. Routine activity theory. In Mitchell Miller, J. (Ed.), *The Encyclopedia of Theoretical Criminology.* Hoboken, NJ: Blackwell Publishing Ltd. Available at: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118517390.wbetc198 (accessed on: 22 June 2020).

Minnaar, A. 2001. Border control and regionalism: The case of South Africa. *African Security Review*, 10(2):9.

Minnaar, A. 2003. *Policing the ports: Reducing illicit trafficking in South Africa.* Chapter

2. ISS Monograph Series, 84. Pretoria: Institute for Security Studies.

Mlambo, V.H. and Adetiba, T.C. 2021. Illegal migration and cross border crimes: Reflecting on the challenges of South African borders. *Loyola Journal of Social Sciences, 2(2): 94-113.* Available at: https://www.researchgate.net/publication/349210970_Illegal_Migration_and_Cross_Border_Crime_Reflecting_On_the_Challenges_of_South_African_Borders (Assessed 25 April 2022).

Mollema, N. 2018. The role of the military in combating human trafficking: A South African Perspective. *Scientia Militaria, South African Journal of Military Studies*, 45(2):20–35. Available at: https://journals.co.za/doi/pdf/10.5787/45-2-1211 (accessed on: 16 August 2020).

Monacelli, N. 2018. *Improving maritime transportation security in response to industry consolidation.* Available at: https://www.hsaj.org/articles/14257 (accessed on: 18 November 2020).

Moodley, D.M. 2014. An investigation into the illegal movement of goods from sea-ports-of-entry: A case study at Durban Harbour. Unpublished MTech dissertation. University of South Africa, Pretoria.

Moon, K. and Blackman, D. 2014. A guide to understanding social science research for natural scientists. *The Society for Conversation Biology***, 28(5): 1167:1177.**

Morris, S., George, D., Haseley, A., Parker, N. and Sherman, B. 2020. *Smart borders increasing security without sacrificing mobility.* Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/dttl-ps-GMBM-Border-Point-Booklet.pdf (accessed on: 16 August 2020).

Nagi, A., Indorf, M. and Kersten, W. (Eds.). 2017. Bibliometric analysis of risk management in Maritime Ports. Available at: https://www.researchgate.net/publication/320170616_Bibliometric_Analysis_of_Risk_Management_in_Maritime Ports (accessed on: 18 November 2020).

Narvenkar, M.V. 2018. *Managing India's Maritime Security post 26/11*. Available at:

http://irgu.unigoa.ac.in/drs/bitstream/handle/unigoa/5727/narvenkar_m_v_2018.pdf?sequence=1&isAllowed=y (accessed on: 16 August 2020).

Neely, W.A. 2012. The perceived effectiveness of container security at Maritime Ports along the gulf coast. Master's thesis. The University of Mississippi, Oxford, MS. Available at: https://www.theseus.fi/bitstream/handle/10024/68155/B-sarja_106.pdf?sequence=1&isAllowed=y (accessed on: 21 August 2019).

Neumann, T. 2020. *South Africa records 195% increase in cargo thefts in 2019: TAPA*. Available at: https://www.logupdateafrica.com/south-africa-records-195-increase-in-cargo-thefts-in-2019-tapa-logistics (accessed on: 2 July 2020).

Ngulube, P. 2015. Qualitative data analysis and interpretation: Systematic search for meaning. In Mathipa, E.R. and Gumbo, M.T. (Eds.), *Addressing research challenges: Making headway for developing researchers* (pp. 131-156). Noordyk: Mosala-MASEDI Publishers.

Nieuwenhuis, G. 2016. Challenges for multimodal freight transport. In Szyliowicz, J.S., Zamparini, L., Reniers G.L.L. and Rhoades D.K. (Eds.), *Multimodal transport security: Frameworks and policy applications in freight and passenger transport* (pp. 21-34). Edward Edgar: Cheltenham.

Ofosu-Boateng, N.R.L. 2017. A SWOT analysis of maritime transportation and security in the Gulf of Guinea. *Open Journal of Social Science*, 5(8):14-15. Available at: DOI:10.4236/jss.2017.58002 (accessed on: 19 November 2020).

O'Gorman, K.D. and Macintosh, R. 2015. Mapping research methods. In *Research Methods for Business and Management* (2nd ed., pp. 50-74). Oxford: Goodfellow Publishers Ltd.

Organized Crime Research Brief. 2018. *Organized Crime Research Brief no. 25: Marine ports and organized crime.* Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rgnzd-crm-brf-25/rgnzd-crm-brf-25-eng.pdf (accessed on: 19 May 2022).

Osimen, G.U., Anegbode, E.J., Akande, C.A. and Oyewole, O.O. 2017. *The*

borderless-border and internal security challenges in Nigeria. Available at: https://www.arcjournals.org/pdfs/ijps/v3-i3/3.pdf (accessed on: 20 August 2020).

Parliamentary Monitoring Group. 2013. *State of Ports of Entry: Department of Home Affairs briefing.* Available at: https://pmg.org.za/committee-meeting/15635/ (accessed on: 25 May 2022).

Panargo Shipping (Pty) Ltd. 2011. *Cape Town Port Information*. Available at: http://www.panargo.co.za/wp-content/uploads/2011/06/ct.pdf (accessed on: 20 November 2020).

Pearl, S. 2019. *Maritime port security: Preventing terrorist attacks in America.* Available at: http://dspace.calstate.edu/bitstream/handle/10211.3/211978/Pearl%20Capstone%20Maritime%20Port%20Security .pdf?sequence=1 (accessed on: 16 August 2020).

Pena, F. 1997. *Port security: A national planning guide.* Department of transportation: United States. Available at: https://rosap.ntl.bts.gov/view/dot/13693 (accessed on: 22 May 2020).

Phelps, J. 2014. *Trafficking: Contraband, smuggling, and the law.* In Phelps, J.R., Dailey, J. and Koenigsberg, M. (Eds.), *Border security* (pp. 167-188). Durham, NC: Carolina Academic Press.

Pinto, M. 2018. *Employment of the Brazilian armed forces against cross-border crimes.* Master's thesis. National Defense University, Washington DC. Available at: https://bdex.eb.mil.br/jspui/bitstream/123456789/2700/1/master%27s%20degree_2018_Col%20Marcelo%20Silva_%201st%20draft%20%281%29.pdf (accessed on: 15 August 2020).

Pichon, E. and Pietsch, M. 2019. *Piracy and armed robbery off the coast of Africa.* European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/635590/EPRS_IDA(2019)635590_EN.pdf?msclkid=68c35204bd9811ecbd38b7283316e2d8

(accessed on: 16 April 2022).

Pohlit, C. 2014. New developments in maritime security and their impact on international shipping. Unpublished MTech Thesis. University of Cape Town, Cape Town.

Ponelis, S.R. 2015. Using interpretative qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies*, 10:535-550. Available at: http://ijds.org/Volume10/IJDSv10p535-550Ponelis0624.pdf (accessed on: 23 November 2021).

Purdy, G. 2010. Perspective ISO 31000:2009 – Setting a new standard for risk management. *Risk Analyst*, 30(6): 881-886. Available at: http://esvc001356.wic015u.server-web.com/pdfs/articles/art_riskanalysis_iso31000.pdf (accessed on: 18 August 2020).

Proag, V. 2014. *The concept of vulnerability and resilience*. Available at: https://www.researchgate.net/publication/270293079_The_Concept_of_Vulnerability_and_Resilience (accessed on: 01 October 2019).

Potgieter, T. and Rommerin, R. 2009. *Maritime Security in Southern African waters.* Stellenbosch: Sun Media.

Ramsaroop, S. 2016. *Understanding the International Ship and Port Facility Security (ISPS) Code: An examination of the implementation and effectiveness of the ISPS Code.* Unpublished MTech Dissertation. University of KwaZulu-Natal, Durban.

Ramson, S.M. and Chetty, R. 2016. *Taking strain: Theorising drug use in the Cape Flats.* Available at: http://digitalknowledge.cput.ac.za/bitstream/11189/5572/1/Ramson_Shakti%20M_Chetty_Rajendra_.pdf (accessed on: 18 August 2020).

Reniers, G.L.L., Rhoades, D.L., Szyliowicz, J.S. and Zamparini, L. 2016. Border

security agency operations. In Phelps, J.R., Dailey, J. and Koenigsberg, M. *Border Security* (pp. 55-106). Durham, NC: Carolina Academic Press.

Rhoades, D.L. 2016. *Multimodal passenger transportation security in Brazil*. (Pp. 276-290). In Szyliowicz, J.S., Zamparini, L., Reniers, G.L.L. and Rhoades, D.K. (Eds.), *Multimodal transport security: Frameworks and policy applications in freight and passenger transport*. Cheltenham: Edward Edgar.

Rehman, A.A. and Alharthi, K. 2016. An introduction to research paradigm. *International Journal of Educational Investigation*, 3(8):51-59.

Ridgway, P. 2020. *Africa ports and ships.* Available at: https://africaports.co.za/cape-town/ (accessed on: 22 December 2020).

Roestenburg, W.J.H. 2021. Qualitative data collection methods. In Fouché, C.B., Strydom, H., and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 199-226). Pretoria: Van Schaik.

Rosenblum, M.R. and Hipsman, F. 2016. *Border metrics: How to effectively measure border security and immigration control*. Available at: http://www.migration4development.org/sites/default/files/bordermetrics-final.pdf (accessed on: 16 August 2020).

Rosenblum, M.R., Bjelopera, J.P. and Finklea, K.M. 2013. *Border security: Understanding threats at U.S. borders*. Washington, DC: Congressional Research Service. Available at: https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=2042&context=key_workplace (accessed on: 13 August 2019).

Sangathan, M.K.S. and Nehru, J. 2011. *IS/ISO 31000 (2009):* Risk *management – principles and guidelines [MSD 4: Management and Productivity]*. Available at: https://law.resource.org/pub/in/bis/S07/is.iso.31000.2009.pdf (accessed on: 21 June 2020).

Schlesinger, J. and Day, A. 2019. *Here's how the trade war could lead to a boom in counterfeit goods.* Available at: https://www.cnbc.com/2019/03/13/heres-how-

the-trade-war-could-lead-to-a-boom-in-counterfeit-goods.html (accessed on: 5 July 2020).

Schurink, W.J., Schurink, E.M. and Fouchė, C.B. 2021. Qualitative data analysis and interpretation. In Fouchė, C.B., Strydom, H. and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 391-415). Pretoria: Van Schaik Publisher.

Schurink, W.J., Schurink, E.M. and Fouchė, C.B. 2021. Thematic enquiry in qualitative research. In Fouchė, C.B., Strydom, H. and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp 289-310). Pretoria: Van Schaik.

Seda, F.L.M. 2015. *Border governance in Mozambique: The intersection of international border controls, regional integration and cross-border regions*. Rotterdam: Erasmus University.

Sefotho, M.M. 2021. Research and professional practice. In Fouchė, C.B., Strydom, H. and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 3-22). Pretoria: Van Schaik Publisher.

Segovia, M., Cavalli, A.R., Cuppens, N. and Garcia-Alfaro, J. 2019. *A study on mitigation techniques for SCADA-Driven Cyber-Physical Systems (Position paper). Available at:* http://www-public.imtbs-tsp.eu/~garcia_a/web/papers/preprint-fps2018.pdf (accessed on: 17 August 2020).

Shariati, M. and Guerette, R.T. 2017. Situational crime prevention. In Teasdale, B. and Bradley-Engen, M.S. (Eds.), *Preventing Crime and Violence* (pp. 261-268). Cham: Springer.

Singh, A. 2019. *Maritime terrorism in Asia: An assessment.* Available at: https://safety4sea.com/wp-content/uploads/2019/10/ORF-Maritime-terrorism-in-Asia-2019_10.pdf (accessed on: 16 August 2020).

South African Government News Agency. 2014. *Port of entry control centre opens in Cape Town*. Available at: https://www.sanews.gov.za/south-africa/port-entry-control-centre-opens-cape-town (accessed on: 20 November 2020).

South African Government News Agency. 2019. *SA playing its part to curb maritime crime.* Available at: https://www.sanews.gov.za/south-africa/sa-playing-its-part-curb-maritime-crime (accessed on: 19 August 2022).

South Africa. 1951. Merchant Shipping Act 57 of 1951. Union Gazette Extraordinary. Pretoria: Government Printers. Available at: https://www.gov.za/sites/default/files/gcis_document/201505/act-57-1951.pdf (accessed on: 2June 2022).

South Africa. 1964. Government Customs and Excise Act 91 of 1964. *Government Gazette*. Pretoria: Government Printers. Available at: https://www.sars.gov.za/wp-content/uploads/Legal/SecLegis/LAPD-LSec-CE-RA-2014-10-Customs-and-Excise-Rules-1995-as-amended.pdf (accessed on: 22 June 2002).

South Africa. 1995. South African Police Act 68 of 1995. *Government Gazette. 16731*. Pretoria: Government Printers. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/act68of1995.pdf (accessed 21 June 2022).

South Africa. 1998. Marine Living Resource Act 18 of 1998. *Government Gazette*. Pretoria: Government Printers. Available at: https://www.gov.za/sites/default/files/gcis_document/201610/a18-98.pdf (accessed on: 22 June 2002).

South Africa. 2002. Immigration Act 13 of 2002. *Government Gazette*. Pretoria: Government Printers. Available at: http://www.saflii.org/za/legis/num_act/ia2002138.pdf (accessed on: 22 June 2002).

South Africa. 2005. National Port Act 12 of 2005. *Government Gazette 792*. Pretoria: Government Printers. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/a12-051.pdf (accessed on: 22 June 2022).

South Africa. 2013. Anti-Trafficking Act 7 of 2013. *Government Gazette. 36715.*

Pretoria: Government Printers. Available at: https://www.justice.gov.za/legislation/acts/2013-007.pdf (accessed on: 22 June 2022).

Steinberg, J. 2005. *An overview of South African border control: 1994-2004*. Institute for Security Studies. Available at: https://issafrica.org/ctafrica/uploads/An%20overview%20of%20South%20African%20border%20control-%201994-2004.pdf (accessed on: 19 August 2022).

Stoneburner, G., Goguen, A. and Feringa, A. 2002. *Risk management guide for information technology systems.* NIST publication. Available at: https://www.archives.gov/files/era/recompete/sp800-30.pdf (accessed on: on 22 May 2020).

Strydom, H. 2021a.Contemporary data collection methods. In Fouchė, C.B., Strydom, H. and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 335-354). Pretoria: Van Schaik Publisher.

Strydom, H. 2021b. Sampling techniques and pilot studies in qualitative research. In Fouchė, C.B., Strydom, H. and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 379-390). Pretoria: Van Schaik Publisher.

Strydom, H. 2021c. Sampling techniques and pilot studies in quantitative research. In Fouchė, C.B., Strydom, H. and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 227-247). Pretoria: Van Schaik Publisher.

Strydom, H. and Roestenburg, W.J.H. 2021. Ethical conduct in research with human participants. In Fouchė, C.B., Strydom, H., and Roestenburg, W.J.H. (Eds.), *Research at grass roots* (5th ed., pp. 117-136). Pretoria: Van Schaik Publisher.

Stuckey, H.L. 2014. The first step in data analysis: Transcribing and managing qualitative research data. *Journal of Social Health and Diabetes*, 2(1).

The Law Library of Congress. 2013. *Citizenship pathways and border protection.* Available at: https://tile.loc.gov/storage-services/service/ll/llglrd/2013417252/2013417252.pdf (accessed on: 16 August

2020).

The “PEW” Charitable Trusts. 2015. *Immigration enforcement along U.S. borders and at Ports of Entry: Federal, state, and local efforts*. Available at: http://www.pewtrusts.org/~/media/Assets/2015/02/BorderEnforcement_Brief_web.pdf (accessed on: 07 June 2020).

TheSAMag. 2018. *The Port of Cape Town: Adapting to the challenges of a modern commercial port*. Available at: https://thesa-mag.com/features/infrastructure/port-cape-town-adapting-challenges-modern-commercial-port/ (accessed on: 21 November 2020).

United Nations Office on Drugs and Crime. 2011. *Smuggling of migrants by sea.* Available at: https://www.unodc.org/documents/human-trafficking/Migrant-Smuggling/Issue-Papers/Issue_Paper_-_Smuggling_of_Migrants_by_Sea.pdf (accessed on: 10 May 2022).

United Nations Office on Drugs and Crime. 2013. *Independent project evaluation of the strengthening law enforcement capacity (border control operations) and criminal justice response to smuggling of migrants and trafficking in person.* Available at: http://www.unodc.org/documents/evaluation/Independent_Project_Evaluations/2013/ZAF_T54_Independent_Project_Evaluation_Report_01Aug2013.pdf (accessed on: 18 November 2020).

United Nations Office on Drugs and Crime. 2017. *Maritime crime: A manual for criminal justice practitioners*. Available at: https://www.unodc.org/documents/Maritime_crime/19-02087_Maritime_Crime_Manual_Second_Edition_ebook.pdf (accessed on: 21 November 2020).

Van Marle, G. 2019. *Shippers and insurers renew calls for transnational coordination to tackle cargo theft.* Available at: https://theloadstar.com/shippers-and-insurers-renew-calls-for-transnational-coordination-to-tackle-cargo-theft/ (accessed on: on 4 July 2020).

Van Nieuwkerk, A. and Manganyi, C. 2019. *South Africa's maritime foreign policy: A conceptual framework.* Available at: https://journals.co.za/doi/pdf/10.10520/EJC-1ddd136531 (accessed on: 16 August 2020).

Vrey, F. and Mandrup, T. 2015.*Towards good order at sea: African Experiences.* Stellenbosch: Sun Media.

Walker, T. 2020. SADC's pursuit of maritime security in a Regional Lacking Regionalism. *South African Journal of Military Studies*, 47(2):53-70. Available at: https://scientiamilitaria.journals.ac.za/pub/article/view/1283 (accessed on: 16 August 2020).

Walker, T. and Reva, D. 2020. *South Africa's maritime domain awareness: A capability baseline assessment.* Institute for security studies. Available at: https://issafrica.org/research/books-and-other-publications/south-africas-maritime-domain-awareness-a-capability-baseline-assessment (accessed on: 26 April 2022).

Welman, C., Kruger, F. & Mitchell, B. 2005. *Research methodology* (3rd ed.). Cape Town: Oxford University Press.

Williams, M.J. 2016. Multimodal freight transportation security in Brazil. In Szyliowicz, J.S., Zamparini, L., Reniers, G.L.L. and Rhoades, D.K. (Eds.), *Multimodal transport security: Frameworks and policy applications in freight and passenger transport* (pp. 160-174). Cheltenham: Edward Edgar.

Young, R.R., Gordon, G.A. and Plant, J.F. 2018. *Railway security: Protecting against manmade and natural disasters*. New York: Routledge.

Yushan, P., Oksavik, A. and Hildre, H.P. 2020. Making sense of maritime simulators use: A multiple case study in Norway. *Technology, Knowledge and Learning*, 26:661-686.

ANNEXURE A: Approval from UNISA CLAW Ethics review committee

UNISA university of south africa

UNISA 2020 ETHICS REVIEW COMMITTEE

Date: 2020:07:22

ERC Reference No. : ST73
Name : MP Munyai

Dear Mrs Mkateko Phillis Munyai

Decision: Ethics Approval from 2020:07:22 to 2023:07:22

Researcher: Mrs Mkateko Phillis Munyai

Supervisor: Prof D Govender

AN ASSESSMENT OF SECURITY MEASURES AT THE MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

Qualification: MA Criminal Justice

Thank you for the application for research ethics clearance by the Unisa 2020 Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **Low risk application** was reviewed by the CLAW Ethics Review Committee on 22 July 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. **The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached.**

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE B: Request for permission letter to conduct research to TNPA

PERMISSION LETTER

Request for permission to conduct research at maritime ports of entry in Durban and Cape Town South Africa

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

09 September 2020

Training Manager
Transnet Security

Dear Mr Goliath

I am Mrs Mkateko Phillis Munyai, I am conducting research for my Master's Degree in Security Management. My supervisor is Prof Doraval Govender, from the Department: Criminology and Security Science at the University of South Africa. We are inviting you to participate in a study entitled, "An assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa". The study is not funded by any external funders and is aimed at knowledge generation and human capital development in response to the needs of South Africa and the African continent.

The aim of the study is to assess security measures at Durban and Cape Town maritime ports of entry. The research objectives are;

- To identify threats, vulnerabilities and security risks confronting maritime ports of entry in South Africa;
- To establish the roles and responsibilities of maritime security officials in ensuring security at the ports of entry in South Africa; and
- To identify security measures to improve security at the maritime port of entry in Durban and cape Town, South Africa.

Your institution has been selected to participate in this study because you are directly/indirectly involved in security at maritime ports of entry in Durban and Cape Town.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392, UNISA, 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE C: Request for permission letter to conduct research to SAMSA

PERMISSION LETTER

Request for permission to conduct research at maritime ports of entry in Durban and Cape Town South Africa

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

09 September 2020

The Head of Research
South African Maritime Safety Authority
Tel: 012 355 6631
wmkuna@samsa.org.za

Dear Sir/Madam

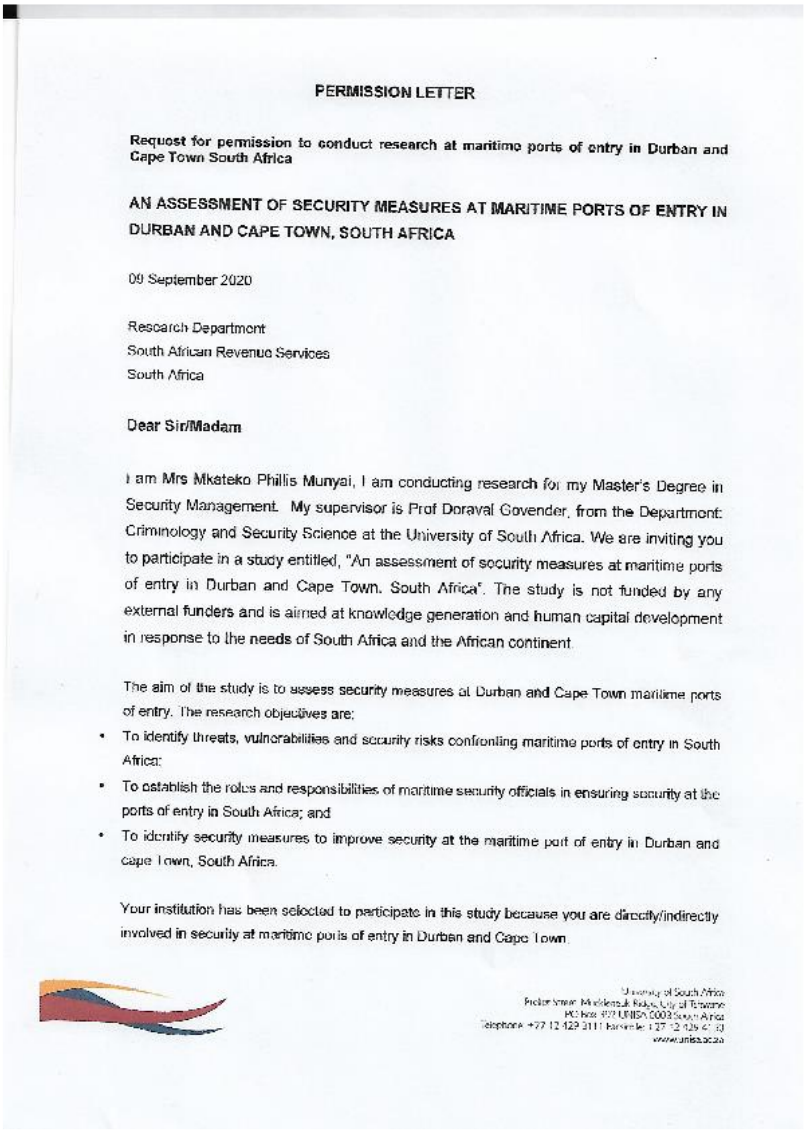
I am Mrs Mkateko Phillis Munyai. I am conducting research for my Master's Degree in Security Management. My supervisor is Prof Doraval Govender, from the Department: Criminology and Security Science at the University of South Africa. We are inviting you to participate in a study entitled, "An assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa". The study is not funded by any external funders and is aimed at knowledge generation and human capital development in response to the needs of South Africa and the African continent.

The aim of the study is to assess security measures at Durban and Cape Town maritime ports of entry, in South Africa. The research objectives are;

- To identify threats, vulnerabilities and security risks confronting maritime ports of entry in South Africa;
- To establish the roles and responsibilities of maritime security officials in ensuring security at the ports of entry in South Africa; and
- To identify security measures to improve security at the maritime port of entry in Durban and cape Town South Africa

Your institution has been selected to participate in this study because you are directly/indirectly involved in security at maritime ports of entry in Durban and Cape Town

ANNEXURE D: Request for permission letter to conduct research to SARS



PERMISSION LETTER

Request for permission to conduct research at maritime ports of entry in Durban and Cape Town South Africa

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

09 September 2020

Research Department
South African Revenue Services
South Africa

Dear Sir/Madam

I am Mrs Mkateko Phillis Munyai, I am conducting research for my Master's Degree in Security Management. My supervisor is Prof Doraval Govender, from the Department: Criminology and Security Science at the University of South Africa. We are inviting you to participate in a study entitled, "An assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa". The study is not funded by any external funders and is aimed at knowledge generation and human capital development in response to the needs of South Africa and the African continent.

The aim of the study is to assess security measures at Durban and Cape Town maritime ports of entry. The research objectives are:

- To identify threats, vulnerabilities and security risks confronting maritime ports of entry in South Africa;
- To establish the roles and responsibilities of maritime security officials in ensuring security at the ports of entry in South Africa; and
- To identify security measures to improve security at the maritime port of entry in Durban and cape Town, South Africa.

Your institution has been selected to participate in this study because you are directly/indirectly involved in security at maritime ports of entry in Durban and Cape Town.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone +27 12 429 3111 Facsimile +27 12 429 4150
www.unisa.ac.za

ANNEXURE E: Request for permission letter to conduct research to DHA

PERMISSION LETTER

Request for permission to conduct research at maritime ports of entry in Durban and Cape Town South Africa

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

09 September 2020

Acting Director Human Resource Development
Research Department
Department of Home Affairs

Dear Sir/Madam

I am Mrs Mkateko Phillis Munyai, I am conducting research for my Master's Degree in Security Management. My supervisor is Prof Doraval Govender, from the Department: Criminology and Security Science at the University of South Africa. We are inviting you to participate in a study entitled, "An assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa". The study is not funded by any external funders and is aimed at knowledge generation and human capital development in response to the needs of South Africa and the African continent.

The aim of the study is to assess security measures at Durban and Cape Town maritime ports of entry. The research objectives are;

- To identify threats, vulnerabilities and security risks confronting maritime ports of entry in South Africa;
- To establish the roles and responsibilities of maritime security officials in ensuring security at the ports of entry in South Africa; and
- To identify security measures to improve security at the maritime port of entry in Durban and cape Town, South Africa.

Your institution has been selected to participate in this study because you are directly/indirectly involved in security at maritime ports of entry in Durban and Cape Town.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392, UNISA 0003, South Africa
Telephone: +27 12 429 4111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE F: Request for permission letter to conduct research to SAPS

PERMISSION LETTER

Request for permission to conduct research at maritime ports of entry in Durban and Cape Town South Africa

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

09 September 2020

The Head of Research
South African Police Services
Tel: 012 393 3118

Dear Sir/Madam

I am Mrs Mkateko Phillis Munyai. I am conducting research for my Master's Degree in Security Management. My supervisor is Prof Doraval Govender, from the Department: Criminology and Security Science at the University of South Africa. We are inviting you to participate in a study entitled, "An assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa". The study is not funded by any external funders and is aimed at knowledge generation and human capital development in response to the needs of South Africa and the African continent.

The aim of the study is to assess security measures at Durban and Cape Town maritime ports of entry, in South Africa. The research objectives are:

- To identify threats, vulnerabilities and security risks confronting maritime ports of entry in South Africa;
- To establish the roles and responsibilities of maritime security officials in ensuring security at the ports of entry in South Africa; and
- To identify security measures to improve security at the maritime port of entry in Durban and cape Town, South Africa.

Your institution has been selected to participate in this study because you are directly/indirectly involved in security at maritime ports of entry in Durban and Cape Town.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12-429 4150
www.unisa.ac.za

ANNEXURE G: Request for permission letter to conduct research to SANDF

PERMISSION LETTER

Request for permission to conduct research at maritime ports of entry in Durban and Cape Town South Africa

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

09 September 2020

Research Department
South African National Defence Force

Dear Sir/Madam

I am Mrs Mkateko Phillis Munyai, I am conducting research for my Master's Degree in Security Management. My supervisor is Prof Doraval Govender, from the Department: Criminology and Security Science at the University of South Africa. We are inviting you to participate in a study entitled, "An assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa". The study is not funded by any external funders and is aimed at knowledge generation and human capital development in response to the needs of South Africa and the African continent.

The aim of the study is to assess security measures at Durban and Cape Town maritime ports of entry. The research objectives are;

- To identify threats, vulnerabilities and security risks confronting maritime ports of entry in South Africa
- To establish the roles and responsibilities of maritime security officials in ensuring security at the ports of entry in South Africa; and
- To identify security measures to improve security at the maritime port of entry in Durban and cape Town, South Africa.

Your institution has been selected to participate in this study because you are directly/indirectly involved in security at maritime ports of entry in Durban and Cape Town.

ANNEXURE H: Inform consent form

UNISA university of south africa

INFORMED CONSENT LETTER

CONSENT TO PARTICIPATE IN THIS STUDY

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the semi-structured interview.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname…… (please print)

Participant Signature……..Date……

Researcher's Name & Surname……(please print)

Researcher's signature……..Date……

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE I: Interview schedule questions

MKATEKO PHILLIS MUNYAI 38893207

INTERVIEWS SCHEDULE

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

Dear prospective participant

I am Mrs Mkateko Phillis Munyai, and I am conducting research for my Master's Degree in Security Management. My supervisor is Prof Doraval Govender, from the Department: Criminology and Security Science at the University of South Africa. We are inviting you to participate in a study entitled, "An assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa". The study is not funded by any external funders and is aimed at knowledge generation and human capital development in response to the needs of South Africa and the African continent.

The interviews schedule has been designed to assess security measures at maritime ports of entry in Durban and Cape Town, South Africa. You were selected to participate in this interview because you are directly/indirectly involved in security at maritime ports of entry in Durban and Cape Town. To participate in this interview, you must be at least 18 years old and employed. By participating in this interview, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the responses I obtain from this interview will help me improve security at maritime ports of entry in Durban and Cape Town, South Africa. However, you are under no obligation to participate in the interview and you may withdraw from the study prior to completing the interview. The interviewee will be anonymous, meaning that I will have no way of connecting the information that you provide to you personally. You may withdraw from the interview at any time without any penalty. If you choose to participate in this interview, it will take 30 minutes of your time. You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will help maritime ports of entry to improve their current security practices. We do not foresee that you will experience any negative consequences by participating in the interview. The researcher undertakes to keep any information provided herein confidential, not to let it out of my possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes where after it will be deleted permanently from the hard drives of the researcher's computers. You will not be reimbursed or receive any incentives for your participation in the interview.

The research was reviewed and approved by the CLAW Ethics Review Committee (ERC). You can contact me, Mrs MP Munyai, the primary researcher, during office hours at 012 427 5072. Should you have ethical concerns about the way in which the research has been conducted, you may contact the Research Ethics Chairperson of

1

the University Research Ethics Review Committee (URERC), Dr Retha Visagie at visagrg@unisa.ac.za.
Alternatively, you can report any serious unethical behaviour at the University's Toll Free Hotline 0800 86 96 93.

Please make a decision whether or not to participate in this interview choosing the appropriate option below.

Do you agree to participate in this interview?	Yes	No

SECTION A

BIOGRAPHICAL DATA

1. Gender

Female	1
Male	2

2. Age range

18-25	1
26-35	2
36-45	3
46- and above	4

3. Educational qualification

Standard 8/grade 10 and below	1
Standard 10/grade 12	2
Post matric certificate	3
Diploma (1 year)	4
Diploma (2 years)	5
Diploma (3 years)	6
Advanced diploma	7
Degree	8
Postgraduate diploma/ degree	9
Other	10

4. At which port of entry are you deployed?

Durban	Cape Town
1	2

5. Indicate your present employer:

Security	Customs	SAPS	SAMSA	SANDF
1	2	3	4	5

6. How long have you been working for your current company / employer?

Less than a year	One to two years	Between two and three years	Over three years but less than five years	More than five years
1	2	3	4	5

7. Have you undergone security-related training on maritime ports of entry?

YES	NO
1	2

SECTION B

THREATS, VULNERABILITIES AND SECURITY RISKS CONFRONTING MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

8. What is your understanding of threats, vulnerabilities and security risks?

8.1 Threats

_____
_____
_____
_____

8.2 Vulnerabilities

_____
_____
_____
_____

8.3 Security Risks

_____
_____
_____
_____

9. Did you ever encounter drug smuggling, theft, human trafficking, vandalism, or any other criminal conduct while working at the maritime port of entry?

YES	NO

1	2

10. Describe the crimes you encountered while working at the maritime port of entry.

_____
_____
_____
_____

10.1 What method was used by perpetrators to commit crimes identified in question 10?

Concealment	False documentation	Counterfeit goods	Corruption by port officials(including assistance by officials)	Other
1	2	3	4	5

11. What resource is used to detect security risks at maritime ports of entry?

Detector dogs	1
Non-intrusive examination through the use of technology	2
Trace particle detection	3
Physical examination of cargo or ship	4
Other (specify)	5

12. Do you think that the resources used by maritime ports of entry to detect security risks are effective?

YES	NO
1	2

12.1 If your response to question 11 is **No**, please provide other resources you recommend to detect security risks at maritime ports of entry?

_____
_____
_____
_____
_____

13. Can you tell me which areas are vulnerable at the maritime ports of entry?

_____
_____

_____
_____
_____

14. What level of security risk do the under mentioned crimes pose at Durban and Cape Town maritime ports of entry? 0= No risk; 1 = low risk, 2= medium risk & 3 = high risk

CRIMES		RISK LEVEL
Armed robbery	1	
Drug trafficking	2	
Illegal immigration	3	
Stowaway	4	
Human trafficking	5	
Container crimes	6	
Vandalism	7	
Other(specify)	8	

15. What level of security risk do the physical protection systems listed below pose at Durban and Cape Town maritime ports of entry? ? 0= No risk; 1 = low risk, 2= medium risk & 3 = high risk

PHYSICAL PROTECTION SYSTEMS		RISK LEVEL
Access Control	1	
Egress Control	2	
Perimeter Fencing	3	
Security Lighting	4	
Human Security/Guards	5	
CCTV cameras	6	
X Ray Scanners	7	
Metal Detectors	8	
Alarm systems	9	
Parking areas	10	
Storage areas	11	

16. Describe specific factors pertaining to discipline of security officials that can be considered as human risks at maritime ports of entry.

_____
_____
_____
_____
_____

SECTION C

ROLES AND RESPONSIBILITIES OF MARITIME SECURITY OFFICIALS IN ENSURING SECURITY AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

17. What is your understanding of the concept "Maritime Security"?

_____
_____
_____
_____

18. Describe your role and responsibilities in ensuring security at maritime ports of entry.

Access control	Patrol duties	Guard duties	Inspections of goods/permit	Surveillance/control room	Other
1	2	3	4	5	6

19. What intervention/s are used by maritime security officials to address security risks at maritime ports of entry?

Cross-border cooperation	1
Information sharing	2
National joint operations	3

20. What challenges do the global and regional maritime security stakeholders face in collaboration and information sharing?

_____
_____
_____
_____

21. How many incidents of crime do you discover during a month?

1-5 incidents	6-9 incidents	10-14 incidents	15-19 incidents	20 and more incidents
1	2	3	4	5

22. What, in your opinion, are the factors that promote illegal immigration and smuggling of illegal goods through maritime ports of entry?

_____
_____

23. Describe the security assessment briefing given to security officials at maritime ports of entry.

24. Explain the legal framework and the policies that govern your work as a maritime security official.

25. Describe the type of training that should be provided to officials in your department who are employed at maritime ports of entry.

26. Do you think that maritime security officials should be trained jointly?

YES	NO
1	2

26.1 If your response to question 26 is **Yes**, discuss your reasons for joint training.

27. Explain how your role and responsibilities should be improved to be more effective.

SECTION D

SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

28. What is your understanding of the concept "Security Measures" at maritime ports of entry in South Africa?

_____
_____
_____
_____
_____

29. What security controls are used at maritime ports of entry?

Immigration controls	1
Customs controls	2
Border safe guarding and surveillance	3
Inspections of goods, animals and human	4
Border policing	5

30. Describe the measures that are available for the safety and security of maritime contractors and companies operating in the coastal areas.

Automatic Identification System (AIS)	1
Identification and Tracking of Ships (ITS)	2
Ship security Alarm System (SSAS)	3
Vessel Traffic System (VTS)	4
Long-Range Identification and Tracking of ships (LRIT)	5
International Ship and Port Facility Security (ISPS) Code	7
Other (specify)	8

30.1 Do the measures mentioned in question 30 help to instil safety and security for maritime contractors and companies operating in the coastal areas?

YES	NO
1	2

31. Are the current security measures effective in providing access control?

YES	NO
1	2

31.1 If your response to Question 31 is **No**, describe the security measures you suggest to improve the current system?

8

MKATEKO PHILLIS MUNYAI 38893207

_____
_____
_____
_____
_____

Thank you for participating in this interview. Your cooperation is highly appreciated.

Date:

Time:

Place:

Number:

ANNEXURE J: Observation checklist

OBSERVATION CHECKLIST

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

OBSERVATION DATE:

OBSERVATION TIME:

NAME OF PORT OF ENTRY OBSERVED:

OBSERVATION POINTS:

1. OUTER LAYERS OF PROTECTION:

ASSET REMOVAL PERMITS

ACCESS CONTROL STANDARDS

INTERNAL CONTROLS

PERIMETER FENCING

BEAMS

BUILDING ACCESS POINTS

MOTION SENSORS

ALARM SYSTEMS

DETECTION OF EXPLOSIVES

EGRESS CONTROL STANDARDS

PARKING AREAS

SEAL AND TAMPER INDICATIVE DEVICES

BARRIERS

BIOMETRIC IDENTITY VERIFICATION SYSTEMS

WINDOWS

ILLUMINATION (LUX UNITS)

DOORS

SECURITY PATROLS

2. INNER LAYERS OF PROTECTION:

SECURITY PERSONNEL

EMPLOYEE VETTING

SYSTEM OPERATION

NETWORK MONITORING

STORAGE AREAS

CLOSED CAMERA CIRCUIT TELEVISION

FINANCE OFFICE

GLASS BREAKER

LOCKS AND KEY CONTROLS

CARD READERS

FIRE AND SMOKE DETECTION

ALERTS AND NOTIFICATION

WARNING SIGNS

COMMUNICATION DEVICES

SEARCH SYSTEMS

SECURITY LIGHTING

DOCUMENT REGISTER

SECURITY PATROLS

POLICIES AND PROCEDURES

SECURITY AWARENESS

EMERGENCY EVACUATION PLAN

ANNEXURE K: Documentary study checklist

MP MUNYAI 38893207

DOCUMENTARY STUDY CHECKLIST: CASE DOCKET ANALYSIS

AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

DETAILS OF CRIMINAL CASE

Crime:

Name of Port of Entry where crime occurred:

Day of week when crime occurred:

Time of occurrence:

Period when crime occurred:

Day (06:00 – 17:59)

Night (18:00-05:59)

MODUS OPERANDI

Method used by perpetrators to commit the crime. Describe in detail:

How was entry gained into premises? Describe in detail:

OUTCOMEOF THE CRIMINAL CASE

Arrests: Who was arrested? Custom officials/ private security/border police officials or private persons:

Any admissions / confessions / statement made by arrested person:

Exhibits: Type of asset involved:

Any recovery of assets:

Motive for the illegal activity:

Guilty/ not guilty:

Conviction/ sentence:

How was case docket closed and filed:

Date when case was closed:

ANNEXURE L: Approval letter to conduct research from SAPS

South African Police Service — Suid-Afrikaanse Polisiediens

Privaatsak Private Bag x94	Pretoria 0001	Faks No Fax No.	(012) 393 2128

Your reference/U verwysing

My reference/My verwysing: 3/34/2

THE DIVISIONAL COMMISSIONER: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Enquiries/Navrae: Lt Col Joubert
AC Thenga
Tel: (012) 393 3118
Email: JoubertG@saps.gov.za

APPROVED

Ms MP Munyai
UNIVERSITY OF SOUTH AFRICA

PERMISSION TO CONDUCT RESEARCH IN SAPS: AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA: UNIVERSITY OF SOUTH AFRICA: MASTERS DEGREE: RESEARCHER: MP MUNYAI

The above subject matter refers.

You are hereby granted approval for your research study on the above mentioned topic in terms of National Instruction 1 of 2006.

Further arrangements regarding the research study may be made with the following office:

The Divisional Commissioner: Operational Response Services:

- **Contact Person:** Lt Col L Geyser
- **Contact Details:** (012) 400 6367
- **Email Address:** GeyserL@saps.gov.za

Kindly adhere to paragraph 6 of our Attached letter signed on the **2020-10-07** with the same above reference number.

MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

DATE: 2020-11-09

1

ANNEXURE M: Approval letter to conduct research from SARS

Office: Enterprise Research and Knowledge Management

Enquiries
Nozuko Twala
Dr Rebone Gcabo

Telephone
012 4227374

E-mail
_SecretariatRC@sars.gov.za

Reference
Request to use SARS data

Date: 15 February 2021

Mrs Mkateko Phillis Munyai

SARS
South African Revenue Service

Pretoria Head Office
299 Bronkhorst Street,
Nieuw Muckleneuk, 0181
Private Bag X923,
Pretoria, 0001

COMMUNICATION FROM THE SARS RESEARCH COMMITTTEE

Dear Mrs M P Munyai

REQUEST FOR ACCESS AND UTILISATION OF TAXPAYER INFORMATION FOR ACADEMIC RESEARCH PURPOSES

Thank you for submitting your research request to SARS for consideration for the topic, *"An assessment of security measures at the maritime ports of entry in Durban and Cape Town, South Africa"*.

The application was submitted to the SARS Research Committee and has been approved. The approval is conditional to adherence of the following:

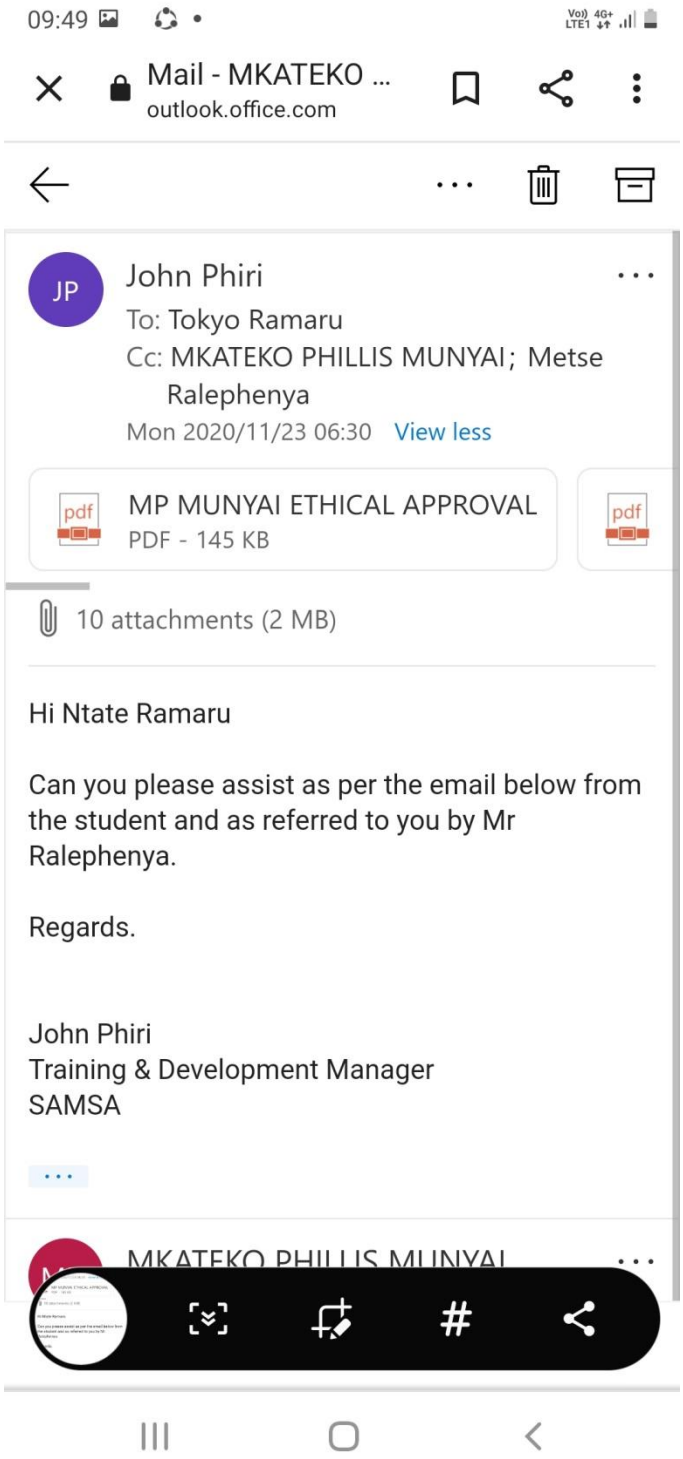
Data requirements:

A quantitative study by means of a semi- structured questionnaire. This will be distributed by SARS to the following sample as guided by the study.

PERSONNEL REQUIRED FROM CAPE TOWN SEAPORTPORT OF ENTRY	PERSONNEL REQUIRED FROM DURBAN SEAPORT OF ENTRY
6 X CUSTOM OFFICERS RESPONSIBLE FOR DAILY CLEARANCE OF GOODS AT THE SEAPORTS OF ENTRY.	6 X CUSTOM OFFICERS RESPONSIBLE FOR DAILY CLEARANCE OF GOODS AT THE SEAPORTS OF ENTRY.
THEIR SUPERVISORS X2	THEIR SUPERVISORS X2
THEIR MANAGERS/ASSISTANT MANAGERS X2	THEIR MANAGERS/ASSISTANT MANAGERS X2

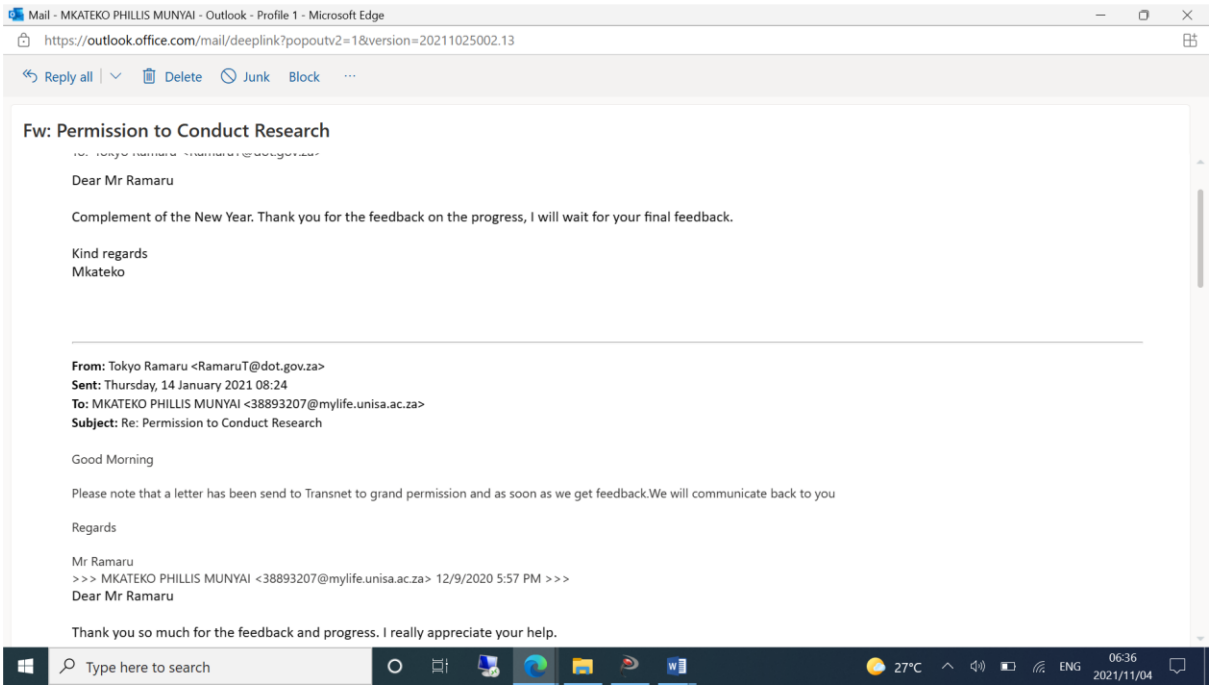
Please note that participant should be permanent officers who were working at the seaports of entry during the period of 1 January 2018 to 31 December 2018 up to date.

ANNEXURE N: SAMSA request for permission to conduct the research email to the NDoT

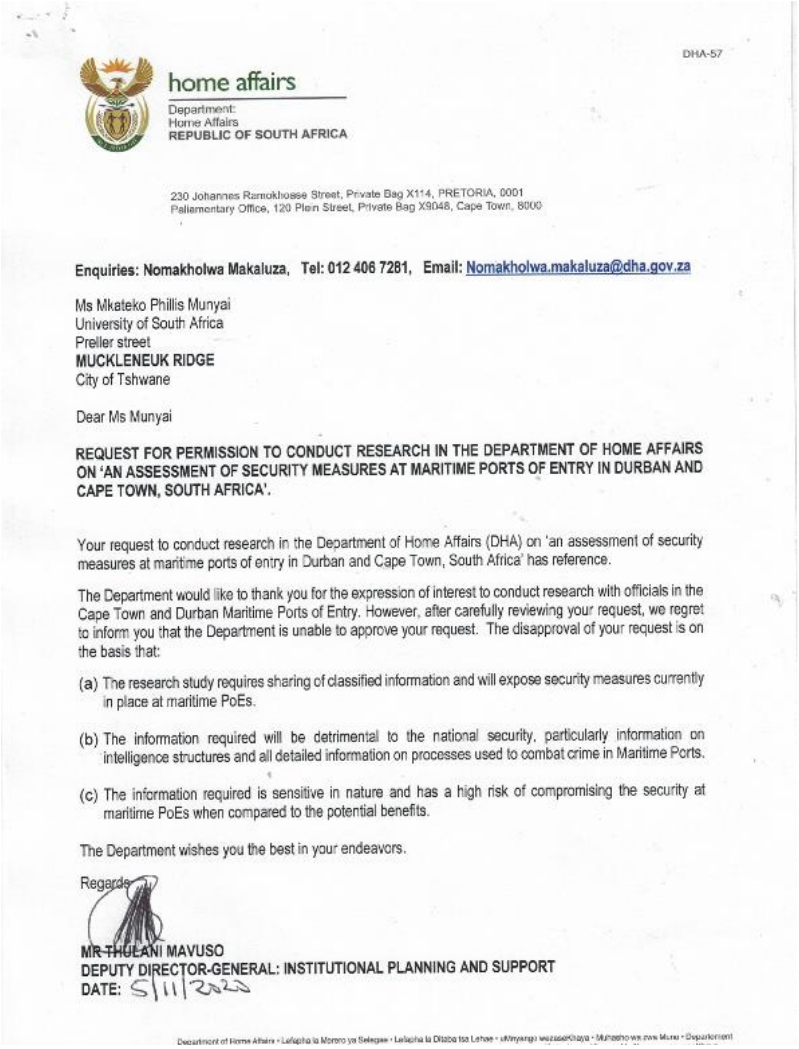


ANNEXURE O: National Department of Transport email to grant SAMSA permission

EMAIL MESSAGE FROM DEPARTMENT OF TRANSPORT



ANNEXURE P: Non approval letter to conduct research from DHA



DHA-57

home affairs

Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA

230 Johannes Ramokhoase Street, Private Bag X114, PRETORIA, 0001
Parliamentary Office, 120 Plein Street, Private Bag X9048, Cape Town, 8000

Enquiries: Nomakholwa Makaluza, Tel: 012 406 7281, Email: Nomakholwa.makaluza@dha.gov.za

Ms Mkateko Phillis Munyai
University of South Africa
Preller street
MUCKLENEUK RIDGE
City of Tshwane

Dear Ms Munyai

REQUEST FOR PERMISSION TO CONDUCT RESEARCH IN THE DEPARTMENT OF HOME AFFAIRS ON 'AN ASSESSMENT OF SECURITY MEASURES AT MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA'.

Your request to conduct research in the Department of Home Affairs (DHA) on 'an assessment of security measures at maritime ports of entry in Durban and Cape Town, South Africa' has reference.

The Department would like to thank you for the expression of interest to conduct research with officials in the Cape Town and Durban Maritime Ports of Entry. However, after carefully reviewing your request, we regret to inform you that the Department is unable to approve your request. The disapproval of your request is on the basis that:

(a) The research study requires sharing of classified information and will expose security measures currently in place at maritime PoEs.

(b) The information required will be detrimental to the national security, particularly information on intelligence structures and all detailed information on processes used to combat crime in Maritime Ports.

(c) The information required is sensitive in nature and has a high risk of compromising the security at maritime PoEs when compared to the potential benefits.

The Department wishes you the best in your endeavors.

Regards

MR THULANI MAVUSO
DEPUTY DIRECTOR-GENERAL: INSTITUTIONAL PLANNING AND SUPPORT
DATE: 5/11/2020

Department of Home Affairs • Lefapha la Moreo ya Selegae • Lefapha la Ditaba tsa Lehae • uMnyango wezaseKhaya • Muhasho wa zwa Mutse • Departement

ANNEXURE Q: Non approval letter to conduct research from SANDF

Good morning Madam

I managed to get an audience with the Acting Director Maritime Warfare this morning.

Captain (SA Navy) J.A. Verster informed me that the mandate for Port security, or even border security for that matter, does not rest with the South African National Defence Force anymore. We currently assist on the border, but the mandate rests with other government departments. The mandate for port security rests with the National Department of Transport.

I hereby regret to inform you that the SA Navy can therefore not grant or deny you permission to carry on with your paper.

I have attached a paper on Maritime Security that was written by one of my mentors. It has various references to Port Security and may assist you. (Apologies if you already have it).

I am sorry I could not have more of assistance.

Good luck with your studies and feel free to contact me if you need any further assistance from the SA Navy.

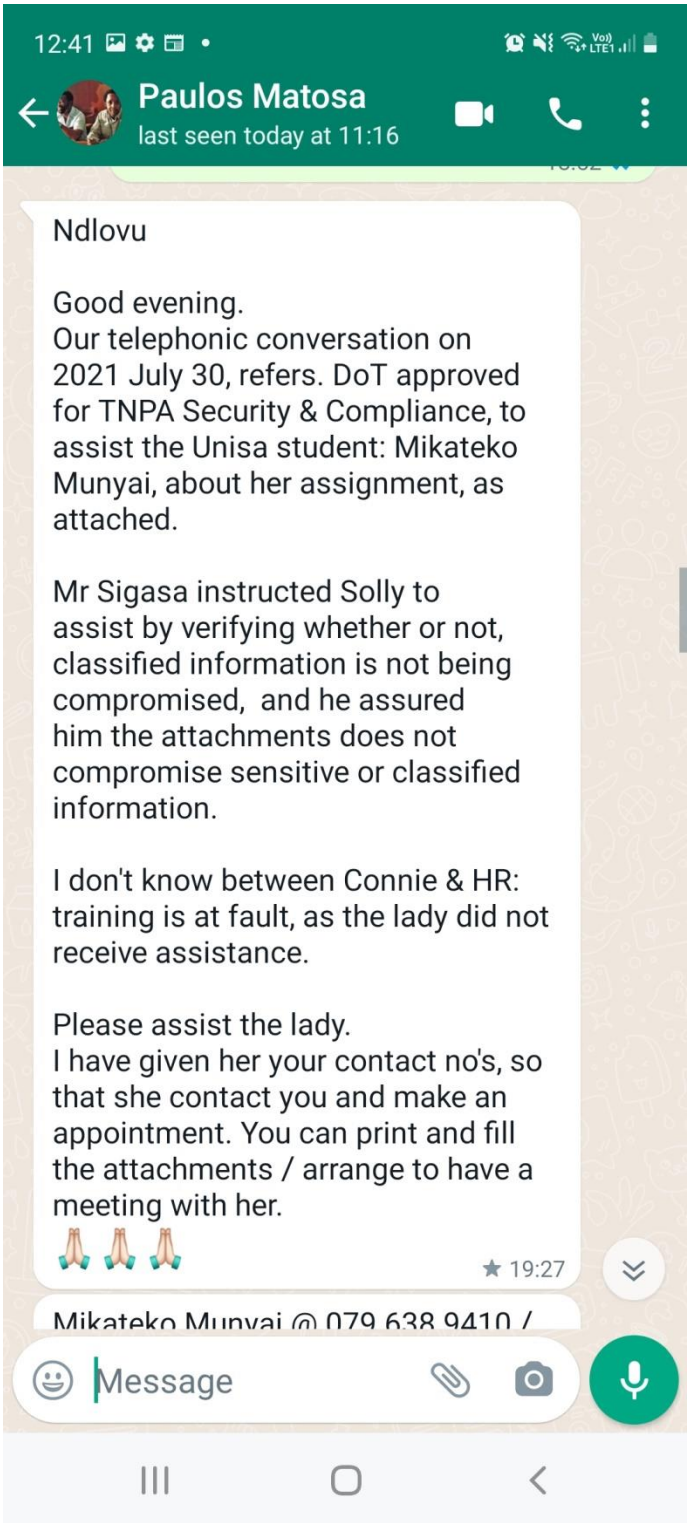
Kind regards

A Greyling

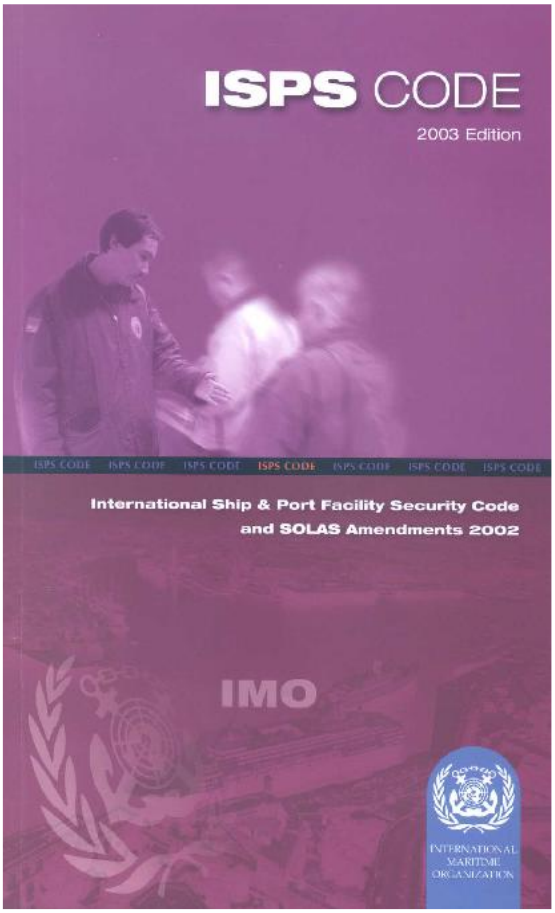
(A. GREYLING)

Commander Andre Greyling
SO1 Maritime Cooperation
SA Navy Headquarters
+27 12 339 4181
+27 84 983 3730

ANNEXURE R: Cell phone message from TNPA Security and Compliance Division to permit for purposive interview



ANNEXURE S: International Ship and Port Security Code



ANNEXURE T: Turnitin similarity report

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Mkateko Phillis Munyai
Assignment title:	Revision 2
Submission title:	AN ASSESSMENT OF SECURITY MEASURES AT THE MARITIME ...
File name:	MP_MUNYAI_DISSERTATION.docx
File size:	15.04M
Page count:	202
Word count:	48,746
Character count:	292,080
Submission date:	27-Sep-2022 01:50PM (UTC+0200)
Submission ID:	1910316836

AN ASSESSMENT OF SECURITY MEASURES AT THE MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

by

MKATEKO PHILLIS MUNYAI

Submitted in accordance with the requirements for the degree of

MASTERS

in the subject

CRIMINOLOGY

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR DORIVAL GOVENDER

SEPTEMBER 2022

ANNEXURE U: Language and technical editing confirmation letter

Barbara Shaw
Editing/proofreading services
18 Balvicar Road, Blairgowrie, 2194
Tel: 011 888 4788 Cell: 072 1233 881
Email: barbarashaw16@gmail.com
Full member of The Professional Editors' Guild

To whom it may concern

This letter serves to inform you that I have done language editing, reference checking and formatting on the thesis

AN ASSESSMENT OF SECURITY MEASURES AT THE MARITIME PORTS OF ENTRY IN DURBAN AND CAPE TOWN, SOUTH AFRICA

by

MKATEKO PHILLIS MUNYAI

Barbara Shaw

23/09/2022