AN EVALUATION OF SECURITY THREATS AND VULNERABILITIES TO A NATIONAL KEY POINT: CASE STUDY OF MEDUPI POWER STATION

by

ELIAS MOTHA THOKA

Submitted in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE

in the subject

SECURITY MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR:

PROF K PILLAY

February 2021

ABSTRACT

The theft of copper cable and working tools at Medupi Power Station is a serious concern. The aim of this study was to explore the occurrence of security threats and vulnerabilities at Medupi Power Stations as a National Key Point. An explorative qualitative research was used. Eighteen participants were selected purposefully. The data were collected using in-depth, semi-structured interviews conducted by telephone and tape recorder. Data were analysed using thematic data analysis. It was revealed that the common modus operandi used by thieves includes the smuggling of stolen goods, including copper. Among the causes of security threats and vulnerabilities are a lack of manpower to perform essential security functions. It is recommended that the theft of copper cable and working tools be prevented and various suggestions are provided. Future research should focus on addressing top management and management responsible for security to play a role in security functions and ensure that sufficient budget is allocated to the security functions.

Key Terms:

Security, threats, vulnerabilities, critical infrastructure, Eskom, Medupi, electricity, critical infrastructure protection

COPYRIGHT

DECLARATION

Name: Elias Motha Thoka

Student number: 33789169

Degree: Magister Technologiae in Security Management

AN EVALUATION OF SECURITY THREATS AND VULNERABILITIES TO A NATIONAL KEY POINT: CASE STUDY OF MEDUPI POWER STATION

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.

_ _____ 31 March 2021_____

SIGNATURE DATE

DEDICATION

This dissertation is dedicated to my late father Mosekate Alpheus Thoka who had so much faith in me and instilled in me from a tender age that I can be anything I want to be. May his soul continue to rest in God’s eternal peace.

To my late Grandfathers: Mr Mphela Piet Thoka and Mr Dihlasana William Mpyana.

To my Grandmothers: Mrs Morakana Rahab Thoka and Mrs Mmatlala Betty Mpyana.

To my late father's brother: Mr Mmutla Elias Thoka, Mokadikwa Emily Theka and my late sister Mokgadi Francinah Thoka.

May their souls rest in eternal peace. Dikwena and Ditlou.

ACKNOWLEDGEMENTS

I would like to thank Jehovah God Almighty for His wisdom, strength, perseverance and guidance that He bestowed upon me throughout the journey in completion of this dissertation.

My sincere thanks also go to the following people for their contributions towards this research project:

- A special word of thanks goes to my mother, Mrs Mabusha Thabitha Thoka, for giving birth to me at the first place and supporting me spiritually throughout my life.

- A special word of thanks goes to my wife, Mrs Magdeline Thoka, for the unrelenting love, support and encouragement she has shown me throughout this project. Not once did she complain about me paying too much attention to my studies. Therefore, I say thanks for everything and God give you all the best in return.

- A special thank you to my mother-law, Mrs Priscilla Maponya, for giving birth to my wife, for remembering me in her prayers and her loyal support during my studies. Ke a leboga kudu.

- A very special thanks to my daughter, Mabusha, and my son, Malea, for their endless love. Thank you for allowing me the time to focus on this study. The moments of loneliness and negligence that you experienced while I was busy compiling this research were not in vain. Your presence in my life encouraged me to work harder both academically and in my professional capacity.

- I would also like to express my sincere gratitude to my supervisor, Prof Krisranden Pillay, for always encouraging, supporting and guiding me throughout the study. The study could not have been a success without you Prof – Man of the moment – for stealing from your quality time with your family.

- A special acknowledgement to the Eskom for the unconditional permission to conduct this study.

- My editor, Mrs Barbara Shaw, for editing my research.

- My friend and fellow student, Obed phuti Mabelebele, and colleague, Elvis Lukhalimana, for motivating me when I wanted to quit my studies.

- My deepest thanks go to all the participants who contributed to this study. Your contribution to this study was not taken for granted.

- Lastly, thank you to the Research Directorate at UNISA for granting me support funding for my research activities.

LIST OF ABBREVIATIONS

CCTV	Closed Circuit Television
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CPTED	Crime Prevention Through Environmental Design
MO	Modus Operandi
NKP	National Key Point
UNISA	University of South Africa

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE
INTRODUCTION AND MOTIVATION FOR RESEARCH

1.1 Introduction

Power utilities produce energy and are regarded as essential infrastructure and their security needs to be evaluated with an intention to reduce vulnerabilities (Sadeghi, Jabbari, Alidoosti & Rezaenian, 2017:17). Benoit (2014:11) indicates that energy infrastructure provides energy continuously unless it is damaged or incapacitated. Most governments use the concept of Critical Infrastructure (CI) when describing systems and assets of high value to the community and economy (Robles, Choi, Cho, Kim, Park & Lee, 2008:17). Spellman and Bieber (2010:1) indicate that CI is any services and systems that are essential to the functioning of a society which, if compromised, would have an impact on the whole country. The energy infrastructure is critical to the country and therefore needs to be protected against any form of attack (Tweneboah-Koduah & Buchanan, 2018:1).

Amin and Giacomoni (2012:34) argue that the interconnection of infrastructure, such as energy, telecommunications, transportation and finance, creates a challenge because they need be secured, reliable and efficient in their operation. CI is exposed to different forms of threat, such as criminals or even terrorists (Tabansky, 2011:64), and it therefore needs to go through a threat and risk analysis process to select the best security measure/s to mitigate the risk (Federal Republic of Germany, 2009:9). CI, which includes resources such as the energy supply, power grid, water, sewerage and gas pipes, communications and transportation, among others (Tweneboah-Koduah & Buchanan, 2018:1; Holmgren, 2004:1), is important to the well-being of the public, organisations and the business community (Van Niekerk, 2011:59). Unguarded assets, cables, working equipment and inadequate security measures provide opportunities for crimes to be committed (Kimiecik, 1995:89; Kashiefa, 2014:1).

According to the Department of Public Enterprises (SA, 2019b),

> *"Eskom generates approximately 95% of the electricity used in South Africa and approximately 45% of the electricity used in Africa. Eskom*

generates, transmits and distributes electricity to industrial, mining, commercial, agricultural and residential customers and redistributors. Additional power stations and major power lines are being built to meet rising electricity demand in South Africa. Eskom will continue to focus on improving and strengthening its core business of electricity generation, transmission, trading and distribution. Eskom buys electricity from and sells electricity to the countries of the Southern African Development Community (SADC). The future involvement in African markets outside South Africa (that is the SADC countries connected to the South African grid and the rest of Africa) is limited to those projects that have a direct impact on ensuring security of supply for South Africa."

Eskom's Medupi Power Station, which is in Limpopo Province, is the fourth largest dry-cooled, coal-fired electricity generating power plant in South Africa and in the world (ESKOM, 2015:1). When Medupi is fully installed, the contracts for its boilers and turbines will be the highest in electricity generation in South Africa. When fully operational, each of the six boilers will have an 800-megawatt output supplying 4 800 megawatts to the national electricity grid daily. Medupi Power Station has a planned operational life of 50 years (SA, 2019a; Kusile & Medupi Power Stations, 2017). For this period, the power station needs properly evaluated and updated security measures to pinpoint weaknesses or shortcomings in its security system.

This study focused specifically on evaluating the threats and vulnerabilities at the Medupi Power Station and not on general security issues facing Eskom in the country. The study examined the existing security measures implemented at the Medupi Power Station (as a National Key Point/Critical Infrastructure), to identify current security threats and weaknesses (possible shortcomings) in those security measures; and to investigate the gaps in the existing security measures. In addition, the study assessed the security measures as implemented at the Medupi site and evaluated the protection of the operations for the generation of electricity. The researcher uses the term "Critical Infrastructure" (CI) instead of "National Key Point" (NKP), since the National Key Points Act 102 of 1980 (SA, 1980) has been repealed and replaced by the Critical Infrastructure Protection Bill of 2007 (CIP) (Mbalula, 2017:48). Since then, the Critical Infrastructure Protection Act No. 8 of 2019 was

passed into law on 28 February 2019.

This chapter discusses the rationale for the study and the research problem. This includes the research questions and the aims and objectives of the research together with key definitions, theoretical concepts, and an outline of the chapters of the dissertation.

1.2 Background to the study

The study focused on the evaluation of threats and vulnerabilities of the Medupi Power Station in the Limpopo Province, a National Key Point in South Africa. Between 2007 and 2016, Medupi Power Station has experienced high crime rates that include the theft of cables and on-site equipment (Dzansi, Rambe & Mathe, 2014). The study was conducted as a result of improper protection of national key points (NKPs) and strategic installations in South Africa (Sovacool, Benjamin & Rafey, 2011).

The main purpose of the National Key Points Act 102 of 1980 (SA, 1980) was to protect all areas of national strategic importance against sabotage. Furthermore, in South Africa, a problem arose in 2015 when breaches at a National Key Point were not declared until after the Johannesburg High Court ruled in favour of the Right2Know Campaign (Right2know, 2015:np). In its judgment, the court directed the SAPS to reveal the list of protected areas within a period of 30 days. In this case, a key problem arose in the application of the National Key Points Act 102 of 1980 (SA, 1980), which dated back to the apartheid government. It was argued that the National Key Points Act 102 of 1980 (SA, 1980), which was being used and applied by the government for decades after the abolishment of the apartheid system, was not in keeping with democratic principles of the new government.

The current South African government repealed the National Key Points Act 102 of 1980 (SA, 1980) and replaced it with the Strategic Installation Bill, 2007 and the Critical Infrastructure Protection Bill in 2017. The Critical Infrastructure Protection Act No. 8 of 2019 was signed into law by the President of the Republic of South Africa on 28 November 2019. The purpose of the legislation is to recognise that specific infrastructures are essential for public safety, national security and the uninterrupted

provision of basic public services. Therefore, the CIP Act 8 of 2019 requires that proper systems should be developed and implemented to safeguard critical infrastructure and provides for the identification and declaration of infrastructure as critical (SA, 2019c).

In South Africa, the Energy supplier, Eskom, is part of Critical Energy Infrastructure that is obliged to ensure that it continues to function properly even in adverse conditions (European Academy, 2011:2). This is an indication that Eskom's core business of providing essential services to South African citizens must be protected against any forms of threats and vulnerabilities. This study focused on the security threats and vulnerabilities at Medupi Power Station which, as a result of criminal activities, can cause disruption to the provision of electricity services to South African citizens.

1.3 Rationale for the study

The study was undertaken due to the increase in crime rates at the Medupi Power Plant which occurred as a result of security risks and vulnerabilities facing the power generation utility. Medupi is considered to be one of the major infrastructure build projects initiated by the South African government to provide a reliable supply to the electricity grid of the country. The rate of crime at Medupi Power Station for the period 2013 to 2017 has fluctuated according to statistics provided by the South African Police Services. The graph below provides the statistics of thefts that took place during this period at Medupi Power Station.

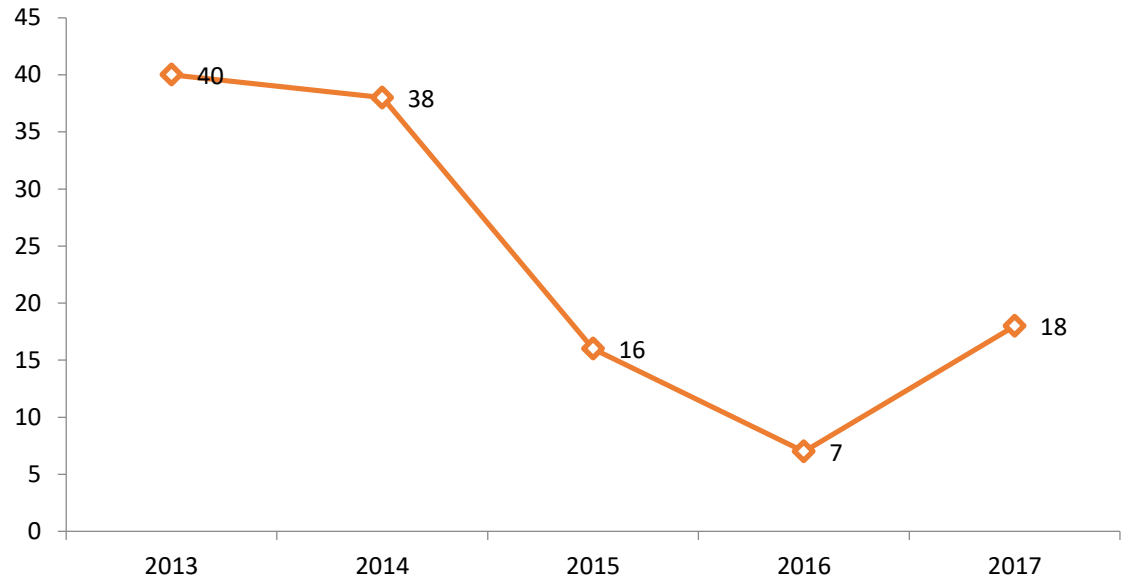


Figure 1: Total number of cases reported at Medupi as General Theft cases from 2013-2017

Source: South African Police Services, 2013–2017.

From the statistics provided by the South African Police Service (SAPS), there were 119 cases of theft reported in a five-year period between 2013 and 2017 with a slight increase in 2017 from 2016. It is clear from the above graph that Medupi Power Station is been a target for criminals who commit crimes on different properties, ranging from generator transformer theft, cable theft, malicious damage to property, housebreaking, security breaches and theft of vehicles. These crimes have cost implications for the power station, which can impair its operations making it vulnerable and unable to attain its strategic objectives.

The rates of crimes, such as industrial sabotage, contribute to the deterioration of a power plant (Peters, 2011:13). A report in Fin24 (2015:np) confirmed that Eskom suspended operations at Medupi Power Plant in order to safeguard property and employees after the National Union of Metalworkers of South Africa (Numsa) went on strike (Fin24, 2015:np). Furthermore, dissatisfied employees can cause acts of sabotage to the power station by bringing in things that could damage the plant, such as bombs and loose bolts, or by taking out essential parts of the machinery to cause turbine failure or other obstacles Fin24 (2015:np).

Consequently, the community, businesses and other government infrastructure

suffer losses as a result of the power failure caused by sabotage at the power station. The location of a National Key Point in this case, bordering on residential areas, leaves the power plant vulnerable to violence, cable theft, burglaries and other crimes which endanger the security of National Key Points (Rantao & Bailey, 2011).

The research sought to identify problems by identifying hazards, risks and vulnerabilities at the power station to ensure effective and uninterrupted operations. The researcher applied assessment methodology to identify risks and vulnerabilities and to make recommendations that will assist the power station in reducing the risks to a continuous supply of electricity.

1.4 Problem statement

The importance of protecting the CI has been long recognised (Van Niekerk & Manoj, 2011). However, in South Africa, the government has not shown an interest in developing the relevant legislation, although they have relied on the old National Key Points Act 102 of 1980 (SA, 1980) to safeguard national key points in the country. This was evidenced by delays in repealing the old National Key Points Act 102 of 1980 (Van Niekerk & Manoj, 2011). The Critical Infrastructure Protection Act 9 of 2020 which replaced the Critical Infrastructure Protection Act No. 8 of 2019 and the old National Key Points Act 102 of 1980 (SA, 1980) makes provision for the necessary protection of Critical Infrastructure (CI) due to the fact that they provide essential services such as water and electricity which, if interrupted, can affect the power plant itself as well as the surrounding community and businesses.

Crimes, such as the theft of property, at Medupi Power Station eventually affect the economic growth of South Africa as they disrupt normal supplies and hinder job creation. Cable theft is not only a South African occurrence and has become a scourge worldwide. For example, countries such as the UK, USA, China, India, Russia, Kenya and Nigeria have experienced severe increases in cable theft in the last few years (Department of Energy, 2018:np). This motivated the researcher to conduct a study to determine the security threats and vulnerabilities that expose Medupi Power Station as a National Key Point to crime. Generally, security measures of National Key Points should be equivalent to the value of the assets that

are protected. That means that if Medupi Power Station wants to improve security measures to protect its property, a security risk assessment should be done to establish the nature and extent of threats and vulnerabilities confronting its operations.

Medupi Power Station has seen an increase in the rate of crimes in recent years. Statistics have indicated that a high crime rate in Lephalale, where the power station is located, has made the power station susceptible to attacks by criminals. This has particularly affected Eskom and the on-site contractors. Criminals steal physical items, such as copper cables, equipment and fiscal assets, inside and outside the power station which has a negative impact on the surrounding community and other critical infrastructures (Kjolle, Utne & Gjerde, 2012:1).

Rakoma (2016:np) points out that, although crime statistics in some areas around the site might decrease, the financial impact of these losses would increase as the actual financial loss suffered by the company would be severe. South Africa, like many other countries around the world, has experienced economic instability due to crimes and violent acts perpetuated against companies that threaten the employers and the employees, and damage the viability of the business (Mahambane, 2017:3).

Violence and crime against power stations hampers the delivery of electricity which affects human rights (De Klerk, 2014). Delivery trucks entering and leaving National Key Points become targets for crimes perpetuated against the National Key Points and its employees (Kimiecik, 1995:178). Security companies and security guards who provide security services but are not vetted pose a security threat at National Key Points (Purpura, 2013:136). These companies and their employees should go through security checks before they provide such services to identify potential security breaches (Greggo, 2011:20).

Based on the above-mentioned factors, the research problem sought to consider the level of security threats and weaknesses occurring at Medupi Power Station.

1.5 Research aim and objectives

1.5.1 Aim of the study

This study aims to evaluate levels of threat to security facing the Medupi Power Station as a Critical Infrastructure, in order to improve the existing security measures at the power plant.

1.5.2 Objectives of the study

Based on the aim, this study explored the security threats and vulnerabilities at Medupi Power Station, as a National Key Point, by focusing on the objectives below:

- To evaluate the nature and range of security threats and vulnerabilities at Medupi Power Station;
- To identify the security threats and vulnerabilities at Medupi Power Station that have caused the increase in crime at Medupi Power Station;
- To evaluate the current physical security systems in place at Medupi Power Station;
- To consider strategies for reducing security threats and vulnerabilities at the power utility.

1.6 Research questions

The following research questions served as guidance throughout the research process:

- What are the security threats and vulnerabilities confronting Medupi Power Station in the Limpopo Province?
- What security measures are currently in place at Medupi Power Station?
- What should be done to improve security measures at Medupi Power Station?

1.7 The value of the research

The study is deemed important since the findings will contribute to the identification of the security threats and vulnerabilities at Medupi Power Station, a Critical Infrastructure facility. It is envisaged the research will improve security measures at Medupi Power Station which will ensure that the power station conducts its day-to-day business with reduced threats and vulnerabilities. It will add value to the lacunae of up-to-date research on threats and vulnerabilities facing power utilities.

The research findings of the study will benefit society as threats and vulnerabilities will be identified and dealt with for the betterment of the community by maximisation of public interest and social justice. The researcher will benefit by becoming knowledgeable and experienced in the field of CI. The research will be of value to the community by increasing job opportunities in order to enhance social responsibilities. UNISA will benefit through increased throughput. The researcher will write articles which will be published in accredited journals.

In summary, the following stakeholders will benefit from the study:

- The value to the researcher: The researcher will benefit from this research by acquiring skills, experience and achievement of academic qualifications;
- The value to the UNISA: The University had benefited through increase in the research throughput and presentation of findings at various platforms when required;
- The value to the security industry: The industry will benefit from the research findings by becoming aware of the kinds of threats and vulnerabilities at Critical Infrastructure;
- The value to the academic society: Academic society will benefited through the methodological dimension as well as theoretical framework used in this study;
- The value to the business and community at large: Both the business community and the community benefited through uninterrupted supply of electricity.

1.8 Definition of key theoretical concepts

1.8.1 National Key Point

According to the National Key Points Act 102 of 1980 (SA, 1980), a National Key Point is defined as “any place or area, which has under section 2 of the National Key Points Act 102 of 1980 (SA, 1980) been declared a National Key Point”. National key points include the Union Buildings, strategic installations, such as provincial legislatures, airports and power stations, and other buildings that require tight security to prevent damage or acts of sabotage (Hi-Tech Security, 2007:np). The following are examples of National Key Points in South Africa: the Union Buildings, OR Tambo International Airport, Legislations, SABC, Eskom National Control Centre at Simmer Pan, Matla Power Station, Duvha Power Station, Mokolo Pump Station, Matimba Power Station, Medupi Power Station, Koeberg Nuclear Power Station, Cape Town International Airport, among others.

1.8.2 Critical Infrastructure (CI)

The term “Critical Infrastructure” is defined by Tweneboah-Koduah and Buchanan (2018:2) as “large-scale socio-technical systems which provide services to the society which is important in its proper functioning”. According to Bergerbest-Eilon (2009:13), CI is a complex of interdependence, which requires a systematic approach. However, Spellman and Bieber (2010:1) indicate that CI consists of services and systems that are essential to the functioning of a society and which, if compromised, would render a serious impact on the whole country. For example, Eskom power failures as a result of criminal activities impact negatively on businesses, government and society in general. According to Mäkinen (2016:10), CI includes all “the functions and structures that are important to maintain the functions of the community”.

1.8.3 Critical Infrastructure Protection (CIP)

The term “Critical Infrastructure Protection” includes all forms of security and systems infrastructure used for the proper and effective running of the society (Schneidhofer & Wolthusen, 2015:2). However, Mäkinen (2016:11) indicates that CIP incorporates all the activities that are purposefully intended to confirm their

continuity, functionality and their integrity to reduce vulnerabilities and risks.

1.8.4 Infrastructure

According to Tabansky (2011:62), infrastructure is critical when its disruption leads to socioeconomic disturbances, which undermine the stability of the community. The criticality of infrastructure is when it plays a major role in society and its disruption collapses the whole system (Federal Republic of Germany, 2009:5). Critical Infrastructure is further defined as “any building, centre, establishment, facility, installation, pipeline, premises or systems required for the functioning of society, the Government or enterprises of the Republic” and includes consumer installations, major hazard installations, nuclear installations and offshore installations, among others.

1.8.5 Security

Purpura (2011:5) defines security as “the state of being safe from threat, terror or nervousness”. Nkwana (2015:6) defines security as the application of economic security measures that, when engaged as a whole, decrease the possibility of loss-incurring events or decrease the effect of loss-incurring events that happen in any given area. According to Minimum Information Security Standards (MISS) Chapter 2 (1998:15), security is defined as that situation that is free of threats or vulnerabilities to lives, property and data generated by the establishment and use of protective security measures. National security, which includes peace, stability, development and progress, incorporates not only the lack of threats, risk or danger, but also includes the basic principles and fundamental values related “to the quality of life, freedom, justice, prosperity and development” (https://www.gov.za/documents/intelligence-white-paper). When looking at the above three definitions from various authors the concept security strives for safety from threats and vulnerabilities that can affect a particular area and in this instance that is the Medupi Power Station as one of the National Key Points area.

1.8.6 Physical security

Physical security is defined as “security of people, property and amenities by making usage of security services, security systems and security techniques” (Purpura,

2001:262). Rouse (2014:np) regards physical security as “the security of personnel, hardware, programs, systems, and information from physical environments and proceedings that could affect severe losses or damage to a business, group, or establishment”. Physical security settings encompass fires, disasters, burglaries, thefts, vandalism, and violence. Fisher, Halibozek and Green (2008:31) explain that the concept of “security” includes “a steady, comparatively foreseeable environment in which an individual or group may follow its ends without disturbance or damage and without fear of trouble or injury”.

1.8.7 Security assessment

Security assessment is the process of gathering information about the risks; this is done by conducting interviews with key employees that are tasked to manage CI, reviewing existing documents and systems with the intention of comparing them with the available standards (Abouzakhar, 2013:7).

1.8.8 Security risks

According to Kole (2015:12), security risks include “the probability of suffering damage or loss, disclosure to the likelihood of loss or damage, a constituent of doubt, or the prospect that affects an act that may not be consistent with the envisioned or expected results”. Mahambane (2017:5) defines security risks as the “prospect of distress maltreatment or loss, revelation to the chance of loss or harm, an element of uncertainty, or the chances that effects an action that may not be consistent with the envisioned or expected results”.

1.8.9 Security Vetting

This refers to “the methodical procedure of investigation followed in determining a person's security competence” (MyHR, 2014:np). Security vetting is also “the scrutiny of the previous and background of constructive candidates and prevailing workforces” (Minimum Information Security Standards, 1998:17). Therefore, for most security positions, screening includes criminal record investigations for previous convictions, penalties and outstanding charges.

1.8.10 Security measures

Van Jaarsveld (2011:5) states that security measures are intended to “thwart, limit and recuperate security-related losses”. According to Mahambane (2017:5), security measures designate all the security measures that must be put in place in order to preclude, confine and recuperate security-associated losses. For the purpose of this study, security measures include the security of people, technology, procedures, policy and physical security aids.

1.8.11 Security officer

The Private Security Industry Regulation Act 56 of 2001 (SA, 2001), defines a security officer as any ordinary individual “who is employed by another person, including an organ of State, and who receives or is entitled to receive from such other person any remuneration, reward, fee or benefit, for rendering one or more security services”. Furthermore, the act defines security officer as a person

> *“who assists in carrying on or conducting the affairs of another security service provider, and who receives or is entitled to receive from such other security service provider, any remuneration, reward, fee or benefit, as regards one or more security services” (SA, 2001).*

1.8.12 Security survey

A security survey is defined as

> *“a critical on-site examination and study of an industrial plant, business, home, or public or private institution in order to establish the current security status, identify deficiencies or excesses, determine the protection needed, and make recommendations to improve the overall security” (Fennelly, 2013:41).*

Adding to the above-mentioned definition, a security survey also refers to “an instrument used to physically study sites and valuations of all security systems and techniques in order to discover any vulnerability. It is further used to lessen risks” (Dempsey, 2008:61).

1.8.13 Security threats

The Business Dictionary (2018a) defines security threats as

> *"an undesirable occurrence that can cause a risk to become a loss, articulated as an aggregate of risk, consequences of risk, and the probability of the incidence of the occurrence. Additionally, a threat may be a normal occurrence such as an earthquake, flood, storm, or a fabricated incident such as burglary, theft, malicious damage to property, fire, power failure, sabotage, etc."*

1.8.14 Threat

According to Christopoulos (2013:19), threat is defined as "natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property".

1.8.15 Vulnerability

According to Mahambane (2017:6), vulnerability is defined as "the degree to which people, property, resources, systems, and cultural, economic, environmental, and social activity is prone to damage, dilapidation, or destruction on being exposed to an hostile factor". This means that assets, such as working tools, may be vulnerable to theft caused by a lack of security measures.

1.8.16 Vulnerability assessment

The Vulnerability Assessment (VA) is a proactive strategy for improving infrastructure security and its ability to provide the necessary information that may be used during the Risk Assessment process (Drago, 2015:10). According to Christopoulos (2013:19), vulnerability is the weaknesses that result in success of crime prevention.

1.8.17 Access control

HiTech Solutions (2007:62) explains access control as the process whereby

> *"people are granted or denied access to restricted areas, such as office*

suites, storage facilities, or parking garages. Office buildings can either house individual tenants and companies in a multi-use property, or be owned and occupied by a single company. Varying degrees of access are required depending on use, and administration of access control for personnel can be distributed amongst several individuals".

Access control is also defined as the control of things moving into and out of a building or another area (Fay, 2010:161).

1.9 Conclusion

This chapter provided an introduction, highlighted the rationale, problem statement and clarified the aims, objectives and benefits of the study. This research is for the benefit of CI protection and describes ways of improving the basic acts, as provided in section 1.7 above, which is backed up by literature and national legislation. This study of the security of Medupi Power Station in the Limpopo Province, a critical infrastructure, will enable it to prevent financial loss, infrastructural degradation and give the surrounding community and businesses access to basic amenities. The qualitative data from this study has been analysed to improve the protection of public infrastructures such as the Medupi Power Station in the Limpopo Province.

1.10 Outline of the dissertation

Chapter One: Introduction and Motivation for the Research

This chapter discusses the rationale for the study, problem statement, research questions, research aims and objectives, key definitions and theoretical concepts and definitions used in the study.

Chapter Two: Research Methodology

This chapter discusses the research methodology, the research approach, design, data collection instruments, data collection, data analysis, reliability and validity of the study as well as the limitations of the research.

Chapter Three: Literature Review on Security at National Key Points

This chapter provides a review of literature. This involves discussing the theoretical areas, interpretation and analysis of previous research done in the field of security for National Key Points.

Chapter Four: Data Analysis and Research Findings

The findings of the research are analysed based on the research information gathered during the collection methods applied in the study.

Chapter Five: Conclusion and Recommendations

This chapter consists of a summary and conclusion of the main findings of the study and provides recommendations and suggestions for future research.

CHAPTER 2
RESEARCH METHODOLOGY

2.1 Introduction

This chapter provides an overview of the research approach and design used in the study. It also discusses the population and sampling, pilot study and data analysis. The chapter discusses the validity, reliability and ethical considerations for the study and the limitations and value of the study.

2.2 Research approach

According to Kumar (2014), “a research approach outlines the techniques, procedures, philosophies and methods that a researcher will follow to achieve the research objectives”. The research approach for this study was explorative . Explorative research is aimed at gaining an insight and familiarity for later investigation and to use for further research (Sastry, 2013:110). The reason for using explorative research is that the researcher was able to ask the research questions and probe the participants for their knowledge of security threats and vulnerabilities at Medupi Power Station.

2.3 Research design

The researcher employed a qualitative research design for this study because the topic under study was not exhaustively researched and there is limited information on National Key Points as a topic. Research design is a way of designing and conducting an investigation (Creswell, 2014). On the one hand, Fowler and Aaron (2010) describe a research design as “a complete practical strategy for obtaining trustworthy solutions to the questions that have been propounded for the study; and for handling some of the difficulties that could be encountered during the research process”. On the other hand, Creswell (2013:44) indicates that qualitative research “begins with assumptions and the use of interpretive/theoretical frameworks that inform the study of research problems addressing the meaning individuals or groups ascribe to a social or human problem”. Qualitative research differs from quantitative research in that it does not use numerical illustration but focuses on having a

thorough understanding of the problem that the research is investigating (Jugder, 2016:370). Sastry (2013:105) indicates that the importance of a research design helps the researcher to properly address concerns in the research and it provides guidance to the research in order to fill inaccuracies which were found during procuring of the data.

2.4 Population and sampling

2.4.1 Population

A population is a group of units from which samples are drawn in order to conduct research (Guest, Namey & Mitchell, 2013:42). Melville and Goddard (2001:34) define population as “any group which is the subject of research study”. The population in this study included all employees that render a security service at Medupi power station.

2.4.2 Sampling

Bless and Higson-Smith (2000:83) define sampling as

> *“the process of selecting the sample from a population in order to obtain information regarding a phenomenon in a way that represents the population of interest and to allow for an accurate generalisation of results”.*

This research employed purposive sampling as he only selected participants who had knowledge and experience of security threats at Medupi Power Station. Brink and Wood (1998:221) indicate that an alternative name for purposive sampling is “judgmental sampling” because samples are chosen for a specific purpose in a research study (Leedy & Ormrod, 2010:212). Thus, the sample for this study consisted of 30 individuals from the total population of 371. Only eighteen (18) participants agreed to participate and included senior security managers, security officers, crime investigation officers, security business intelligence officer, security technology officer, security inspectors, and contracted security service providers.

2.5 Pilot study

Prior to the conducting of the project, the researcher conducted a pilot study to test the research questions in order to determine whether they would yield the anticipated results and also to modify them to ensure that they did not confuse the participants. A pilot study is important to improve the quality and efficiency of the study (Hazzi & Maldaon, 2015:53). It provides the methodological evidence about the research design, planning and justification of a pilot study (Blatch-Jones, Kirkpatrick & Ashton-Key, 2018:1). According to Doody and Doody (2015:1074), a pilot study "contributes valuable information to assist a researcher in the conduct of their study". The other reasons for conducting a pilot study were that the researcher was able to test how the questions were answered by the participants. The researcher randomly selected a small sample of five respondents to conduct a pilot study before the main study was conducted. A pilot study was a useful exercise for the researcher to refine data collection questions (Ishmail, Kinchin & Edwards, 2018:4).

2.6 Data collection

The research approach for the study was qualitative in nature and the process of collecting data is indicated below:

2.6.1 In-depth, individual interviews

According to Queiros, Faria and Almeida (2017:378), in-depth interviews provide the researcher with an opportunity to ask follow-up questions, probe the respondent for additional information, justify what was already discussed and establish a connection between different topics in the discussion. An in-depth interview uses direct questions which are used to elicit detailed information from the participants (DiCicco-Bloom & Crabtree, 2006:315).

2.6.2 Semi structured interviews

Semi-structured interviews use non-standardised questions (Torkar, Zimmermann & Wilbrand, 2011:45). This means that semi-structured interviews involve a combination of structured and unstructured questions. An interview schedule was

used by the researcher when facilitating the interviews. In the semi-structured interviews, useful information was obtained through a two-way communication with the research participants (Pathak & Intratat, 2012:4). During the interviews with the participants, the researcher assured the participants that their privacy and confidentiality issues would be respected in terms of the Policy on Research Ethics (UNISA, 2016). Interviews were conducted in a quiet place to ensure that the participants were not distracted from the communication with the researcher. The interviews were recorded on an electronic device. The research interviews were facilitated through the use of an interview schedule which mainly focused on the research problem and research questions of the study in order to probe the participants on the threats and vulnerabilities at the Medupi Power Station.

When conducting interviews, the researcher wrote down notes which were written in the presence of the participants to ensure that the participants were not coerced. This means that the research did not influence the participants to give detailed answers to research questions. No leading questions were asked of the participants as this would have had a negative influence on the results of this research.

The researcher formulated detailed research question prior to conducting semi-structured interviews (Pathak & Intratat, 2012:4). According to Kallio, Pietila, Johnson and Kangasniemi (2016:4), a good quality interview guide used during semi-structured interviews yields positive results. The researcher used open-ended questions which were posed to the participants and they provided the researcher with an opportunity to probe the participants about the subject matter.

2.7 Data analysis

Parahoo (2006) indicates that “data analysis was a cohesive part of research design and it is a way of making sense of data before presenting them in an understandable manner”. Data analysis is a “disintegration of data into controllable themes, patterns, trends and relationships” (Mouton, 2001:108). In a qualitative methodology, data analysis includes taking the interview transcripts together with observation notes and non-textual material collected and systematically sorting and arranging the data to gain a deeper understanding of the phenomenon under study. The researcher is certain that the interview questions did not mislead the participants. In order to

ensure that the data analysis method was valid, the researcher has used Thematic Analysis techniques that were tested by different authors, such as Braun and Clarke (2006), as discussed below:

2.7.1 Thematic Analysis (TA)

Data were analysed using the Thematic Analysis (TA) process that is defined as “a method for systematically identifying, organising and offering insight into, patterns of meanings across a dataset” (Braun & Clarke, 2012:22). Data analysis involves preparation and organising the data and then the thematic reduction of data by carrying out a process of coding and contracting the codes (Creswell, 2013:180). Nowell, Morris, White and Moules (2017:2) contend that TA is normally used to answer qualitative research questions.

According to Braun and Clarke (2013:120), TA is very important in identifying and analysing patterns in the data. TA develops classification and themes that are related to the data (Ibrahim, 2012:40). Jugder (2016:3) believes that TA complements the research questions.

2.7.2 Six phases of thematic analysis

The following are the six steps used to analyse the collected data (Braun & Clarke, 2006):

1) **Familiarisation with the data:** When the researcher reads and re-reads the transcripts, he/she will become familiar with the data. This includes replaying the audio-tapes and going over the field notes several times.

2) **Coding:** During data analysis, the researcher generates concise labels for important features of the data. The end-product of this process is to collate all the codes and relevant extracts from the data.

3) **Searching for themes:** Searching for the codes happens when the researcher looks for the similarities in the data, however, such codes must be relevant to the research questions of the study. All the codes related to the theme are collated by the researcher.

4) **Reviewing themes:** This involves the checking of the themes based on the coded extracts and the full data set. Of importance is that the researcher will look at any theme that is convincing about the data. In some cases, themes may be separated or merged.

5) **Defining and naming themes:** Once the researcher has conducted a detailed analysis of the data, he/she will be in a better position to define and name the themes.

6) **Writing up:** Once the themes have been defined and named, the last step of the process is to write up the report based on the analysis. In this step, the researcher is able to narrate a story based on the extracted data (Braun & Clarke, 2006).

2.8 Measures used to ensure validity

Trustworthiness is considered as the overarching evaluative standard for field research (Sango, 2013). This requires conducting a research and presenting the study in a way that the reader can believe the results and be convinced that the research conducted was worthy. In this study, the objectives of the study and the knowledge collected during the literature review ensured that the interview questions represented national and international literature research findings regarding the assessment of security threats and vulnerabilities.

Validity refers to the trustfulness, accuracy, authenticity, genuineness and soundness of a study (Delport & Roestenburg, 2011:171). Also, validity means that the data has revealed accurate or error free conclusions (Lani, 2009:3). According to Van Niekerk (2015:11), validity in research ensures that the research is based on quality data and their interpretations.

Researchers mostly ascertain the validity of a study by asking a number of questions, and finding the answers in the research of previous researchers. Dantzker and Hunter (2012:53) classify validity into four parts, namely, face, content, construct and criterion validity. To ensure that validity is achieved, a pilot study is conducted in order to test the research instruments for content and construct validity (Dikko, 2016:521). In the face of validity, the judgement of the researcher played a role as

the interview questions measured what the researcher wanted to measure. Similarly, criterion validity was achieved by ensuring a good relationship between the interview schedule and the result of the findings. The researcher carried out both the internal and external validity of the research instrument in order to make the research study scientifically reliable and trustworthy. In this study, the researcher confirmed that the research instruments that were presented to the participants allowed them to give consistent answers.

2.9 Measures used to ensure reliability

The reliability of a study is the act of constructing the same results on continuous conditions. The accounts provided by other researchers have pronounced reliability as the level to which results were dependable over time and a true idea of the whole population that was investigated and whether the study was able to be reproduced under the same conditions (Delport & Roestenburg, 2011). Reliability was also ensured since the measuring instruments that were used in the research study yielded consistent results when repeated by other researchers.

Open-ended questions using in-depth, individual, semi-structured interviews were used. This enabled the researcher to focus on asking questions that were on the interview schedule. The researcher used the same interview schedule for all the participants. Prior to conducting semi-structured interviews with the participants, the researcher guaranteed their confidentiality and privacy. The researcher did not ask leading questions during the interviews with the participants.

2.10 Ethical considerations

According to De Vos, Strydom, Fouche and Delport (2011:115), research ethics is defined as “a set of moral principles which offers rules and behavioural expectations about the most correct conduct towards participants, organisations and or sponsor”. Research ethics requires that, during data collection, the researcher should respect participants’ privacy, rights, integrity and confidentiality.

To ensure that the study was ethically acceptable, the researcher complied with the University of South Africa Policy on Ethics. This means that the researcher first applied for ethical clearance prior to conducting the study. The researcher also

sought written consent from the head of security to carry out the research in the limits of the study area. In conducting this research, the researcher complied with the following ethical principles (UNISA, 2016):

- **Protection of and respect for the rights and interests of participants and organisations**

The researcher showed respect for and safeguarded the dignity, privacy and confidentiality of both the participants and UNISA. This was done by ensuring that personal information of the participants was not shared with any other person. They participated of their own free will and the taped materials were destroyed after three months. In other words, no information related to the participants was exposed to any person or organisation for profit or personal gain. This means that the data were only collected for the purpose of an academic qualification.

- **Informed and non-coerced consent**

Participants participated in the study voluntarily without being coerced. This was done by designing an informed consent form which was signed by the participants who were also informed that their participation in this research was voluntary (Dongre & Sankaran, 2016:1191). Informed consent means that the researcher has a responsibility to make sure that participants are aware of the different phases of the research (Sanjari, Bahramnezhad, Fomani, Shoghi & Cheraghi, 2014:3).

- **Respect for cultural differences**

The researcher respected the cultures of other participants. The researcher requested permission from individuals to interview them. The study involved participants from different cultures such as Zulu, Xhosa, Pedi, Tsonga, Venda, Ndebele, Sotho and Tswana. The researcher, as an Eskom employee, which is a diversified organisation, was thus was able to conduct the interviews fairly and in a consistence manner.

- **Justice, fairness and objectivity**

The researcher ensured a fair selection of the participants by taking a representative sample from the population in a scientific manner. Participants were selected based

on their availability at Medupi Power Station at a specific time and the researcher's knowledge.

- **Integrity, transparency and accountability**

The researcher was honest, fair and transparent during the conducting of the interviews. In this study, the researcher collected data and did not make use of field-workers. The researcher did not promise the participants any gifts or payment and they were informed of this when they completed an informed consent form. All the participants were acknowledged for their participation in the research.

- **Risk minimisation**

The participants were not exposed to any form of risk since they were interviewed at their place of employment in the boardroom and offices at a time suitable for them. The researcher was aware of the potential harm that might be inflicted upon the participants (Sanjari, Bahramnezhad, Fomani, Shoghi & Cheraghi, 2014:3). It was important to protect the participants by applying the ethical principles (Arifin, 2018:30).

2.11 Limitations of the study

Limitations are issues that may emerge within a research that are beyond the researcher's control (Simon & Goes, 2013:3). Prior to conducting the research, the researcher conducted an extensive literature review of the topic. However, the literature review proved that there is limited information available about the topic of National Key Point security in South Africa.

The study was limited to the security officers employed at Medupi Power Station at Lephalale, Limpopo Province. Data saturation limited the researcher from interviewing all the 30 individuals since the data was saturated at the 11th interview and there was not necessary to proceed with the interviews since no new themes were coming through. The results obtained were not generalised due to the qualitative nature of the methodology and the small sample that was used.

2.12 Conclusion

This chapter discussed the research design and approach used in the study and gave the reasons that guided the researcher to use them. The research design and approach were presented regarding the population, the sampling method and that pilot study that was performed in order to test the questions on the interview schedule. The chapter also discussed the data collection and data analysis techniques. Of importance was the discussion of the measures that were used to ensure validity and reliability, and the ethical considerations that were adhered to during the study. The limitation and the value of research were also part of the discussion in this chapter. In the next chapter, the researcher discusses the literature reviewed for the study.

CHAPTER THREE
LITERATURE REVIEW

3.1 Introduction

The focus of this study was to examine security threats and vulnerabilities at a National Key Point, namely, Medupi Power Station which is one of the critical infrastructures in South Africa. A “Critical Infrastructure” (CI) refers to the infrastructures that provide essential services to the society to ensure their well-being, in terms of public safety and services (Poustourli, Ward, Zachariadis & Schimmer, 2015:2; Hammerli & Renda, 2010:22). It involves the protection of physical assets which, if not protected, will impact negatively on the economy, health and security, public safety, service delivery and the general quality of life of the citizens (Alcaraz & Zeadally, 2015). Salient examples of critical infrastructure include communications, airports, emergency services, energy and financial institutions, among others. Therefore, any form of interference like vandalism or theft, can threaten the ideals of society and erode public confidence in the society (Hemme, 2015).

Critical infrastructure protection is the key to the sustainable management of key national infrastructure in any nation (Hemme, 2015:np). Critical infrastructure must be duly secured to deter any damage or vandalism due to natural disasters, political unrest and collateral damage during all forms of attack that can leave a country vulnerable (De Bruijne & Van Eeten, 2007:12). This chapter examines the available literature on CIP perspectives especially from the countries with advanced CIP systems, such as the United Kingdom (UK), Western Europe and the United States of America (USA), and their relevance to developing countries like South Africa.

Protection of critical infrastructure is important because it ensures effective and efficient function of the economy. Rehak, Hromada and Novotny (2016:943) provide further examples of CI that include electricity generations, transmission and distribution of oil/gas, production, transport and distribution, telecommunication, water supply and waste water/sewage, food production and distribution, public health, transportation (fuel supply, railway network, airports), harbours, financial services, and security services including the police and the military.

The review of the literature indicates that the term Critical Infrastructure Protection differs from country to country especially those attributes which may be considered “critical”. Therefore, each country has a list of critical infrastructures that must be protected from risks, vulnerabilities and any potential hazard to ensure its safety, stability and smooth functioning.

3.2 The importance of critical infrastructure

The term “critical infrastructure” was coined by the Clinton administration in 1996 (Aradau, 2010:500). Critical Infrastructure is a term referring to the importance of certain infrastructures which are defined as the systems, assets, facilities and networks that provide essential services, which are required for the national security, economic security, health and safety and prosperity (Shared Narrative, 2014:2). In essence, the concept of “critical” refers to the essential services which, if disrupted, can disturb the society and economy of countries.

According to Hammerli et al (2010), infrastructure means “physical infrastructure, such as good roads, potable water installations, telecommunication masts, houses, and electrical supply plants, and often intangible assets” which are not physical and may be classified as either definite or indefinite. Examples of intangible assets are patented technology, computer software, databases and trade secrets, trademarks, trade dress, newspaper mastheads, internet domains, video and audio-visual material (e.g. motion pictures, television programmes), customer lists and mortgage servicing rights. Critical infrastructures are regarded as the providers of services that are of national importance (Zaballos & Jeun, 2016:1) therefore their failure will have a significant impact on national interests of the economy, security and the expectation of society (Rehak et al, 2016:3).

Melchiorre (2018:12), describes the concept of critical infrastructure as

> *“a system constituted of those facilities, services and information systems that are essential for the maintenance of vital societal functions, health, safety, security, economy and social well-being of people and disruption or disruption has a debilitating impact on national security, national economy, public health, safety and on the effective functions of a*

government".

According to Katina and Hester (2012:1), research conducted on CIPs seeks to develop strategies to protect infrastructure systems by reducing hazards, risks and threats from both natural and man-made events. Factors of criticality enable proper allocation of resources and serve as a necessary process in ensuring proper protection of assets before a threat is discovered and act as a mitigating factor during an event and during recovery from a threat event (Katina & Hester, 2012:2).

In the context of this study, the infrastructure at Medupi Power Station at Lephalale serves as one of the main power stations in South Africa and it is responsible for generating electricity to a large area of the country. It is one of the largest electricity generation power plants of its kind in the southern hemisphere and in the world. At Medupi, the concept of infrastructure refers to the physical infrastructure used to store assets, machinery and equipment used to generate electricity. Any disruption in meeting its mandate to generate and provide electricity services to the community will have detrimental effects on the South African economy and society at large. For example, electricity has to generate power uninterrupted and free from any form of vulnerabilities.

3.3 The significance of critical infrastructure protection

Critical Infrastructure (CI) is a very important component of national security around the world as was recognised in 1999 by countries such as Canada, the United Kingdom (UK), Sweden and Switzerland (Izuakor, 2016:10; Steele, Hussey & Dovers, 2017). However, since the infamous terrorist attacks of September 11, 2001 in the USA, most European countries have redefined how they protect their critical assets and some have launched strategies to protect their critical infrastructures (CIs) to maintain important functions of society and ensure that everyday life is stable, safe and healthy (Heino, Takala, Jukarainen, Kalahti, Kekki & Verho, 2019:3).

3.4 International perspectives on critical infrastructure protection

Internationally, ensuring the security and protection of critical infrastructure has been largely shaped by the terror campaign unleashed on the developed world by Osama Bin Laden (CTED and UNOCT 2018). The attacks on the World Trade Centre on

September 11, 2001 created shockwaves across the civilised world and this forced many governments to review their critical infrastructure protection systems. According to Heino et al (2019:123), the disruption of CIs can have an impact on the social stability, national security and trust of the citizens based on whether the CIPs are able to uphold social stability (Heino et al, 2019:2). Therefore, any form of attack on the CI of a country can cause serious damage to the national security which may lead to the collapse of the entire infrastructure (Hemme, 2015:25; Melchiorre, 2018:11).

The protection of critical infrastructure is considered of strategic importance for any country because it safeguards the lifestyles, the quality of life and the constitutional rights of the citizens. When the citizens' trust in government institutions is undermined by an interruption of service delivery due to damage to the infra-structure or the compromised capacity of the utilities, this affects economic performance and can foster conditions that can make a country ungovernable. Disruptions of public services can also become a threat to the sustainability of democratic systems (Heino et al, 2019).

In the United States of America, the energy sector has been declared "uniquely critical" by Presidential Policy Directive Twenty One due to its enabling function across 15 other critical infrastructures (Hemme, 2015:36). The energy infrastructure therefore becomes a strategic national resource whose assets have to be protected "against any form of attack as part of national defense planning since World War II and throughout and after the Cold War" (Zaballos et al, 2017:7).

According to Zaballos et al (2016:1), critical infrastructure is referred to as "the basic physical and organizational structure required for a society to operate". In the UK, Canada and USA, CI therefore has national security strategies (Brunner, Cavelty, Giroux & Suter, 2010:6).

3.4.1 The European Programme for Critical Infrastructure Protection (EPCIP)

On the 17 June 2004, three months after the Madrid train bombings, the European Council requested the European Commission to develop a strategy to protect CIs (Fritzon, Ljungkvist, Boin & Rhinard, 2007:32; Caldeira, 2013:5). This communication was regarded as the first step in the protection of the CIs within the European Union.

The European Union has taken measures to curb the rise of terrorism which is fuelled by Islamic extremists and jihadists. As a unionised bloc, it is sensible for the European Union to reply as a bloc. This allows the states that are not as financially strong and technologically advanced to profit from the CIP from the bloc as a collective and enjoy stronger nations' technological infrastructure and resources. Reciprocally, this guarantees economic sustainability for the bloc which provides the Euro currency and makes the market a lucrative and favoured destination. Similarly, Karabacak et al (2009:291) found that, during these years, there was a request for the commission to prepare an overall strategy to protect CIPs in the European countries. Aradau (2010:491) indicates that the "EC lists the protection of infrastructures alongside the protection of the borders and that of citizens."

3.4.2 Critical Infrastructure in the United Kingdom (UK)

The UK has one of the most advanced CIP systems in the world. (CTED and UNOCT, 2018). The CIs in the UK are categorised in terms of the national infrastructure based on their contribution to the national economy (Ani, Watson, Nurse, Cook & Maple, 2019:3). These CIs are defined as those "facilities, systems, sites, and networks which are necessary for the effective functioning of the country in their efforts to deliver essential services upon which daily life depends" (Shared Narrative, 2014:12). According to Zaballos et al (2016:41), the UK policy on CIP is primarily focused on the economic significance and contribution of any identified critical infrastructure. This generates conditions necessary for policies that favour the economic growth of the UK. Consequently, the UK is able to prioritise CIP due to the perceived economic contribution that it makes to the GDP. In other words, economic reforms will never compromise the vital support that the CIP enjoys because it is an integral part of the economy (Steele et al, 2017).

The UK's advanced state of infrastructures enhances the national production, increases global competition and thus allows business growth by enabling suppliers and deepening the labour and product markets (Zaballos et al, 2016:41). This indicates that infrastructures at the UK are at the stage where growth is increasing which positively enables economic growth.

3.4.3 Critical Infrastructure Protection in the United States of America (USA)

Critical Infrastructure Protection in the USA goes back to the late 1990s when it originally gained recognition among American scholars. It became increasingly clear that the government can reduce the risk of incurring physical damage to strategic infrastructure which can be perpetrated by enemies created by the military aggression and American foreign policy (Flick & Morehouse, 2010:np). The purpose of employing security at the CIs is to provide physical defence. This perspective endorses the fact that CIP has a natural strategic role that requires strategic protective intervention measures to deter vandalism or terrorist activities targeted at undermining the functionality of American society (Leventakis, Nikitakos & Sfetsos, 2017:14).

In the context of the USA, the concept of “CI” was first used in October 1997 in the document entitled “Critical Foundations: Protecting America’s infrastructures” (Karabacak et al, 2009:280). The events that took place on September 11, 2001 in the USA resulted in the production of documents by international organisations, including governments and research institutions, on the vulnerabilities and protection of the CIs in the USA that require stakeholder engagement from variety of role players on how to protect the CIs. This is crucial because it improves the chances for developing robust CIP systems which, in turn, increase the quality of national security and lower the risk of compromise on any level (Zaballos & Jeun, 2016:np). In the USA, under the framework of the CI Advisory Council, there are Sectorial Coordinating Councils consisting of government and sector charters. In this way, more effort is made in the protection of the CIPs. However, protecting CIs is the responsibility of all the federal, public and private owners and operators of the CIs (Zaballos et al, 2016:29). The understanding between various departments and how they are interconnected, interrelated and interdependent helps the country to realise progress on the CIP objectives. This also minimises risks of security compromises and helps the country to fight any threats systemically (Bhaskar & Kapoor, 2014:67).

In addition to the above-mentioned, the USA government introduced the Risk management framework in the protection of CIs .The USA CIP strategy evolved in a very short space of time in an effort to make up for the intelligence failure that resulted in the 9/11 terrorist attacks on American soil. In this regard, the USA has

become a pioneering champion in advanced CIP and has prioritised the significance of Infrastructure Protection policies more than any other nation. The United States Guidance of the Presidential Policy Directives (PPD) 21 provides the CIP with flexible policies and research to address threats to CIs (Hemme, 2015:25). Flexibility of CIP policies and decentralisation helps to combat and curb future foreign or domestic terrorist threats that may undermine infrastructure protection, target vulnerabilities and endanger the lives of the citizens.

The National Infrastructure Protection Plan (NIPP) provides for a comprehensive risk management framework which defines the roles and responsibilities of the stakeholders of the CIs (Brunner & Cavelty, 2011:4). Thus, the USA NIPP is a risk management methodology which "enables the process for combining threats" (Poustourli et al, 2015:5). The USA has become one of the leading nations in the mastery of risk management methodology ever since 9/11 marked a new beginning in the age of CIP.

Hemme (2015:25) concurs that, in the USA, CIs is essential for security to be protected from both internal and external threats and also to ensure the physical repair of damaged CIs to prevent further disruption of essential services. Giannopoulos et al (2012:6) indicate that the purpose of the CIP framework allows for the partners of the department to identify, prioritise and protect the CIPs within communities against terrorist attacks.

It is critical for the USA to take CIP seriously in order to prevent domestic or foreign threats that may cause harm to the key economic and security apparatus which may result in socioeconomic dysfunction. This will help preserve peace and keep production levels high which is good practice for economic well-being and quality of life of the citizens. A country should prioritise CIP in order to ensure that its citizens' quality of life, health and social well-being are not compromised. This helps the country to have stronger institutions derived upon trust. Any government that chooses to compromise its CIPs duties is short-sighted and in a very weak and fragile position.

The strategic infrastructures stated and deemed as critical will mainly depend on geopolitical factors and the description and nature of a country's major economic

activities. Hence, each country's strategy has to factor in approaches that may be different from its neighbours or the rest of the world. For instance, an island nation like Singapore may have a different CIP system and evaluation criteria compared to a country that is landlocked like Zambia (Bhaskar & Kapoor, 2014).

It is evident from the literature that South Africa lags behind with Critical Infrastructure Protection (CIP). Europe, UK and the USA being the masters of CIP are at an advanced level of managing CIPs. In Europe, this is called the "European Programme for Critical Infrastructure Protection (EPCIP)" and in the US it is called "Critical Infrastructure Protection (CIP)".

These countries developed a comprehensive risk management framework as the methodology to protect the CIPs. They also developed a National Infrastructure Protection Plan which caters for all the CIPs which includes the sharing of resources across CIPs. In the European Union (EU), CIPs have policies to protect CIPs which includes food safety and disaster response to protect CIPs.

In these countries, CIPs are interrelated and managed by the government. In Europe for instance, these include energy, food, Information and Communication Technology (ICT), pipes and pumps, water, defence, public safety, health, telecommunication, transport, financial sector, vital human services, and the chemical and nuclear industries. These CIPs are managed by different bodies, for example, in the US, they are managed by the President's Commission on Critical Infrastructure Protection (PCCIP) and, in Europe, the European Council on the Protection of Critical Infrastructure Framework manages the CIP. It is clear that these countries are advanced in CIPs as compared to South Africa. The CIPs in these countries are not the responsibilities of the police, as in South Africa, but they have established bodies reporting to the commissions on CIPs. In support of the stricter rules and policies, these countries protect the CIPs with security measures such as the security and physical measures in the same way as in South Africa.

To summarise the above, South Africa did not develop policies on CIPs as guided by the Critical Infrastructure Protection Act. The CIPs are functioning in isolation and security officers and the police are utilised to protect these CIPs.

Despite the fact that South Africa has legislations on the prevention of threats and vulnerabilities, they still persist for National Key Points. This legislation was meant to protect these infrastructures against sabotage. Some of the threats and vulnerabilities in CIPs in South Africa have been evident. Eskom has been experiencing malicious attacks on its security grids which can cripple CIPs in South Africa. The South African NKP was also exposed to abuse by Ministers who need their homes to be declared NKPs and believe that their protection is more important than that of ordinary citizens. Some of the breaches to NKP are service delivery protests, student protests, and the third force to these protests.

3.5 Legislative framework on the protection of critical infrastructure in South Africa

3.5.1 National Key Points Act 102 of 1980

The necessity for protecting CI in South Africa was introduced through legislations such as the National Key Points Act 102 of 1980 (SA, 1980) and, more recently, the Critical Infrastructure Protection Act, No. 8 of 2019 that makes provision for the protection of state assets against any form of attack. The National Key Points Act 102 of 1980 (SA, 1980) was the first piece of legislation introduced by the apartheid government to identify certain areas of critical importance as national key points (Du Plessis, 2013).

In their fight against apartheid, black South Africans made the country ungovernable through protests that caused social unrest, violence against security officers, vandalism of strategic institutions and so-called terrorist acts by the military branch of the ANC (Du Plessis, 2013). Because of this, the apartheid government was forced to divert additional military resources to protect national key points in order to avoid a complete shutdown of the economy at the time when the country was already plagued by sanctions and isolation due to its apartheid policies (Du Plessis, 2013). The purpose of the NKP Act was to give the Minister of Defence more powers to declare certain areas to be national key points and to impose certain security requirements for them (Pothier, 2013:1).

The National Key Points Act 102 of 1980 (SA, 1980) was introduced to protect key state infrastructures, which are of the strategic importance to the country, against

sabotage. These areas include airports, energy and water resources, the military, dams, financial services, emergency services and health care, among others. At the heart of the National Key Points Act 102 of 1980 (SA, 1980) was the protection of infrastructure and government assets from theft, vandalism and other threats. Therefore, the essential purpose of the National Key Points Act 102 of 1980 (SA, 1980) was to assess and identify risks, threats and the vulnerabilities of national key points in the Republic of South Africa. By factoring in the significance of key infrastructure, such as telecommunications, energy production and banking, South Africa positions itself as an investor friendly destination because the infrastructure protection policy helps to de-risk the costs incurred in doing business in the country (Oforis, Hindle & Hugo, 1996).

3.5.2 Critical Infrastructure Protection Act, 2019 (No. 8 of 2019)

A concern was raised by the apartheid government in the late 1970s about the possibility of sabotage by the banned African National Congress across South African borders which led to the introduction of the National Key Points Act 102 of 1980 (SA, 1980), which was introduced to protection key strategic government installations, such as oil refineries, nuclear plants and electricity generation plants in South Africa. This was replaced by the CIP Act No. 8 of 2019.

The main purposes of the Critical Infrastructure Protection Act No. 8 of 2019 are:

> *"to provide for the identification and declaration of infrastructure as critical infrastructure; to provide guidelines and factors to be taken into account to ensure transparent identification and declaration of critical infrastructure; to provide for measures to be put in place for the protection, safeguarding and resilience of critical infrastructure".*

These factors are used to identify and declare critical infrastructure (Critical Infrastructure Protection Act No. 8 of 2019: np). The figure below shows how critical infrastructure is determined:

(a) the infrastructure must be of significant economic, public, social or strategic importance;
(b) the Republic's ability to function, deliver basic public services or maintain law and order may be affected if a service rendered by the infrastructure is interrupted, or if the infrastructure is destroyed, disrupted, degraded or caused to fail;
(c) interruption of a service rendered by the infrastructure, or the destruction, disruption, degradation, or failure of such infrastructure will have a significant effect on the environment, the health or safety of the public or any segment of the public, or any other infrastructure that may negatively affect the functions and functioning of the infrastructure in question;
(d) there are reasonable grounds to believe that the declaration as critical infrastructure will not have a significantly negative effect on the interests of the public;
(e) the declaration as critical infrastructure is in pursuance of an obligation under any binding international law or international instrument; and
(f) any other criteria which may, from time to time, be determined by the Minister by notice in the *Gazette*, after consultation with the Critical Infrastructure Council.

Figure 2: The identification and determination of critical infrastructure complex
(Source: Critical Infrastructure Protection Act No. 8 of 2019: ch 3(16) (2)).

Ponthier (2013:1) indicates that some of the national key points include power-stations, harbours, airports, factories producing ammunition and explosives, oil refineries and other important government properties that include Parliament and the Reserve Bank. The criteria to identify an area to be national key point in terms of section 2 of the Act 8 of 2019 is that the Minister of Defence has the power to declare a structure, installation or building a national key point when it can affect the economy, intelligence and the development of the country (Boda & Dullabh, 2019). Chapter 1 of Protection of Critical Infrastructure Bill is to ensure

> *"(a) the adequate protection of Critical Infrastructure within the Republic; (b) the creation of procedures for the determination and protection of Critical Infrastructure that are open and transparent; and (c) accountable administration of Critical Infrastructure while ensuring that the security of the Republic is maintained"*
>
> (https://juta.co.za/media/filestore/2015/09/PMB4_2015.pdf).

3.5.2.1 Strategic Installations Bill (Notice 432 of 2007)

The main purpose of this Bill is to protect places and premises and areas that are deemed to be of strategic interest against sabotage or other forms of attack. These are energy infrastructures and all areas as stipulated in Chapter 3 of this bill. It is therefore the responsibility of government to ensure that the necessary measures are put in place to enhance security of these areas. In terms of Chapter 3 of this Bill, the Minister of Police has the power to declare National Key Points, Strategic Installations and places of strategic importance that meet the criteria based on the committee evaluation.

More still has to be done by way of progressive legislation to ensure that the security and quality of life in the young South African democracy is not compromised. However, the steps that the government has taken to date prove that we are going in the right direction. Hence it will be necessary to make sure all our practices are at par with the best in the world since this is likely to strengthen our place as an economic powerhouse in the southern hemisphere and boost our branding efforts Ponthier (2013:1).

3.6 Theoretical basis for the study

The incidents of crime taking place at Medupi Power Station can be attributed to the weakness in crime prevention measures as a result of security threats and vulnerabilities affecting the power generating plant. To this extent, the Opportunity Theory, Routine Activity Theory and Rational Choice Theory are examined to explain such anti-social behaviour at Medupi Power Station.

3.6.1 Crime Opportunity Theory

This theory suggests that offenders make a rational choice and choose targets that offer high levels of rewards with little risk (Gritzalis, Theoharidou & Stergiopoulos, 2019:65). In the context of Medupi, this poses serious threats to the assets and offenders are well motivated to commit crimes in an environment that creates an opportunity for crimes to be perpetrated. Opportunity theorists Marcus Felson (1947) and Lawrence E. Cohen (1974) argue that the key issues that must be present in the commission of crime are motivation, opportunity and a lack of guards. The crimes

committed by international crime syndicates target items with high returns and little effort plus highly manageable risks. If the CIP is more advanced and the regulations and legislation around CIP and charges are stricter, this reduces the likelihood of crime. Longer prison sentences, tighter restrictions and an aggressive approach to the CIP regulation and training of personnel will most likely reduce the risk of CI theft. It is arguably a highly productive approach to pursue opportunity crime theories against other prevailing perspectives in order to resolve the crime motivation phenomenon.

It seems evident that more scholarly work must be done in this area in order to prove the validity of the theories. Advances in this area will increase the capabilities of the advisors on such aspects to key organisations and state organs. This way the CIP goal can be realised more readily and more effectively. It is imperative that the critical infrastructure security features will readily increase the reliability of CIP and hence further the overall objective of improved security.

Site designs allow for access control, target hardening, and surveillance potential. Access control refers to the control of movement into, out of, and within a specified area that facilitates the convergence of offenders and targets/victims. Similarly, target hardening is “the mechanism through which access to individual property targets can be restricted for all but legitimate owners and users” (Reynald, 2015:79). Surveillance is related to the design and layout of buildings, streets, and walkways (Jacobs, 1961). It describes the way that people in a particular area can see and be seen. It also includes technological devices such as lighting and security cameras.

Surveillance, to a greater extent, defines why western countries have managed to take the lead in providing security before the rest of the world. Surveillance technology increases the barriers to theft and vandalism because the chances for apprehension by authorities are high unless there is malfunction or purposeful criminal intention to undermine the surveillance infrastructure.

Research has shown that access control, target hardening, and surveillance may provide opportunities for crime. Routes in and out of an area, traffic and proximity to a highway are positively related to crime while restricting access and the use of locks, alarms and marking of property can reduce crime (Bowers et al, 2004,

Donnelly & Kimble, 1997, Johnson & Bowers, 2010; Eck & Guerette, 2012).

Surveillance infrastructure is a key component of CIP protection that can minimise losses that the state or its organs may incur if the surveillance technology has been compromised. It is therefore necessary for procurement for infrastructure in the government or state organs to invest in surveillance technology as the evidence of its general effectiveness is compelling.

According to Felson and Clarke (1998:9-22), the following are the ten principles of opportunity and crime:

1. Opportunities play a role in causing all crime

Crime and opportunity are related to one another. In the context of Medupi, most of the hazards and threats that occur are due to the fact that opportunity prevails to an extent that it motivates offenders to commit theft of assets which, in turn, creates more threats to the whole CI operation. Although opportunity plays an important role in every crime, the nature of opportunity determines the type of crime that occurs.

2. Crime opportunities are highly specific

Crime does not take place without an opportunity. Felson and Clarke (1998:9-22) agree that opportunity plays a major role but that no single crime opportunity factor applies to all forms of crimes. According to these authors, crime opportunities are specific to each offence and offender subset. For example, in the context of Medupi, an offender may look for something in the plant to steal or may be interested in stealing cables or property, such as office or plant contents, to sell to pawnshops or at flea markets.

3. Crime opportunities are concentrated in time and space

Crime opportunities are not equally distributed for the following reasons:

- **Some people and properties are not suitable targets for criminal attacks***:* For example, during the day in the presence of employees, offenders are unwilling to commit crimes and some locations have security guards or other security features (Felson & Clarke, 1998:14).

- **The spatial and temporal distribution of people and things is highly uneven and sets the stage for crime to occur at a particular place and time:** For example, a robber may commit robbery in a place with weak security measures when security guards move away from their posts. In order to breach strong security measures, the offender may apply aggressive force to gain entry into the restricted areas during the night.

- **Crime opportunities depend on everyday movements:** A place that has little movement creates a space for crime and a place where there is a high movement of people reduces the possibility of crime occurring. The flow of workers in and out of the plant acts as a barrier for crimes to occur (Felson & Clarke, 1998:16).

- **One crime produces opportunity for another:** An offender can find opportunities to commit other crimes in the course of committing a criminal act; one crime can generate multiple crimes (Felson & Clarke, 1998:17). For example, criminals may threaten or kill victims or security guards, assault and tie them up or rape female security guards.

- **Some products offer more tempting crime opportunities:** According to Felson and Clarke (1998:19), any form of valuables that can be transformed into cash may be stolen. This is also true of the Medupi Power Station whereby offices are left open, valuable items lying on the table, such as laptop, computers and cellphones.

- **Social and technological changes produce new crime opportunities:** As technology frequently produces new products, these become targets for theft (Felson & Clarke, 1998:22). Old technology is not as attractive to thieves so is unlikely to get stolen. Computer theft has been an issue of concern for the Medupi Power Station.

- **Opportunities for crime can be reduced:** Security measures put in place using “problem-oriented policing, defensible space, crime prevention through environmental design and situational crime prevention” (Felson & Clarke, 1998:23) should reduce the opportunities for criminals. Medupi has CCTV

surveillance cameras, alarms and other security measures which are designed to reduce the opportunities for crimes to be committed.

- **Reducing opportunities does not usually display crime:** According to Felson and Clarke (1998:25), the theory of crime displacement means that the different ways of reducing crime opportunities often just move crime from one area to the next. This is called “geographical displacement, temporal displacement, target displacement, tactical displacement and crime type displacement” (Felson & Clarke, 1998:25).

- **Focused opportunity reduction can produce wider declines in crime:** Apart from crime displacement, sometimes the reverse of displacement may occur. In other words, it is important that the prevention measures also be used in areas away from the places where opportunities exist (Felson & Clarke, 1998:30). For example, when CCTV cameras were introduced to monitor thieves in the Medupi Power Station, crime declined not only in an area that is covered by surveillance cameras but in adjacent locations as well.

3.6.2 Routine Activity Theory (RAT)

Routine activity theory seeks to find explanations for the causes of crime. It also highlights that crime is caused by three elements: a suitable target, a lack of protection and a motivated offender (Argun & Daglar, 2016:1189). Offenders in this theory are not influenced by socio-economic factors such as poverty, unemployment and other ills. Once the three elements are present, crime becomes an alternative hence people become attractive targets for those motivated (Hsieh & Wang, 2018:335). RAT is an important tool to reduce crime, evaluate crime problems and take routine precautions that reduce crime opportunities in people’s daily lives (Argun & Daglar, 2016:1189). According to Savard (2018:57), criminologists use RAT to study why a criminal event takes place. In the context of Medupi, this study examined the occurrence of crime as a result of security threats and vulnerabilities.

3.6.3 Rational Choice Theory (RCT)

The RCT theory focuses on the offender’s decision-making prior to committing a crime (Felson & Clarke, 1998:7). According to Kumar, Kelly, Clare, Wuschke and

Garis (2019:4), RCT contributes to rational choice to explain the crime by assuming that the decision to commit crime is made by a person who thinks that they can reap a reward that outweighs the risks involved. Offenders are driven by their situations and environments to analyse the potential risks and compare them with the profits of the act (Gul, 2009:37). Burns and Roszkowska (2016:196) argue that the purpose of this theory is to determine an individual's choices and their social behaviour.

According to Burns and Roszkowska (2016:197), RCT has the following multiple components: an actor in a decision situation identifies the possible and clear options, determines their preference for the likely outcome resulting from each of the alternatives, compares the consequences of each option and then decides which option provides the highest net gain (Burns & Roszkowska, 2016:197).

3.7 Conclusion

The purpose of this chapter was to discuss critical infrastructure and the importance of CIP. The international perspectives on CIP were discussed drawing lessons from the EU, UK, USA and South Africa. It is clear from international literature that South Africa lags behind in terms of CI and its protection. The criteria used to identify CI in South Africa are different to those of other countries. The EU and its member states have a model of CIP which should be given serious attention by our government.

The threat of apartheid may be over but, in this new era, we are seeing an ever increasing global crisis of terrorism that is affecting both the developed and the developing world. Even on our doorstep, since oil was discovered in Mozambique, that country has been experiencing terrorist activity. If oil is discovered in South Africa, it may spark similar conflicts hence it is critical for the CIP legislation and policy to be quickly promulgated and implemented to protect the country's well-being.

The role that CIP plays in this modern world can be the difference between a loss-making and a profit-making parastatal. It is evident that CIP intelligence failures and compromised CIPs, such as 9/11, are disastrous for the economies of entire blocs, nations and the world and have far reaching effects on the political and socio-economic landscape.

The government and the stakeholders, like universities, must undertake advanced CIP studies in the unique localised context of the South African national infrastructure. This will generate data that the stakeholders and key decision-making boards can use to leverage the maximisation of CIP to concretise the approaches and develop robust strategies for progressive CIP initiatives. Whilst studies from other countries that have far more advanced CIP may be of great help, the challenge is that our geopolitical interests are different and hence the approaches we use will differ.

In the next chapter, the researcher discusses the findings of the study.

CHAPTER 4
DATA ANALYSIS AND DISCUSSION OF FINDINGS

4.1 Introduction

This chapter presents the data analysis and discusses the research findings of data collected during the study. The findings answer the questions on security threats and vulnerabilities at a national key point with a case study of Medupi Power Station. To collect data, the researcher conducted eighteen (18) telephonic and face-to-face interviews using purposive sample techniques with employees who perform security functions at the power station. The findings are divided into two sections. In Section A, the researcher discusses the demographic make-up of the sample by evaluating variables such as, sex, age, marital status and educational background. Section B discusses and analyses the responses provided by respondents to the questions contained in the interview schedule based on the aims and objectives of the study.

The focus of the study was to evaluate security threats and vulnerabilities occurring at Medupi Power Station. To do this, the researcher formulated the following objectives which were linked to the research questions:

- To evaluate the nature and extent of security threats and vulnerabilities at Medupi Power Station
- To identify the security threats and vulnerabilities that contribute to the increase in crime at Medupi Power Station.
- To evaluate the present physical security systems in place at Medupi Power Station
- To consider strategies for reducing burglary and theft at the power utility.

The findings of the study are discussed in the next section.

4.2 Section A: Demographic details

Table 1: Summary of demographic details of participants

Participant Number	Age	Gender	Marital status	Current position at Medupi
1	23-27 years	Male	Married	Security Officer
2	38 years	Female	Single	Investigator
3	28-32 years	Male	Unknown	Security Officer
4	Unknown	Male	Unknown	Security Officer
5	44 years	Male	Married	Security Officer
6	53 years	Male	Married	Senior Manager
7	Unknown	Male	Unknown	Security Officer
8	57 years	Male	Married	Senior Inspector
9	42 years	Male	Married	Security Officer
10	Unknown	Male	Married	Security Officer
11	42-48 years	Male	Married	Intelligence
12	42 years	Male	Married	Security Officer
13	34 years	Female	Married	Security Officer
14	39 years	Male	Unknown	Security Officer
15	Unknown	Male	Married	Security Officer
16	37-42 years	Female	Single	Technology
17	45 years	Male	Unknown	Contractor
18	18-22 years	Unknown	Married	Security Officer

In this study, there were fifteen (15) males and three (3) female participants. The reason for this was that there were fewer females employed in the security department and those participants selected were available and agreed to participate in the interviews. With regard to the age of the participants, two were aged between 33 and 37 years, four were aged between 38 and 42 years, one was aged between 43 and 52 years and three were aged 53 and above. The ages of other participants

were between 18 and 22 years, 23 and 27 years and 28 and 32. It is clear from the information on the age categories that all the participants were adult and mature enough to understand security threats and vulnerabilities at the Medupi Power Station.

Eleven of the participants were married, two were single and the status of five participants was unknown. Most of the participants were married. With regard to the qualifications of the participants, six of the participants had certificates; one had an advanced diploma; four had diplomas and one participant had grade 12. The qualifications of six of the participants were unknown. The majority of the participants acquired certificates other than diplomas and advanced diplomas. It is clear that these participants have limited levels of education. In summary, most of the participants were married and aged between 38 and 42 with certificates as their qualifications.

4.3 Section B: Findings

In this section, the researcher discusses and interprets the research findings of the study.

4.3.1 Discussion and interpretation of findings

The findings are discussed in relation to the research objectives and linked to the research questions. The data were collected and recorded using a mobile phone and an audio-tape recorder. All the data were transcribed verbatim and subjected to thematic analysis procedures as outlined in Chapter 2. The purpose of applying the thematic analysis was to make sense of the data. It involved identifying, organising, verifying, analysing and reporting themes and sub-themes. The analysis was based on the following research questions:

4.3.1.1 What types of crimes occur at Medupi Power Station?

Theme 1: Criminal activities at Medupi Power Station

The purpose of this question was to establish the types of crimes that are experienced at Medupi Power Station. In this theme, the categories of theft of copper cable and working tools emerged during analysis of the data.

(a) Copper cable theft

Almost all the participants indicated that copper cable theft is a serious problem at Medupi. Critical infrastructure (CI) involves the protection of physical assets which, if not protected, will impact negatively on the economy, health and security of the citizens (Alcaraz & Zeadally, 2015). The participants also stated the modus operandi of thieves who steal copper cables, and how they steal it. Pretorius (2012:56) found that the theft of important assets, such as copper cables, remains a serious challenge facing the economy of South Africa as it has a negative impact on a variety of disciplines. According to Pretorius (2012:2), copper cable theft constitutes more than 90% of all copper theft, and the remainder consists of copper items in direct support of the copper cable network. Because copper cable theft brings with it safety problems to the general public (Narayan, 2013:1), it is of serious concern to the community and the power station.

The following verbatim statements reflect the experiences of the participants:

> *"… you can say, because people, they're stealing cable"* - **P8** (Senior Inspector), responsible for infrastructure inspection related information.
>
> *"[theft] such as copper cable, mostly is committed by contractors"* **- P1** (Security Officer), guarding and protection of assets and people.
>
> *"There is a lot of theft with copper cable"* **- P16** (Technology), infrastructure technology related information.
>
> *Criminals steal physical items, such as copper cables, equipment, fiscal assets inside and outside the power station"* **- P9** (Security Officer), guarding and protection of assets and people.
>
> *"Copper cables – the actual financial loss suffered by the company is severe"* **- P12** (Security Officer), guarding and protection of assets and people.

According to the participants, copper cable theft is a crime which takes place both during the day and at night at Medupi Power Station. They further indicated that copper cable theft has dire consequences for the power station.

(b) Theft of working tools

The participants indicated that theft of contractors' working tools is rife at the power station due to the number of contractors employed at Medupi. Also, contractors' employees steal from other contractors. Participants believed that this is due to negligence. Theft of this nature is associated with economic loss and displeasure (Narayan, 2013:1). The participants said that:

> *"Working tools at Medupi Power Station may be exposed to a security threat such as theft"* **- P5** (Security Officer), guarding and protection of assets and people.
>
> *"This is an indication that store men are careless when tools are missing"* **- P2** (Investigation), crime investigation related information.
>
> *"They're just leaving their tools"* **- P3** (Security Officer), guarding and protection of assets and people.
>
> *"… and when these letters are being investigated, you'll find that equipment were left unattended"* **- P10** (Security Officer), guarding and protection of assets and people.
>
> *"… and some resources like machines, grinding machines, used daily by their contractors"* **- P16** (Technology**).**
>
> *"Crime theft that I I've been on, like theft of cables and theft of the electric, eh, appliances, lights, grinder's drills"* **- P14** (SO**).**

The participants believed that tools are stolen as and when an opportunity prevails. Some of the tools are left deliberately to sabotage the contractor. They indicated that it is not possible to accuse any person in possession of tools as all the contractors use same tools. The following participants explained the reasons for leaving the tools behind.

The participants said that:

> *"Tools are stolen because they used to share those tools"* - **P17** (Contractor), provide security services.

"They are stealing the materials meant to do the work" **- P18** (SO**).**

This is because those responsible for the safe-keeping of tools shift the responsibility to those who use them. In other words, when tools are shared, no one takes responsibility for the loss and they blame each other.

Participants said that:

"… and the other thing, just stealing tools from one company to another" **– P7** (SO).

According to the participants, the fact that companies employ many people means that tools may be stolen by employees of another company. The participants also maintained that theft of tools does not only affect the contractor but it also affects the power station and the community. Employees or contractors at Medupi are not vetted and they do not care about the impact of crime.

Theme 2: Description of the modus operandi of crime

The purpose of this question was to understand how the assets are stolen at Medupi. Modus operandi is the method used by criminals to steal copper cable. It is the way in which a crime has been committed and comprises choices and behaviours that are intended to assist in the completion of crime (Van Der Watt, Van Graan & Labuschagne, 2014:62). Thieves use different modi operandi to steal copper wire. The modus operandi of the suspects can be used to pro-actively profile the suspect to increase successful prosecution (Liebenberg, 2018:17). Participants indicated that thieves make sure that they are not seen. They cut the cable into pieces and conceal them in small quantities in containers, such as two-litre Coke bottles, as they are able to take it out without being seen. From the analysis of data under this theme, the following category and sub-categories were identified:

(a) Cut cables and put in bags, of two litre Coke bottle and lunch box

Almost all the participants indicated that employees cut copper cables into pieces and rolled them to fit in a bag or a two litre Coke bottle. This finding is new and it will therefore add to the existing gap in the literature. The following are verbatim statements from the participants:

"… they're skinning cables and they put it in the bottle" **- P17** (Contractor**).**

"They put cables and then put it through inside the containers" **- P5** (SO**).**

"… they're skimming the cables, put them in their bags so that, when they go out … they put it maybe in the container, the lunch containers, so that, when you go out, you will have thought that they have their leftovers then they put them inside those containers" **- P1** (SO**).**

"… the cables cut into pieces, wherever they put it in the bags, they are using to go to work, which one wrapped up with a glove" **- P3** (Security Officer**).**

"… they put those pieces inside the two litre of cold drink" **- P11** (Intelligence), crime intelligence related information.

"… the criminal, they skin, the cable, and they are putting the two litre of drink" **- P2** (Investigator), crime investigation related information.

"… cables are skinned and put it inside the bags" **- P4** (SO),

"… the theft of copper; they just take it and they put it into two piece plastic aside wires aside, they tied to their body and they put another jacket on top" **- P16** (Technology**).**

The participants revealed that copper cables are cut and put in portable containers so that they could be easily hidden. These employees intend to sabotage the employer (contractor) to ensure that their employers suffer as a result of their actions.

(b) Cables are stolen from inside and thrown over the fence

In this study, the participants reported that thieves often throw stolen cables over the perimeter fence surrounding Medupi Power Station. The following statements confirm this:

"They took the cables and scaling up the fence when they were on strike. They burnt vehicles and damaged buildings" - **P9** (SO**).**

"… you can say, because people, they're stealing cable or they're skinning cables, yes. Or to the skin cube, will they put it in the bottle" - **P5** (SO**).**

"Most people waiting inside; you break them into small pieces so that they are portable enough for them to smuggle out of sight without being noticed" - **P1** (SO**).**

"… they just cut them into small pieces and smuggle them out" **- P17** (Contractor).

"… [they cut] copper cable into pieces, and throwing them in there" **- P16** (Technology).

"… there were pieces of cable being cut on every day because every time it was cut or not marked" **- P11** (Intelligence).

The reason for that is because they will either collect it after hours during the night or have people who will collect it on their behalf. According to Narayan (2013:11), copper cable theft occurs during the construction of the power utility and again when the utility is operational.

(c) Cables are put inside the bonnet of a vehicle

The participants in this study confirmed that thieves smuggled stolen copper cable by hiding it under the bonnet of a vehicle. This was revealed by participants 11, 18 and 13 when they said that:

"And things could be easily placed inside the bonnets and taken out" -**P11** (Intelligence).

"… they just put it maybe inside the bags or at the front of the bonnet and then to get outside" **- P18** (SO).

"… when they put it in the bonnet, they are aware it is the place for the engine and some of them do not switch off the engine during search" **- P13** (SO).

This is a new modus operandi which is not supported by the literature.

(d) Cables are put under the seat of a bus

Participants confirmed that stolen goods are smuggled under the seats of buses. This is confirmed by the following statements:

> *"Some, they're putting them on the seats of the bus"* **- P7** (SO).
>
> *"And other people … they put it under behind the seat"* **- P16 (**Technology**).**
>
> *"So normally, they put cables on that transport on the one that transport tissue only he didn't place his luck buses"* **- P5** (SO).
>
> *"… when we do searching, we found them in the car, under the seats, hiding under the seats, cutting cables at the plant"* **- P18** (SO**).**

(e) Cut fence to get access into premises to commit other crimes

Another modus operandi for committing crime at Medupi Power Station is by cutting the fence to gain access to the power station. This is a new finding which is not supported by the existing literature review. It also demonstrates a gap in the literature. Participants had this to say:

> *"… cutting the defence in order to gain access in order to steal the cable or the material or the vehicle and stuff like that"* **- P2** (Investigator).
>
> *"… they are cutting fences, taking them outside by cutting fences, some are coming out with them at the gateway by taking chances for not being searched by the security"* **- P17** (Contractor).
>
> *"… the copper cables during the night or in the place where they usually cut the cable which one cannot throw so can number two housekeeping happen in your area usually containers where no visible security"* **- P9** (SO).
>
> *"… used to cut out earlier or to cut our fence to get inside our premises for the housebreaking"* **- P14** (SO).
>
> *"We can cut the fence, go through underneath and come [up]"* - **P17**

(Contractor).

(f) Wrap stolen cables around the body

Some of the thieves wrap the stolen copper around their body parts, such as on the legs or the body which is covered by clothes. This type of modus operandi lacks support from the literature which renders it to be a new theme that emerged from the findings of this study. The following are some of the responses from the participants:

> *"… for that for cables, sometimes they skinny the skinny those cables and they sometimes roll them on the upper bodies or put them in the dustbin or put them in the bottles, the plastic bottles and bottles"* **- P2** (Investigator).

> *"They are hidden on their body"* **- P9** (SO).

> *"They do that. Some of them are wrapping it on their legs"* **- P18** (SO).

In order to determine from the participants the key types of security threats and vulnerabilities that occur at Medupi, they were asked about how crime can be reduced at the site.

(g) The manner in which crime is reduced at the site

The main purpose of this question was to explore the participants' experiences on how crime can be reduced at the site. The participants indicated that they use a variety of measures to reduce crime from happening at the site that included patrols and conducting searches on vehicles and persons. The use of CCTV cameras is regarded as a proactive approach to policing due to the fact that criminals can be identified leading to arrests (Moyo, 2019:9). Cebekhulu (2016:42) contends that CCTV cameras are deterrences and that an opportunist criminal is intimidated by a noticeable camera. The literature indicates that CCTV surveillance cameras, access control measures and biometrics are the measures used to reduce crime (Moyo, 2019; Cebekhulu, 2016).

(h) Patrols

The participants indicated that conducting foot and vehicle patrols by armed security

officers contributes to the reduction of crime on the site (City of Tshwane, 2016:2). The following are direct quotes from the participants:

> *"… Another thing is patrol. Regular patrol at the night must be conducted"* **- P7** (SO).

> *"… that I patrol the premises NKP fence"* **- P9** (SO).

> *"… make sure that we use our vehicle to patrol the premises"* **- P17** (Contractor).

> *"… the patrol can be for an hour or after one hour 30 minutes to check if our set is in good condition"* **- P10** (SO).

> *"… we conduct regular patrols to ensure that you keep the site when they win when such a person has got the knowledge"* **- P4** (SO).

(i) Conduct searches

Searches are one of the measures that are in place to reduce crime at the site. Participants indicated that they search vehicles and persons to ensure that they are not leaving or entering the premises with stolen items. The following are the verbatim statements from the participants:

> *"We searching everyone entering the site"* **- P2** (Investigator).

> *"… access control – I'm searching people because everyone entering and leaving the site making sure that every equipment in the site authorised to leave the site so that any devices that you're using to search those vehicles"* **- P6** (Senior Manager), security management related information.

> *"Body searches done at the exit points at the security point"* **- P9** (SO).

It is evident from the participants that conducting searches when people enter and leave the premises can be an effective tool in reducing crime at the site.

(j) CCTV surveillance cameras

The participants view CCTV surveillance cameras as another measure to reduce crime. Some findings, for example, Moyo (2019:60), confirm that CCTV systems are used as a security tool to enhance the level of protection and the assets against security risks. Security officers are able to detect an intrusion in progress through the CCTV surveillance cameras (Cebekhulu, 2016:42). Gibson (2017:22) indicates that one or more CCTV cameras are deployed at the same time. They are of the view that CCTV cameras can reduce crime because they are available during the day and night. Participants explained:

> *"… the security measures that I can see to fit, is for having CCTV camera"* **- P2** (Investigator).

> *"… we are using good quality CCTV"* **- P15** (SO).

> *"CCTV security room monitors or discovers any wrongdoing or illegal irregularity"* **- P12** (SO).

According to the participant's responses, CCTV surveillance cameras play a pivotal role in combating crime.

(k) Using access control measures

According to the participants, access control measures play a role in reducing crime. This includes the use of biometrics and searches of persons and vehicles entering and leaving the premises. There is evidence in the literature about the role of access control, for example, Musonza (2016:55) points out that access control facilitates the movement of people, vehicles and goods in and out of the premises. Access control measures are achieved using a number of measures that include security guards, locks and biometrics (Borham, Abas, Azizan & Syariff, 2016:3). The following are the verbatim statements from the participants:

> *"When we do access control"* **- P6** (Senior Manager).

> *"… we observe the vehicles inside and we check all those hidden areas. Those are the methods we're using, especially on the entrance or the*

access control" **- P5** (SO).

"… to reduce crimes on the site is to make sure that we are doing access control basically in those vehicles and passes when they enter the site mostly" **- P15** (SO).

Access control restricts access and thus can reduce crime (Bowers et al, 2004; Donnelly & Kimble, 1997; Johnson & Bowers, 2010). "Access control is the way by which people are approved or refused admission to controlled areas, such as office suites, storage amenities or car parks" (Integrated Solutions, 2009:62).

4.3.1.2 What types of security threats and vulnerabilities occur at Medupi?

Theme 3: Identification of security threats and vulnerabilities

The following categories were identified under this theme:

The participants were of the view that there were many security threats and vulnerabilities at Medupi. They also indicated that threats are caused by the following:

(a) More than one gate and a lack of resources including manpower

The participants were concerned about multiple gates in the premises while there is a shortage of resources and manpower to perform duties at these gates. Pretorius (2012:170) established that having security manpower was not sufficient to effectively mitigate copper cable theft as they lacked security experience and knowledge. The participants who were concerned about multiple gates indicated:

"The threats that I see here are a lot of gates … lots of gates that are entering" **- P18** (SO).

"… we've got a lot of gates around the side" **- P1 (**SO).

"… most of the gate or several of the gates …" **- P10** (SO).

Some of the participants were concerned about the lack of manpower. They maintained that there were not sufficient security officers to man the gates and this

compromises the security of the station. They said that:

> *"… sometimes you will find out that you don't have enough manpower on some of the gates"* **- P14** (SO).
>
> *"Manpower is limited"* **P17** (Contractor**).**
>
> *"… normally we always work with a short shift. Not full with manpower"* **- P8** (Senior Security Inspector**).**
>
> *"… not working with full manpower"* **- P2** (Investigator).
>
> *"… we need to get more manpower within this unit to get people to be on [duty]"* **- P5** (SO).

It is evident from the above responses that insufficient manpower has an effect on the commission of crime in the premises. According to the participants, a lack of resources meant that they were not fulfilling the tasks as anticipated. Some of the participants said:

> *"To be honest, in terms of combating crime, we don't have resources"* **P13** (Security Officer**).**
>
> *"… we don't have any resources up to so far"* **- P16** (Technology).
>
> *"… we do not have resources"* **- P18** (Senior Inspector).
>
> *"… we don't have enough resources to combat crime"* **- P4** (SO).

It is clear from the participants that it is not practically possible to reduce security threats and vulnerability at these gates without sufficient manpower and the availability of the necessary resources.

(b) Employee negligence on security related issues

The participants were of the view that one of the security threats at Medupi is employee negligence. Employee negligence is not supported by literature therefore it will add to the existing gap in the literature. The following are some of the views of the participants:

"… they're mostly getting stolen as a result of negligence from the site" **P7** (Security Officer).

"… as well as negligence …" **- P11** (Intelligence).

"The other issue is of negligence and ignorance on security issues" **- P12** (SO).

It is clear from the participants that employees, including contract workers, are negligent about security threats and vulnerabilities.

(c) Sharing of computer passwords

A concern regarding theft of information is caused by people who share passwords. The sharing of computer passwords is not supported by literature. Some of the participants indicated:

"So if I want to, I want to get your password, I can see. I know some of the passwords are like that" **- P15** (SO).

"… stolen credentials, as stolen passwords, are the simplest and most common causes of data breaches and criminals and hackers might gain access to sensitive information …" **- P8** (Senior Inspector).

"This is a serious concern, because people can get information that they should not have; they access computer as they share passwords" **- P1** (SO).

The participants felt that unauthorised access to sensitive information is a major threat to Medupi. People share passwords while some hack the system to get access to information.

(d) Cutting of the fence

According to the participants, criminals gain access into the premises by cutting the fence. This theme is not supported by literature and therefore relies on evidence from the participants. It will thus add to the existing gap in the literature. Some of the participants indicated:

"… and people who are cutting fence to access the NKP" **- P14** (SO).

"… they are cutting the fence in order to gain access in order to steal the cable or the material or the vehicle and stuff like that" **- P9** (SO).

"… the people are cutting the fences and get into the site" **- P16** (Technology).

The participants felt that the type of fence and the manner in which it is constructed does not deter criminals from accessing the premises.

4.3.1.3 What are the security measures at Medupi?

According to the participants, the following are the security measures that exist at Medupi:

Theme 4: Types of security measures

(a) Boom-gate

The participants indicated that there are boom-gates at some of the entrances to the premises. A boom gate system is an automated vehicle access at the access control point. It is a gate that automatically opens for a specific period of time and then closes (Enokela & Tyowuah, 2014:86). Some of the participants indicated:

"… all entrances have boom-gates …" **- P8** (Senior Inspector).

"… boom-gates are used for access control" **- P16** (Technology).

"If boom-gates are effective, they facilitate smooth access control to the site" **- P5** (SO).

"*Boom-gates allow for simple access to Medupi"* **- P18** (SO).

According to these participants, access to the premises is controlled by the use of boom-gates. Prior to using the boom gate, a person driving a vehicle must satisfy the security officers at the gate to qualify for such entrance. Only then is access granted.

(b) Security officers

One of the security measures in Medupi is security officers. The role of security officers is to conduct patrols to ensure that everything is in order and report the findings to the occurrence book (OB). Security officers play a fundamental role in reducing crime and increasing detection (Ariel, Bland & Sutherland, 2017:3). Some of the participants said that:

> *"… security officers are deployed …"* **- P10** (Security Officer**).**
>
> *"… security officers patrol the area and report the incidents to the supervisor"* **- P1** (SO).
>
> *"… the role of security officer is to ensure high visibility on entry points by conducting search and screening of personnel"* **- P8** (Senior Inspector).
>
> *"… security officers must also escort individuals that gained access to vulnerable assets …"* **- P16** (Technology).

According to the participants, security officers are one of the security measures employed to reduce threats and vulnerabilities within the premises of Medupi Power Station.

(c) CCTV surveillance cameras

CCTV surveillance cameras were indicated as one of the security measures to reduce threats and vulnerabilities at the premises. CCTV cameras enable the operators to observe suspicious behaviour, people, vehicle and objects (Mahambane, 2017:50). CCTV improves the rate of arrest and ensures successful prosecution of offenders by facilitating the effective deployment of security officers and the gathering of evidence (Moyo, 2019:63). The participants indicated that:

> *"… we are using the CCTV camera to monitor"* **- P4** (SO).
>
> *"… we also use CCTV …"* **- P18** (SO).
>
> *"… by monitoring a CCTV camera …"* - **P11** (Intelligence).

The participants were vocal about the fact that they use CCTV cameras to reduce

threats and vulnerabilities at the premises.

(d)Turnstile as part of access control measure

The participants indicated that, at the access control point, they use turnstiles as one of the security measures used to reduce threats and vulnerabilities at the premises. According to Mahambane (2017:4), access control is the means by which people are granted or denied access to restricted areas. This means that unauthorised people do not have access into the premises (Borham et al, 2016:4). Some of the responses from the participants are that:

> *"… turnstiles which people are using when entering and leaving the site …"* **- P6** (Senior Manager).

> *"… we use a turnstile to control our employees"* **- P12** (SO).

> *"… we have a turnstile whereby access control …"* **- P3** (SO).

It is evident from the participants that they use turnstiles at the premises to reduce threats and vulnerabilities.

(e) Access cards

The use of access cards to control access into the premises was mentioned. The following are some of the responses from the participants:

> *"… the access control, with access card …"* **- P7** (SO).

> *"… access card that is being issued by the security upon such person's production of an ID or passport …"* **- P14** (SO).

> *"… the use of an access card …"* **- P18** (SO).

It is clear from the participant's responses that the access card is used to control access into the premises.

(f) Electric fence

The participants indicated that an electric fence is used to prevent unauthorised

entry into the premises. The use of electric fences can serve as a preventive measure (Cavalcanti, Grawshaw & Tortato, 2012:299). The following are some of the responses from the participants:

> *"The electric fence that is preventing the intrusion into this to come on site"* **- P6** (Senior Manager**).**
>
> *"… we having electric fences looking at those measures …"* **- P11** (Intelligence).
>
> *"We use electric fences as well"* - **P15** (SO).

The participants are of the view that electric fences are used to reduce threats and vulnerabilities.

(g) Biometrics

According to Sabhanayagam, Ventatesan and Senthamaraikannan (2018:2276), biometric refers "to certain physiological or behavioural characteristics that are uniquely associated with a person. For example, face, iris, fingerprint, retina, hand geometry and DNA biometrics. The participants mentioned that they also have biometric systems at the gate to control access into the premises. Biometric security measures reduce the opportunities for the commission of crimes (Ariel et al, 2017:1). According to Edure and Adio (2018:2), biometrics are used in different applications to prevent unauthorised access to the use of private information such as ATMs, smart cards, computer networks and desktop PCs, etc. The following are the participant's views on this:

> *"We have a biometric system in place"* **- P8** (Senior Inspector).
>
> *"… and also have the biometric machines at the gate"* **- P17** (Contractor).
>
> *"… also biometric …"* **- P5** (SO).

It is clear from these participants that a biometric system is available at the access control point.

(h) Metal detectors

According to the participants, security officers use metal detectors as one of the access control measures. Some of the participants said:

> *"We are using metal detectors for checking"* **- P1** (SO).
>
> *"Metal detector is the one that we can use at the gate"* **- P9** (SO).
>
> *"Metal detector is the one that you scan when the person is entering the site"* **- P10** (SO).

It is clear from the participants that metal detectors are one of the security measures that they are using for access control.

4.3.1.4 How can power station security officers combat criminal activities at Medupi?

Theme 5: The security officers' role in combating crime

The following categories were identified under this theme:

(a) Conduct regular patrols and attend incidents

According to the participants, combating crime includes conducting regular foot and vehicle patrols and attending to security threat incidents. Some of the participants indicated:

> *"We are always doing patrols around the area"* **- P14** (SO).
>
> *"Sometimes we attend crime incidents that have happened"* **- P3** (SO.
>
> *"Every time, we are patrolling"* **- P18** (SO).

It is clear from the participants that security officers conduct patrols on foot and also in vehicles within the premises.

(b) Strengthen access control measures

An access control point authenticates entry and exit into the facility (Musonza,

2016:56). The participants indicated that they strengthen access control by ensuring that everyone and all the vehicles entering the site are subjected to searches. The responses from the participants indicate states that:

> *"We do access control most of the time"* **- P11** (Intelligence).

> *"Although we have other measures, we also do searches"* **- P9** (SO).

> *"It is important to search all the employees entering, if we can"* **- P7** (SO).

It is clear from the participants that access control measures need to be strengthened by searching all the peoples and vehicles entering the site.

(c) Dishonest security officers

The participants stated that some of the security officers were not honest. In a study conducted by Nkwana (2015:115), it was established that the probability of internal staff getting an opportunity to commit theft was found to be high due to a lack of security control measures. Some of the participants said:

> *"You cannot trust some of the security guards"* **- P2** (Investigator).

> *"They connive with the contract workers to steal cables from the site"* **- P6** (Senior Manager).

> *"One security officer was found stealing without wearing a uniform and disguised as a contract worker"* **- P8** (Senior Inspector).

According to the participants, some of the security officers were regarded as dishonest employees as they were involved in criminal activities when they had a legal duty to protect and serve.

(d) Enforcing compliance with site rules

Combating crime onsite is important because all employees must be compliant with the rules and regulations governing the site. Some of the participants indicated that:

> *"… the employees that are going around within the site ensure that employees are complying with the site rules"* **- P1** (SO**).**

"Officers should ensure that all employees and contractors comply with the rules onsite" **- P5** (SO).

"… officers to ensure that people want to come, they need to comply at all times" **- P13** (SO).

"Compliance also includes compliance with the Occupational Health and Safety Act of the government" **- P16** (Technology).

According to the participants, security officers ensure that anyone entering the site should comply with the regulations.

(e) Inability to deal with suspects that are armed

The participants indicated that one of the challenges of their duties is that they were not able to deal with armed suspects since they were not armed. This theme was not supported by literature. Some of the participants indicated that:

"…our guys that are under threat or they've been attacked because they don't have resources" **- P9** (SO).

"You cannot approach armed suspects empty handed" **- P14** (SO).

"This puts our lives in danger because we are not armed" **- P10** (SO).

According to the participants, it is difficult to arrest an armed suspect due to the fact that security officers are not armed. This poses a serious threat to the lives of the security officers and also puts the assets of the Medupi in serious danger.

Theme 6: Participants' experiences of combating crime

This theme identifies the participants' understanding of their role in combating crime. The following categories emanated from this theme:

(a) Ensure that all equipment and personnel are protected on site

The participants indicated that their role is to ensure the protection of all the people and assets on site. Some of the participants indicated:

"What I want to see that everything here should be protected" **- P8** (Senior Inspector**).**

"There is a need for the protection of all assets and all the people" **–P17** (Contractor).

"All the people and assets have to be protected by security officers" **- P1** (SO).

According to the participants, protection of all the assets and people on site is required.

(b) Sharing information with the police

The participants indicated that all crime related information is shared with the police so that they can conduct investigations and effect arrests. This theme is not supported by literature. It is clear that there is dearth of literature on this theme. Some of the participants indicated:

"When there is something that requires the police, we call them" **- P6** (Senior Manager**).**

"It is important to work with the police when crime occurs" **- P10** (SO).

"The police come here to arrest those that are committing crimes" **- P18** (SO).

According to the participants, it is necessary to liaise with the police when crime takes place on site.

(c) Foot and vehicle patrol

The participants indicated that they conduct patrols using vehicle and also foot patrol. Some of the participants indicated:

"We also do the patrols" **- P4** (SO).

"… we mentioned the issue of the vehicle patrols" **- P7** (SO).

"During the day, we do foot patrol, and during the night, we do vehicle patrol" **- P11** (Intelligence).

It is clear to those participants that they are conducting vehicle and foot patrols on the site.

(d) Encourage team work among members

The participants indicated that they encouraged their security officers to work in teams to support each another. Some of the participants indicated:

"What is important is to motivate employees is to work as a team" **- P5** (SO).

"Working as a team is very important" **- P8** (Senior Inspector).

"It is important that employees are encouraged to work in teams" **- P16** (Technology).

It is clear from the participants that security functions require security officers to work in teams to ensure successful functioning.

(e) Conduct searches when entering and leaving the site

The participants indicated that they conduct searches when employees enter and leave the premises. This is done in order to ensure that no dangerous items enter and employer properties do not leave the premises. Some of the participants indicated:

"… all employees entering the site are properly searched" **- P3** (SO).

"We also check to ensure that no one leaves with the employer's property" **- P9** (SO).

"Searching employees is important in ensuring the protection of the employer's assets" **- P14** (SO).

(f) Tool verification when exit the site

The participants indicated that, in order to prevent crime in the premises, it is important to ensure that tools entering and leaving the site are verified to check if they are stolen or dangerous. Tools are assets and thus every asset has to be verified for its authenticity and also to determine if it is possessed by an authorised person. The participants indicated:

> *"Tools must be verified if they are not stolen from the site"* **- P1** (SO**).**
>
> *"It is necessary to verify the tools that employees are found to be in possession with"* **- P5** (SO).
>
> *"… and also verify the tools in possession of any person"* **- P17** (Contractor).

It is clear from the participants that all tools must be verified.

(g) Prevent any threat to the safety of people and assets

The other role that the participants play is to ensure that all threats to the safety of the assets and people on site are prevented. Physical security threats may come from the internal staff, such as security officers, contractors and trusted employees (Borham et al, 2016:4) as some of the participants indicated:

> *"… it is to ensure that all the people are working on an environment free from threat"* **- P16** (Technology).
>
> *"Threats should be eliminated at all costs"* **- P7** (SO).
>
> *"We have to remove all the threats and potential dangers to ensure the safety of the people and assets"* **- P12** (SO).

It is clear from the participants that anything that poses a threat to the safety of the people and assets should be eliminated.

(h) Enhance compliance with policies, procedures and directives

The participants indicated that they played the role of ensuring that the employees

on site comply with policies, procedures and security directives. Some of the participants indicated:

"People must comply with the law all the time" **- P2** (Investigator).

"It is necessary for compliance here" **- P6** (Senior Manager).

"Compliance to the law and rules is important to adhere to" **- P9** (SO).

The above participants indicated that they ensured that all the employees were adhering to the rules and regulations, as well as the legislative framework.

(i) Ensure alarms are functional

The participants ensure that all the alarms on site are functional. This includes reporting to the management and ensuring that they are properly fixed. Some of the participants indicated:

"All the alarms are working" **- P3** (SO).

"The alarms are always problematic, but must make sure that they are working" **- P8** (Senior Inspector).

"We must ensure that alarms are in good conditions all the time" **- P17** (Contractor).

It is clear from the participants that the alarms are effective at all times.

(j) Doors closed and locked

According to the participants, they ensure that all the doors are closed and locked after hours. It is clear from the evidence that doors must be kept locked when there is nobody in the space. Some of the participants said:

"When we patrol, we must close all doors that are left open" **- P1** (SO).

"Close all the doors" **- P5** (SO).

"All doors must be closed" **- P10** (SO).

The participants indicated that all the doors that are left open are closed by the security officers during patrol.

(k) Educate visitors on the violation of access control procedures

The participants indicated that they ensure that all employees and visitors are educated on access control procedures at the access control point. Some of the participants indicated that:

> *"All visitors must be educated about the access control"* **- P7** (SO).

> *"… anyone entering must be informed of the procedures"* **- P12** (SO).

> *"Educating them about access control is important"* **- P18** (SO).

It is clear from the participants that one of their roles is to ensure that visitors are educated about access control measures.

Theme 7: Methods or strategies to combat crime

The following categories were identified for this theme:

(a) Encourage healthy work relationships

According to the participants, in order to combat crime, they encourage their subordinates to perform better by having healthy working relationships. This includes open communication regarding work and home situations that may impact negatively on their performance. Some of the responses from the participants were:

> *"… we are working having a very close relationship with …"* **- P2** (Investigator).

> *"… and close relationship and report suspicious activities for relevant authority …"* **- P9** (SO**).**

> *"… We have a very good relationship [so] that we communicate on a regular basis and show each other the importance of keeping the information …"* **- P11** (Intelligence).

The participants indicated that they motivate their employees to perform their tasks.

(b) Encourage reporting of suspicious activities

The participants were of the view that they encourage their subordinates to report suspicious activities to combat crime. Some of the participants said that:

> *"… to encourage them all the time to encourage them to report"* **- P9** (SO**).**
>
> *"… inform and encourage employees to report any suspicious activities"* **- P15** (SO).
>
> *"… and then my role is to encourage my team. Let's search people when they are entered on site and then when they leave site … we verify tools that they have to try to produce their claim … one can try to commit on our side"* **- P1** (SO).

(c) Monitor movements and details of people and vehicles entry onsite

According to the participants, their role is to ensure that all the movements of the people and vehicles are closely monitored while in the premises. Some of the participants said that:

> *"… monitoring the movements and details of people and vehicles and also taking note of the vehicle make and the registration as well as personnel closing"* **- P7** (SO).
>
> *"Check the warehouses; check the movement of the person inside"* **- P18** (SO).
>
> *"If there was any movement, we have to know immediately"* **- P10** (SO).

It is evident that the participants ensure that they keep records of the movement of vehicles and people on site.

(d) Using personnel identification cards

The participants indicated that they were using access cards for access control. Some of the responses were:

"… information by verifying the access card …" **- P4** (SO).

"I must ask the access card for the person who look for a key to check and record the relevant information on the register" **- P14** (SO).

"… people used to place the card on the machine and gain access" **- P8** (Senior Inspector).

"… access card ensures that anybody without card means that person must not be allowed on site" **- P3** (SO).

(e) CCTV surveillance cameras

The participants revealed that they use CCTV surveillance cameras in addition to the police to combat personal and property crimes on site (Moyo, 2019:74). According to Johnsen and Stene (2016:305), CCTV cameras can be used as a proactive control tool to deter incidents of crime and also to learn by finding and analysing a situation after it has taken place. Some of the participants indicated that:

"… effective entity such as this, we have reliable surveillance cameras at all times" **- P15** (SO).

"… we are having CCTV camera in the control room" **- P16** (Technology).

"And we also have monitoring for our CCTV cameras by security control office" **- P6** (Senior Manager).

"… efficient CCTV cameras are in place in and around Medupi" **- P11** (Intelligence).

"… we use the monitoring CCTV cameras" **- P13** (SO).

According to the participants, CCTV is one of the security measures that they use to combat crime on site.

(f) Patrols

According to the participants, patrols combat crime on site. Some of the participants indicated:

"Regular patrol at the night is conducted" **- P8** (Senior Inspector).

"… almost make sure that I patrol the premises" **- P12** (SO).

"… make sure that we use our vehicle to patrol the premises" **- P15** (SO).

"We also have to conduct patrol at the fence" **- P2** (Investigator).

"… conducting patrols at the crime hotspots" **- P9** (SO).

The participants indicated that they patrol the area using vehicles. They also conduct patrols at crime hotpots. The purpose of patrols is to identify anomalies occurring in the premises and to ensure that those responsible are held to account.

(g) The use of metal detectors

The participants indicated that they used metal detectors for access control. Some of the participants said that:

"… metal detector, we use to scan when the person is entering the site" **P7** (SO).

"Metal detector is the one that we can use it the gate" **- P13** (SO).

"… we're using, detectors, metal detectors for checking all those stolen cables, we were using" **- P5** (SO).

"Those are the reasons you're using metal detectors" **- P1** (SO).

According to the participants, metal detectors at the access control play a role in combating crime before it enters the site.

Theme 8: Resources required to combat crime

The purpose of this question was to explore the type of resources that the participants need to reduce threats and vulnerabilities in the Medupi Power Station. The following are the sub-themes under this theme:

(a) CCTV surveillance cameras

According to the participants, they require resources, such as CCTV cameras that are functional at all times, to be able to do their jobs. CCTV cameras are targeted at places where there are entrance and exit doors (Moyo, 2019:66). The role of CCTV cameras is to provide evidence that can be used during investigations of crime (Ashby, 2017:4). They also protect members of the public from harm (Kurdi, 2014:199). Some of the participants said that:

> *"… those cameras … that can view anything that can cause harm to the … post issue, should be effective, monitored and fixed"* **- P18** (SO).

> *"The cameras must always be on. And then it must be someone on the camera room monitoring people"* **- P2** (SO).

> *"CCTV cameras are needed to play a role in here"* **- P8** (Senior Inspector).

It is evident from the participants that they need effective CCTV cameras that are functional. Cameras need to be properly maintained in order to be functional at all times.

(b) Security alarm systems

The term security is defined by Borham et al (2016:2) as "the quality or state of being secure which means to be free from danger". The participants indicated that they must have alarm systems to send a signal so that they are able to respond. Some of the participants said that:

> *"If we can have alarms, the better"* **- P11** (Intelligence**).**

> *"We should get alarm systems to be installed and people should be able to respond to it immediately"* **- P6 (Senior Manager).**

> *"You see, alarms are good, to have it can assist us a lot"* **- P5** (SO).

(c) Locking systems for doors and windows

The participants were of the view that there must be effective locking systems for both the windows and doors to prevent intruders. Some of the participants said:

"… so that we will lock the doors and windows to prevent people entering the warehouse to steal" **- P10** (SO).

"… and locked with it; maybe with lock all the doors in our warehouse area" **- P17 (**Contractor).

"… upgrading the locks on doors, windows and outbuildings" **- P7** (SO).

According to the responses from the participants, there it was necessary for the protection of assets by upgrading the locking system. The most inexpensive door locks are easily breached by anyone with knowledge of its weaknesses (Henage & Henage, 2013:84).

(d) Two-way radio communication

The participants indicated that it is important to have two-way radios to enhance their communication about problems related to threats and vulnerabilities. They indicated that:

"… the two-way radio is an essential means for communication" **- P1** (SO).

"Having radio communication is important to communicate about crime" **- P8** (Senior Inspector**).**

"Through two-way radio, we able to respond to the crime incident quicker" **- P16** (Technology).

According to the responses of the participants, two-way radio communication is necessary for the security officers to communicate. It is important that all security officers must be equipped with two-way radios to communicate amongst each other (Visser, 2015:54).

(e) Flashlight torches

The participants voiced the value of having flashlight torches. Some of the participant's responses were:

"… and then others are torches to check during the night" **- P5** (SO).

"During the night we are struggling, we are even afraid of patrolling because we do not have torches" **- P13** (SO).

"If we can have torches, [we] will be able to patrol much easier rather than to put our lives in danger during the night" **- P9** (SO**).**

(f) Digital cameras to use during patrol

"I think it is important if we can get digital cameras to record all the incidents at that particular time, maybe can serve as evidence" **- P3** (SO**).**

"The use of digital cameras will make our work a lot easier" **- P8** (Senior Inspector**).**

"And the digital camera is essential during patrols where CCTV cameras are not installed" **- P4** (SO).

It is clear from the participants that it is important to have digital cameras that they can use during patrols to record the events that they observe.

(g) Pocket book

The participants indicated that they should be given pocket books to record events when conducting patrols. The following are verbatim statements from the participants:

"… as well as having a pen and a pocket book to provide reports, observations and incidents or get on site in during our patrol" **- P7** (SO).

"It is necessary for the officers to be equipped with pocket books so that it corresponds with OB" **- P6** (Senior Manager).

"Pocket books can be used to record anything that the security officers observe during patrol within the premises" **- P11** (Intelligence).

(h) Night vision cameras

The participants indicated that they require night vision cameras to be able to capture events in the dark. Some of the participants indicated that:

"… because a few have a night vision camera, you can see on the people who are trying to enter …" **- P10** (SO).

"And the night vision camera will normally be used, especially in the bush, where we do patrols around the dam …" **- P16** (Technology).

"There are a lot of trees, there are a lot of elements that site or tents or people can try to hunt those animals at night. So we monitor that through the night vision camera to reduce people who are hunting" **- P18** (SO).

According to the participants, the use of night-vision cameras can be helpful for them when they do patrol during the night especially in places where there are no cameras, such as the dam.

(i) Firearms and bullet proofs vests

The participants indicated that firearms and bullet proof vests are necessary in order to protect themselves against armed suspects. Copper cable thieves are careful about their planning and also carry firearms, which requires security officers to be armed (City of Tshwane, 2016:2). Some of the participants indicated that:

"And bullet proofs are required so we wear them at all times" **- P17** (Contractor).

"… then the bullet proofs are important for use as security officers" **- P14** (SO).

"If we can have bullet proofs, we can save our lives from criminals who are armed" - **P5** (SO).

"They should at least give us firearm" **- P13** (SO).

"We must be provided with firearms to protect ourselves from the thugs" **- P10** (SO).

The participants were of the view that the firearms and bullet proof vests protect them against armed criminals.

Theme 9: The challenges experienced when combating crime

The participants indicated that they experienced many challenges when combating crime that include: employee negligence, leaving valuable items, such as laptops, unattended; warehouses and offices left open; fences that are cut to gain access into the premises and community members who collect firewood in the premises. Another challenge is that security officers do not have sufficient resources to enable them to perform security functions that include patrolling dark areas during the night without torches. The participants reported that requests for resources are ignored by the management. There is also lack of cooperation between employees, security and contract workers. Some of the responses from the participants said that:

> *"Some employees do not care about us when doing our duties"* **- P12** (SO).
>
> *"Sometimes when we conduct patrol, we found warehouse left open and valuable resources not attended or kept in a safe place"* **- P6** (Senior Manager).
>
> *"The suspects were arrested for cutting the fence when they want to enter the premises with the intention to commit crime"* **- P11** (Intelligence).
>
> *"What makes things worse is that we don't have the necessary resources to perform our functions as security officers"* **- P8** (Senior Inspector).

It is clear from the participants that there are many challenges when performing security functions.

(a) Suggestions for best practices to combat crime

The participants suggested that more security officers were required to improve security on site and that a contactor must be appointed to maintain surveillance cameras. The participants felt that the best practice is to enforce the law when performing security functions. It is important for the management to reprimand employees who come to work while under the influence of alcohol and drugs. It is necessary to ensure that the participants are provided with sufficient resources, such as firearms, pocket books, bullet proof vests, etc. Anyone involved in criminal activities within the premises should be arrested and handed over to the police.

Some of the participants indicated that:

> *"Security officers should be enough to be able to perform security duties during the day and the night"* - ***P1*** (SO).
>
> *"Management must be at the forefront of security, they must have buy-in into the security issues"* **- P7** (SO).
>
> *"No, the problem is management, people must not come to work drunk, no, is not allowed"* **- P13** (SO).
>
> *"These people are not considerate of the security and their duties"* **- P11** (Intelligence).
>
> *"We cannot allow criminal activities; we should be able to arrest everyone involved in crime"* - **P10** (SO).

The participants suggested that security patrols should be conducted three times during the day and three times during the night. It was also suggested that management should be on board regarding security issues. The participants also suggested that steps should be taken against those who report for duty while under the influence of alcohol or drugs.

4.3.1.5 What are the causes of the security threats and vulnerabilities to the power station?

The purpose of this question was to explore the participants' views on the causes of security threats and vulnerabilities.

Theme 10: The causes of security threats and vulnerabilities to the power station

The participants believed that there were many causes of security threats and vulnerabilities faced at the Medupi that included:

(a) Unauthorised employee absenteeism

Unauthorised absenteeism takes place when an employee is absent without prior permission from the employer (Singh, Chetty & Karodia, 2016:107). Some of the

participants indicated that unauthorised employee absenteeism is rife at the site on weekends and month ends:

> *"… absenteeism is at highest on weekends, and month end"* **- P12** (SO).

> *"Employees are not showing up when they got paid"* **- P17** (Contractor).

> *"They are always not coming to work when they are supposed to"* **- P3** (SO).

According to the participants, employee absenteeism is a serious concern because it affects production of the power station.

(b) Employee negligence on security related issues

The participants were believed that employee negligence is among the causes of threats and vulnerabilities as it results in the theft of equipment. Some of the participants said:

> *"The other issue is of negligence and ignorance of present"* **P11**(Intelligence).

> *"Employee negligence is a serious problem here"* **- P6** (Senior Manager**).**

> *"They are not serious, this is negligent"* **- P2** (Investigator).

> *"… stubborn employees questioning the authority of officers were performing duties on the ground"* **- P18** (SO).

> *"… they are leaving those appliances lying around"* **- P12** (SO).

> *"They're just leaving their tools"* **- P6** (Senior Manager).

> *"… they're not taking care of those appliances; they are leaving those appliances lying around"* **- P2** (Investigator).

> *"And the door is wide open without locking the door and making sure that everything is safe"* **- P9** (SO).

> *"… we are not taking our job seriously because we have to take our drop*

serious" **- P17** (Contractor).

Another participant said that negligence was due to a lack of discipline:

"… due to lack of discipline and motivation" **- P1** (SO).

"People do as they please" **- P13 (SO).**

"… there is no discipline, for instance" **- P4** (SO).

It is clear from the participants that negligence by employees contributes to threats and vulnerabilities.

(c) Lack of sufficient security personnel

According to the participants, there are insufficient security officers to perform security functions in an effective and efficient manner. Some of the responses of the participants were:

"… sometimes you find out that maybe you don't give them enough manpower to maintain the relevant posts where people are waiting" **- P9** (SO).

"And the size and capabilities of security staff that we have on site" **- P15** (SO).

"We are very few security officials to do security work" **- P8** (Senior Inspector).

"Looking at the number of people, how big the company is, with limited security officers is difficult" **- P5** (SO).

"… we have a shortage of manpower after peak hour" **- P16** (Technology**).**

"We cannot safeguard this, this kind of power station with four officers during the night or four officers during the day" **- P11** (Intelligence).

According to the participants, the number of security deployed is inadequate to perform security functions and that this contributes to the causes of security threats

and vulnerabilities.

(d) Leakage and improper protection of information

The participants maintained that improper protection of information contributed to security threats and vulnerabilities. Nkwana (2015:55) indicates that, should information be leaked by an employee, the impact will affect the objectives of organisation causing harm. Some of the participants indicated:

> *"According to my understanding is the issue of not protecting information"* **- P11** (Intelligence).
>
> *"Caused by some of our officers who can fail to protect the information on our station"* **- *P1*** (SO).
>
> *"They are sharing information, sharing sensitive information with the people who are not in security department …"* **- P10** (SO).
>
> *"Someone can take his USB and then enter the server room and then took the information from that who is on the server"* **- P18** (SO).

It is clear that the leakage of information by employees was a serious concern for the participants as it can be used to the disadvantage of the employer.

(e) Lack of budget on security measures

The participants indicated that the management of Medupi does not allocate sufficient funds for the security measures. The major risk that contributes to ineffectiveness of security risk control measures was budgetary constraints (Nkwana, 2015:116). Some of the participants indicated that:

> *"…station lack of money to fund security measures to prevent crime"* **- P4** (SO).
>
> *"…the problem is lack of budget"* **- P8** (Senior Inspector).
>
> *"…they are not giving any money for security functions"* **- P7** (SO).
>
> *"…the employer is valuing more money than to protect the site"* **- P13**

(SO).

It is clear from the participants that budget constrains contributes to the causes of security threats and vulnerabilities at Medupi Power Station.

(f) Poor management and communication

The participants indicated that poor management is characterised by a lack of effective communication with employees. In a study conducted by Pretorius (2012:170), findings indicated that top management should be responsible for security as some of the participants noted:

> *"… that poor management in this station is a serious problem"* **- P18** (SO).

> *"… poor communication can cost the station too much"* **- P3** (SO).

> *"Communication is difficult especially to us. As security officers, we need that daily"* **- P10** (SO).

> *"Knowing what to do on a daily basis; start strategising our daily duties"* **- P11** (Intelligence).

> *"We are trying by all means to engage our supervisors and managers about the challenges that we're having here. But it takes a long time to come [back] to us"* **- P8** (Senior Inspector).

It is clear from the participants that poor management is characterised by a lack of communication. This negatively impacts the performance of the security officers.

(g) Improper search due to a lack of manpower

The participants indicated that a lack of manpower restricted them from conducting thorough searches of people entering and leaving the premises. People are therefore able to go inside with dangerous objects and also to leave with property stolen from the employer without being searched. Some of the participants said:

> *"We are not doing a thorough searching because of shortage of manpower"* **- P17** (Contractor).

"… shortage of manpower gives people opportunity to bring with them things [that] are not required" **- P1** (SO).

"Manpower problem has been a challenge for a long time" **- P15** (SO).

It is clear from the participants that an insufficient number of officers pose a serious challenge to the safety and security of people and assets at the Medupi Power Station.

(h) Theft committed by contract workers

According to the participants, contract workers are responsible for the number of threats and vulnerabilities within Medupi. Some of the participants noted:

"They are involved in theft of laptops and other equipment used by the contractors" **- P13** (SO).

"… thief can come and over overpower those at the gate and get access" **- P1** (SO).

"… we've had complaints from subcontractors that people are stealing stuff" **- P7** (SO).

"Most of the people are contractors who are working with those cables or copper and they steal them" **- P12** (SO).

"… and contractors … are always found to be in possession of illegal firearms and ammunition" **- P2** (Investigator).

"And then, on the issue of nonferrous metals, such as copper cable, mostly is committed by contractors" **- P5** (SO).

"… when contractors engage in a protest, they end up committing property crimes such as a malicious injury to property" **- P18** (SO).

It is clear from the participants that contract workers were responsible for crimes in the Medupi Power Station.

4.3.1.6 What type of security measures is needed to reduce security threats and vulnerabilities?

Theme 11: Types of security measures to reduce security threats and vulnerabilities at Medupi Power Station

In this question, the participants were expected to explain the types of security measures to be installed to prevent threats and vulnerabilities effectively and efficiently. The following are some of the categories that emerged on this question:

(a) The use of one gate for all personnel

The participants agreed about the problems of the use of multiple gates and they suggested that the number of gates be reduced so that the movement of people and vehicles can be effectively controlled even though there was a shortage of manpower and resources. This theme is not supported by any evidence from the literature therefore it will add to the existing gap in the literature. Some of the participants said that:

> *"… maybe the main thing is to use only one gate, then we can manage to search and do proper security work"* **- P3** (SO).

> *"… they may decide to have one gate and then the crime will be combated"* **- P6** (Senior Manager).

> *"Using one gate makes the job easier with high impact in combating crime"* **- P12** (SO).

It is clear from the participants that many gates compromise the security of the assets and people. They suggested that the number of gates be reduced to a manageable size.

(b) Deploy more manpower to ensure effective patrols

The participants suggested that there was a need to recruit more officers to perform security functions in a more effective and efficient manner. Some of the participants said that:

"… we don't have enough manpower to deal with the challenges we are facing" **- P18** (SO).

"… if we can have the ones that can be broken by having enough manpower for conducting searching at the gates" **- P16** (Technology).

"… enough manpower to maintain the relevant posts where people are waiting" **- P4** (SO).

The participants believed that more manpower was needed to combat crime at the premises.

(c) Patrol all areas three times a day and also during the night

The participants also suggested that an ideal security measure would be to ensure that patrols are done at least three times during the day and at night because cable thieves operate mostly at night (Pretorius, 2012:54). This would increase the number of patrols they currently have. Some of the participants said:

"… routine patrol must be taken at least three times a day and three times during the night that can help to minimise…" **- P13** (SO**).**

"I want to see vehicles patrolling" **- P11** (Intelligence**).**

"I want to see people that are driving at high speed on a plant can discipline for them they see people that are driving unworthy vehicles on the … plant, also be disciplined" **- P7** (SO).

The participants indicated that patrols should be conducted three times during the day and at night to assist in reducing crime through security visibility.

(d) Effective communication and two-way radio communication

The participants desired effective communication, amongst themselves, employees and management. Some of the participants indicated that:

"I mean, like engaging each other, having the meeting together" **- P1** (SO).

"I think [it] is where we can talk to each other" **- P12** (SO).

"The more meetings we can have will reduce lot of uncertainties and increase the level of trust" **- P6** (Senior Manager**).**

The participants said that there was a need for effective communication between all the role-players in security that include security officers, management and employees within Medupi. In terms of radio communication, some of the participants said that:

"… anytime or mostly anytime, but especially where you may find that there is an incident or an irregularity that we want to communicate about" **- P13** (SO).

"… and effective communication" **- P4** (SO).

"… so we need effective methods and effective communication if there are emergencies to understand; so that they spend must be less than 10 minutes to the site. So, but so that it can stop people from damaging the property" **- P9** (SO).

"… use the two-way radio is an essential means for communication" **- P11** (Intelligence).

It is clear from the participants that communication is the key to productivity. They believed that, where there is effective communication, there are fewer uncertainties and an open-door policy.

(e) CCTV surveillance cameras

According to the participants, there was a need for the installation of CCTV surveillance cameras around the premises. According to Moyo (2019:5), CCTV cameras are used as solution to security problems in crime prevention and control. CCTV cameras also play a role during evidence gathering (Visser, 2015:44). The participants viewed CCTV as an effective tool to enhance the protection of assets and people. Some of the participants indicated that:

"… CCTV cameras can be installed in all the places and be monitored by

two officers" **- P3** (SO).

"… for having CCTV camera in the control room, and that control room supposed to be operational …" **- P9** (SO).

"The cameras must always be on and then it must be someone on the camera room that is looking around the side 24/7" **- P10** (SO).

"… then monitor the CCTV so that people must not for anything out of fence" **- P17** (Contractor).

"CCTV cameras are in place in and around Medupi to assist in in physical security" **- P18** (SO**).**

"… we need to have camera systems around the perimeter fence" **- P11** (Intelligence**).**

The participants indicated that having CCTV cameras around Medupi would impact positively on combating crime.

(f) Provision of sufficient manpower and resources

The participants believed that there was a need for more manpower and resources to enable the effective functioning of security officers. Some of the participants indicated that:

"… my manager for applying to heavy enough resources we are using … for conducting proper duties" **- P12** (SO).

"… not working without full manpower" **- P15** (SO).

"… must maintain more manpower because it's the national. This power station is maintained by the country so it needs more protection than anything" **- P2** (Investigator).

"… having enough security officers perform their duties without fear …" **- P8** (Senior Inspector).

According to the participants, there was a need for more personnel in the security

department to be able to perform security functions.

(g) The use of law enforcement and external private security investigators

The participants' responses indicated that, once a crime has occurred, there is a need for the use of the police and investigators from the private security industry. It is important that investigators from both the police and security industry get involved in the collection and analysis of information about crimes (Lutchminarain, 2015:54). This is an integrated approach to solving crime in the premises. Shuping (2018:1) asserts that, in November 2016, the security officers and private investigators contracted by ESKOM were combined to arrest the accused after they were found cutting copper cable. Some of the participants felt that:

> *"… so that they can call the police to come in take arrest that person …" -* ***P1*** *(SO).*
>
> *"I want to see arrests being made"* ***- P11*** *(Intelligence).*
>
> *"We must work together with both the police and security investigators"* ***- P16 (****Technology).*

According to the participants, there was a need for an integrated approach with other law enforcement agencies to assist security officers when crime has taken place.

(h) The need for the technology to detect people far from the fence

The participants suggested that there was a need for technology to detect trespassers around the perimeter fence. This theme is not supported by literature as it only relies on the evidence from the findings. Some of the participants said:

> *"… in this station, we need … advanced technology that can detect … any … trades, a hundred, 1200 kilometres away from the power station"* **- P4** (SO).
>
> *"Though we not know what technology can be used, something needs to be thoughtful for"* **- P6** (Senior Manager).
>
> *"Such technology must detect the potential intruder's movement before*

they enter, so that we can be alerted and prevent them from committing crime" **- P18** (SO).

The participants suggested that, in order to deter the intruders from entering, there is a need for a specific technology that can be used to deter criminals from entering the premises.

(i) Identification mark for all the tools used

The participants suggested that all the tools that are used should be marked so that they are identifiable. Some of the participants indicated that:

"… most tools, when I'm talking specifically for the tool has been mapped, the assets like laptop printer should have been checked, put the checker on it" **- P12** (SO).

"Tools, such as the grinder, should be marked, so that, once is lost, we can check for the mark" **- P13** (SO).

"… for the tools, we can look on a certain mark for a certain company, so that we can get all those tools and detain the criminals" **- P11** (Intelligence).

According to the participants, all the tools used in the premises should be provided with identification in case a tool is lost or is in possession of a certain person who should be identifiable.

Theme 12: Description of the participant's role in the proposed security measures mentioned above

The participants indicated that their role in security measures is to ensure that there is sufficient manpower daily. Some of the participants said that:

"… making sure that we have enough manpower on a daily basis …" **- P7** (SO).

"… and every night, I think it's, we can do lot by ensuring that security functions are performed adequately" **- P1** (SO).

"We cannot safeguard power station with four officers during the night or four officers during the day" **- P15** (SO).

According to the participants, they played a key role in ensuring that everything is in order at all times.

(a) Effective communication

The participants believed that effective communication with security officers is important:

"… effective communication, if there are emergencies to understand, so that they spend must be less than 10 minutes to the site …" **- P5** (SO).

"Security job needs officers to communicate effectively" **- P9** (SO).

"We must ensure that we communicate more and more" **- P18** (SO).

According to the participants, communication plays a fundamental role in the security environment.

(b) Good relationship with security officers

According to the participants, there was a need for the managers to have good relationships with the security officers. Some of the participants said that:

"… inform and encourage employees …" **- P10** (SO).

"… o have a good and close relationship" **- P4** (SO).

"… we need to have a very good relationship that we communicate on a regular basis and show each other …" **- P17** (Contractor).

According to the participants, a good relationship with security officers is important because, when they are motivated, they to perform their duties well.

(c) Motivate the security officers

According to the participants, there was a need to motivate the security officers to perform their duties as motivation can increase employee performance (Singh et al,

2016:107). Some of the participants indicated that:

> *"… you must motivate your guys when you work with so that they can have energy on whatever they are doing …"* **- P3** (SO).

> *"… motivate your staff, so that they must not feel or they are not welcome on your site; they must feel happy when they wake up every day go into it, they must know we are going to do our job"* **- P7** SO).

> *"Motivate them to do the work"* **- P10** (SO).

According to the participants, motivation was important in boosting the moral of the security officers so that they were able to conduct their duties with the necessary energy. Participants said that:

> *"Say thank you very much what a good job done, well done"* **(P6).**

> *"You've got to be humane as well and we've got to treat our security as humans"* **- P11** (Intelligence).

> *"… we cannot treat them like having to say when you employ monkeys, I mean, you employ monkeys, you're gonna pay peanuts to do the job"* **- P16** (Technology).

4.4 Conclusion

The purpose of this chapter was to discuss and interpret the findings of responses received from participants during the interview sessions. In terms of the demographic make-up of the participants, most of them were married and aged between 38 and 42 with certificates as their qualifications. During the data analysis phase, the researcher identified twelve themes and several categories arising out of the data analysis process.

In summary, criminal activities at Medupi Power Station emerged as a significant theme, in particular, crimes such as theft of copper cable and theft of working tools emerged as categories from the participants during analysis of the data.

In another theme, participants described the different modus operandi of crimes

committed at Medupi and categories, such as smuggling of stolen goods, were identified. Almost all the participants indicated that employees cut copper cables into pieces and rolled them to fit in either a bag or a two litre Coke bottle to smuggle them out of the power station.

Identification of security threats and vulnerabilities was another theme identified in the study. The participants believed that security threats and vulnerabilities at Medupi are high even though a number of security measures exist at Medupi such as boom-gates, security officers, CCTV surveillance cameras, turnstiles, access cards, electric fences, biometrics and metal detectors. Under the theme of the security officers' roles in combating crime, the following categories were identified: conduct regular patrols and attend to incidents, strengthen access control measures, enforce compliance with site rules and their inability to deal with armed suspects.

Participants' experience of combating crime was another important theme identified in the study. Some of the categories recognised were, inter alia, ensuring that all equipment and personnel are protected on site, sharing information with the police, more foot and vehicle patrols and encouraging team-work among members. Methods or strategies to combat crime was another theme and the following categories were identified for this theme: encouraging healthy work relationships, encouraging the reporting of suspicious activities, monitoring movements and details of people and vehicles on site, using personnel identification cards, CCTV cameras and patrols.

Under the theme of resources needed to combat crime, categories, such as CCTV surveillance cameras, security alarm systems, locking systems for doors and windows, two-way radio communication, flashlight torches and digital cameras were some of the categories identified in the study. In another theme, the challenges experienced when combating crime, the participants indicated that they experienced many challenges when combating crime including employee negligence, leaving valuable items such as laptops unattended and warehouses and offices open. The type of security measures to reduce security threats and vulnerabilities at Medupi Power Station was another theme identified in the study.

The study also indicated that criminals are using different modus operandi to steal

copper cables and commit a variety of other crimes at Medupi Power Station. Therefore, reducing the threats and vulnerabilities will impact positively not only on the security department and management, but also on the country as a whole.

CHAPTER 5
SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The purpose of this chapter is to discuss the conclusions and recommendations of the study as guided by the findings of the study. The aim of this study was to evaluate security threats and vulnerabilities confronting the Medupi Power Station in the Limpopo Province as a Critical Infrastructure, in order to improve existing security measures at the power plant. The research approach for this study was explorative in nature. The researcher employed a qualitative research design for this study because the topic under study was not exhaustively researched and there is limited information on security threats and vulnerabilities confronting the Medupi Power Station as a Critical Infrastructure.

For this study, the researcher used purposive sampling to select the sample as only participants who had knowledge and experience of security threats at Medupi Power Station were included. Eighteen (18) participants who were purposively selected agreed to participate and they included senior managers, security officers, investigator, intelligence, technology, senior inspectors, and contractors.

5.2 Summary of findings

The participants' responses indicated that copper cable theft and theft of working equipment's are on the increase in the Medupi Power Station. It was revealed that the modus operandi used to commit copper cable theft is to cut cables into pieces and put them in bags, place them in two litre Coke bottles and even lunch boxes. This is a new finding that will to add to the existing gap in the literature. The stolen cables are smuggled by hiding them inside the bonnet of their vehicles. This is also a new modus operandi which is not supported by the literature. Some smuggle it under the seat of a bus or wrap stolen cables around their body parts, such as on the legs covered by trousers and on the body covered by clothes. This type of modus operandi lacks support from the literature which renders it to be a new theme as emerged from the findings. In addition, copper cables are also stolen inside and

thrown over the fence for later collection, either at night or to be collected by their accomplices. Criminals also cut fences to get access to premises to commit other crimes.

The findings also revealed that in order to reduce crime on site, security officers perform searches of vehicles and persons, and also carry out foot and vehicle patrols. The responses showed that security officers use CCTV surveillance cameras and access control measures to reduce crime. The study found that the security threats and vulnerabilities that occur at Medupi are caused by the use of more than one gate due to a lack of resources, employee negligence and sharing of computer passwords.

The participants revealed that some of the security measures that are available at Medupi are: boom gates, security officers, CCTV surveillance cameras to monitor the movement of people entering and leaving the premises, turnstiles to control access at the gate, access cards to ensure that only authorised people enter the premises, electric fences and biometric systems to prevent unauthorised access, and metal detectors to search people when they enter and leave the premises.

The power station security officers combat criminal activities by conducting regular patrols and attending the scenes of incidents in the premises and by strengthening security measures by controlling access. It was also established that security officers may collaborate with criminals to steal from the employer. In order to combat criminal activities, security officers need to enforce the law in combination with the site rules. It was also revealed that, although security officers play a role, they have challenges when faced with criminals who are armed.

The findings also indicate that the role of security manager in combating crime is to ensure that all equipment and personnel are protected on site at all times. It was also revealed that the security officers need to share crime related information with the police. Activities that are conducted in order to combat crime include conducting foot and vehicle patrols, tool verification at the access control point, encouraging the security officers to perform security functions diligently and ensuring that alarms are always functional. The participants said that they conducted searches of people and vehicles that enter and leave the premises. They are also responsible for locking the

doors, enhancing compliance with policies, procedures and directives, and educating visitors and employees on access control procedures.

The participants indicated that methods or strategies that they use to combat crime are to encourage healthy work relationships among security officers and also to encourage employees to report any suspicious activities. The participants indicated that they also monitor the movements of people and keep records of people and vehicles entering the site. The use of CCTV surveillance cameras was also established during the interviews with the participants. The findings also indicated that they conduct patrols, use metal detectors and personal identification cards at access control points. In order to combat crime effectively and efficiently, the responses indicated that they need security alarm systems, door locking systems, flashlight torches, two-way radio communication, pocket books, night vision cameras, firearms and bullet proof vests.

The findings revealed that the causes of security threats and vulnerabilities at the power station were: unauthorised employee absenteeism, employee negligence, a lack of sufficient security personnel, leakage and improper protection of information, a lack of budget for security measures, poor management and a lack of communication, a shortage of searches due to a lack of manpower, and theft committed by contract workers.

5.3 Conclusion

In this study, it was found that the ideal security measures to reduce threats and vulnerabilities are: the use of one gate for all personnel, deployment of more manpower to ensure effective patrols, patrolling of all areas three times a day and also during the night, effective communication and two-way radio communication, CCTV surveillance cameras, provision of sufficient manpower and the necessary resources, the use of law enforcement and external private security investigators, the need for the technology that has the capability to detect people far from the fence and identification marks for all the tools used on site.

The management of Critical Infrastructure should be responsible for the prevention of crime and ensure that security officers are thoroughly vetted before they are

employed. Vetting will ensure that people chosen have good credentials; they will be security officers who are committed to doing their duties and will perform security functions within the law. Tightening security measures needs to be supplemented by security policy and procedures. The management of the power station should ensure that contractors ensure that their employees are paid at the date and time that they have agreed upon as this will have positive effect on addressing the theft of working tools. Finally, the study found that the role of security supervisor or manager in the proposed security measures is to ensure effective communication, good relationships amongst security officers and ensure continuous motivation of security officers.

5.4 Recommendations

The recommendations of this study emanated from the research findings that Medupi Power Station, as a Critical Infrastructure, is vulnerable to security threats. The findings of this research revealed that there is a gap in the literature on security threats and vulnerabilities of Critical Infrastructures in South Africa. Based on this, the researcher proposes the following recommendations:

- **The prevention of copper cable theft, theft of computers and theft of working tools**

The findings revealed that the major criminal activity taking place at Medupi Power Station is copper cable theft, theft of computers and theft of working tools. Copper cable theft does not only affect the employer, but also the whole of society that expects uninterrupted services from the power station. It is recommended that the power station should ensure that sufficient budget is allocated to security functions. In addition, an intensive security risk survey be conducted in order to determine the type of security measures are required to address specific type of threats and vulnerabilities such as the theft of copper cables. This will help to address criminal activities due to the gap in security measures.

- **Top management and security managers to play a role in preventing threats and vulnerabilities**

The problem of theft and other forms of crime can be reduced if management has

buy-in into security functions. The head of the security department should have the relevant qualifications in security and ensure that education, training and awareness of crime on site are conducted.

- **Education, training, security awareness and security culture**

The security department should be responsible for creating a security culture. All employees, not only security officers, should be part of the overall security. Training on security related issues can be provided by a private security provider.

- **Conducting a comprehensive security survey**

A comprehensive security survey should be conducted by an independent security consultant.

- **Budget allocation for security measures**

It is recommended that the management should assign sufficient budget for security functions in order to achieve return on investment.

- **Provision of sufficient manpower**

The participants outlined manpower as a serious challenge to reduce threats and vulnerabilities. It is recommended that security survey should be conducted in order to determine the number of security officers required. It is suggested that the recommendations of the survey be implemented with caution and that budget should be allocated to address the recommendations in the survey report.

- **Provision of the necessary security measures**

The findings revealed that there are insufficient security measures and that some of them are there but are not being monitored, for example, CCTV cameras. It is recommended that a company be contracted to be responsible for the maintenance of the CCTV cameras.

- **Access control measures**

The responses indicated that access control measures are compromised due to a

lack of resources. It is recommended that budget should be set aside for the purchase of access control measures as per the recommendations of the security survey.

- **Identification marks for working tools**

It is recommended that each contract company be encouraged to mark their working tools. This will assist the security officers manning access control to know which tools belong to each company, and will also assist in knowing who took a specific tool so that the relevant people are held to account.

- **Perimeter fence**

It is recommended that the perimeter fence be high enough to deter criminals and that concrete is poured underneath it to prevent criminals from digging under the fence.

- **Use of more than one entrance and exit gate**

It is recommended that, due to a lack of manpower, only one gate be used for efficient access control to ensure that only authorised people gain access.

- **Employees' attitudes towards crime and security measures**

It is recommended that awareness and training be conducted to change the attitudes of employees so that they will understand the impact of crime on the power station.

- **Information security**

It is important to encourage users of computers about the impact of sharing their passwords to access information about the power station. Employees should be encouraged to report any misuse or unauthorised use of passwords.

- **Effective security policy and procedures**

It is recommended that security policy and procedures be aligned with the findings of the security survey and clearly state the security functions (Fay & Patterson, 2018). This will assist in ensuring that any security breach is contained in the policy and

those that breach be held accountable.

- **Enhance communication**

Poor communication between security management and security officials is a barrier to effective security. Therefore, it is recommended that the management enhance communication channels to ensure that employees are provided with the necessary information they require to do their jobs.

- **Information leakage**

To discourage the leakage of information, it is recommended that security officers are vetted and/or sign a confidentiality contract while awaiting the outcome of the vetting process.

- **Integrated approach in reducing threats and vulnerabilities**

It is recommended that, in order to reduce threats and vulnerabilities, there is a need for integrated approach which involves the security supervisor, security investigators, and police.

- **Crime Prevention through Environmental Design (CPTED)**

Crime Prevention through Environmental Design (CPTED) needs to be applied to protect entities such as Critical Infrastructure. CPTED can be used as a tool to discourage crime at Medupi. It is an environmental approach to prevent crime which focuses on reducing crime opportunities by manipulating the physical and social quality of an environment (Shariati, 2017:1). Lee, Park and Jung (2016:5) state that CPTED decreases the fear of crime by enhancing CPTED principles such as access control, natural surveillance, territoriality, activity support and maintenance.

5.5 Suggestions for future research

There is a need for future research to evaluate the effectiveness of security measures especially at National Key Points, such as Medupi, that are still under construction. Future research should also evaluate the impact of the contractors working within the NKP on crime. The relationship between contract security and in-

house security on the occurrence of crime on site needs to be part of a service level agreement. To stimulate further research, it is recommended that a thorough security survey analysis be conducted prior to the employment of contractors. A security survey will guide the management on security budget allocation in order to effectively and efficiently prevent crime in the NKP.

It is recommended that future research should focus on management's attitude to security measures since the findings established that security threats and vulnerabilities occur at Medupi as a result of poor management. Research could focus on addressing top management and management responsible for the role and function that security can play to ensure that sufficient budget is allocated to the security functions. Potential research should include case studies conducted on other Critical Infrastructure entities in South Africa to provide useful markers to assist managers of Critical Infrastructure to reduce security threats and vulnerabilities.

LIST OF REFERENCES

Abouzakhar, N. 2013. *Critical infrastructure cybersecurity: A review of recent threats and violations.* Paper presented at 12th European Conference on Cyber Warfare and Security, Finland, 11 July, pp. 1-10.

Akaranga, S.F. & Makau, B.K. 2016. Ethical considerations and their applications to research: A case of the University of Nairobi. *Journal of Educational Policy and Entrepreneurial Research,* 3(12), 1-19.

Alcaraz, C. & Zeadally, S. 2015. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection,* 8, 53-66. 10.1016/j.ijcip.2014.12.002

Amin, S.M. & Giacomoni, A.M. 2012. *Smart grid, safe, secure, self-heading: Challenges and opportunities in power system security, resiliency and privacy.* IEEE Power & Energy Magazine, 33-40.

Ani, U.D., Watson, J.D., Nurse, J.R., Cook, A. & Maple, C. 2019. *A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape*. Available at: http://arxiv.org/ftp/arxiv/papers/1904/1904.01551.pdf Accessed 26 April 2020.

Aradau, C. 2010. Security that matters: Critical Infrastructure and objects of protection. *Security Dialogue*, 41(5), 492-514.

Argun, U. & Daglar, M. 2016. Examination of routine activities theory by the property crime. *International Journal of Human Sciences*, 13(1), 1188-1198.

Ariel, B., Bland, M. & Sutherland, A. 2017. Lowering the threshold of effective deterrence – Testing the effect of private security agents in public space on crime: A randomized controlled trial in a mass transit system. *PLoS ONE*, 12(12), e0187392. https://doi.org/10.1371/journal.pone.0187392

Arifin, S.R. 2018. Ethical considerations in qualitative study. *International Journal of Care Scholars,* 1(2), 30-33.

Ashby, M.P.J. 2017. The value of CCTV surveillance cameras as an investigative

tool: An empirical analysis. *European Journal of Crime Policy Research*, 23, 441-459.

Benoit, J. 2014. Assessing security threats to Canada's energy infrastructure: The Enbridge Northern Gateway pipeline. Unpublished dissertation, Fraser University, Canada, British Columbia.

Bergerbest-Eilon, D. 2009. *Critical infrastructure protection (CIP)***.** *Fall*, 11-13.

Bhaskar, R. & Kapoor, B. 2013. *Computer and information security handbook.* 2nd edition. Burlington, MA: Morgan Kaufmann.

Blatch-Jones, A.J., Kirkpatrick, E. & Ashton-Key, M. 2018. The role of feasibility and pilot studies in randomized controlled trials: A cross-sectional study. *BMJ Open*, 8(9), e022233 DOI: 10.1136/bmjopen-2018-022233

Bless, C. & Higson-Smith, C. 2000. *Fundamental of social research methods: An African Perspective*. 3rdEdition. Landsdowne: Juta Education.

Boda, R. & Dullabh, R. 2019. South Africa: Critical Infrastructure Act. 26 December 2019. *ENSafrica*. https://www.ensafrica.com/news/detail/2139/critical-infrastructure-act-2019. Accessed on 17 June 2020.

Borham, S.R., Abas, H., Azizan, A. & Syariff, S.A. 2016. Physical security enhancement in higher institutions. *Open International Journal of Informatics*, 1(2016), 1-10.

Bowers, K.J., Johnson, S.D. & Pease, K. 2004. Prospective hot-spotting: The future of crime mapping. *Britain Journal of Criminology,* 44(5), 641-658.

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77-101.

Braun, V. & Clarke, V. 2012. *Thematic analysis.* In Cooper, H. (Ed.), *The handbook of research methods in psychology*. Washington, DC: American Psychological Association.

Brink, P.J. & Wood, M.J. 1998. *Advanced design in nursing research*. Thousand

Oaks, CA: Sage.

Bruijne, M. & Van Eaten, M. 2007. System that should have failed: Critical Infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*, 14(1), 18-29.

Brunner, E. & Cavelty, M.D. 2011. *Lessons from the US National Infrastructure Protection Plan (NIPP) for sector specific and cross-sector risk analysis in Switzerland*. Switzerland: Centre for Security Studies. [Factsheet].

Burns, T. & Roszkowska, E. 2016. Rational choice theory: Toward a psychological, social and material contextualization of human choice behavior. *Theoretical Economic Letters*, 6, 195-207.

Business Dictionary. 2018a. Threat. Available at: http://www.businessdictionary.com/definition/threat.html Accessed on: 18 July 2018.

Business Dictionary. 2018b. Vulnerability. Available at: http://www.businessdictionary.com/definition/vulnerability.html Accessed on: 18 July 2018.

Caldeira, F.M.S. 2013. Trust and reputation for critical infrastructure protection. PhD thesis, University of Coimbra, Coimbra.

Cavalcanti, S.M.C., Grawshaw, P.G. & Tortato, F.R. 2012. Use of electric fencing and associated measures as deterrent to Jaquar predation on cattle in the Pandanal of Brazil. In Somers, M.J. & Haywards, M. (Eds.), *Fencing for conservation: Restriction of evolutionary potential or a riposte to threatening process?* (pp. 295-309). New York: Springer.

Cebekhulu, N.P. 2016. Assessing security measures at hotels: A case study from Gauteng. Master's thesis, University of South Africa, Pretoria.

Christopoulos, C. 2013. The role of state and local jurisdictions in identifying and protecting critical infrastructure. Dissertation, Naval Postgraduate School, Monterey, CA.

City of Tshwane. 2016. *How can we use open data to reduce cable theft in Tshwane?* Pretoria: City of Tshwane.

Clarke, V. & Braun, V. 2013. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, 26(2), 120-123.

Cohen, L.E. & Felson, M. 1974. Sv 'Routine activity theory'. In Cullen, F.T. & Willcox, P. (Eds.), *Encyclopedia of criminological theory*. Thousand Oaks, CA: Sage.

Counter-Terrorism Committee Executive Directorate and United Nations Office of Counter-Terrorism (CTED & UNOCT). 2018. *The protection of critical infrastructure against terrorist attack: Compendium of good practices*. New York: United Nations Office of Counter-Terrorism.

Creswell, J.W. 2014. *Research design*: *Qualitative, quantitative, and mixed methods approaches*. 4th edition. Thousand Oaks, CA: Sage.

Creswell, J.W. 2013. *Qualitative inquiry & research design*: *Choosing among five approaches*. 3rd edition. Thousand Oaks, CA: Sage.

CTED & UNOCT, see Counter-Terrorism Committee Executive Directorate and United Nations Office of Counter-Terrorism.

Dantzker, M.L. & Hunter, R.D. 2012. *Research methods for criminology and criminal Justice*.3rd edition. Burlington, MA: Jones & Bartlett.

Davis, R. 2013. *What's the point of National Key Points?* Daily Maverick, https://www.dailymaverick.co.za/article/2013-05-24-whats-the-point-of-national-key-points/

De Klerk, N. (2014). Shoot-out during heist at Gauteng mall. *News24*. 23 May. Available at: http://www.news24.com/SouthAfrica/News/Shoot-out-during-heist-at-Gauteng-mall-20140523 (Accessed on: 22 June 2018).

De Vos, A.S., Strydom, H., Fouche, C.B. & Delport, C.S.L. 2011. *Research at grassroots for the social sciences and human service professions*. 4th edition. Pretoria: Van Schaik.

Delport, C.S.L. & Roestenburg, W.J.H. 2011. Quantitative data collection methods: Questionnaires, checklists, structured observation and structured interview schedules. In De Vos, A.S., Strydom, H. & Fouche, C.B. (Eds.), *Research at grass roots: For the social sciences and human service professions*. 4th edition. Pretoria: Van Schaik.

Dempsey, J.S. 2008. *Introduction to private security*. Belmont, CA: Thomas Wadsworth.

DiCicco-Bloom, B. & Crabtree, B.F. 2006. Making sense of qualitative research. *Medical Education*, 40, 314-321.

Dikko, M. 2016. Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic Insurance). *The Qualitative Report*, 21(3), 521-528.

Dongre, A. & Sankaran, R. 2016. Ethical issues in qualitative research: Challenges and options. *International Journal of Medical Science and Public Health*, 5(6), 1187-1194.

Donnelly, P.G. & Kimble, C.E. 1997. Community organizing, environment change and neighbourhood crime. *Crime & Delinquency*, 43(4), 493-511.

Doody, O. & Doody, C.M. 2015. Conducting a pilot study: Case study of a novice researcher. *British Journal of Nursing,* 24(21), 1074-1078.

Drago, A. 2015. Methods and techniques for enhancing physical security of critical infrastructures. Unpublished dissertation, University of Naples "Federico II", Naples, Italy.

Du Plessis, D.J. 2013. A critical reflection on urban spatial planning practices and outcomes in post-apartheid South Africa. *Urban Forum,* 25, 69-88. Available at: http://doi.org/10.1007/s12132-013-9201-5

Dzansi, D.Y., Rambe, P. & Mathe, L. 2014. Cable theft and vandalism by employees of South Africa's electricity companies: A theoretical explanation and research agenda. *Journal of Social Sciences*, 39(2), 179-190.

Eck, J.E. & Guerette, R.T. 2012. Place-based crime prevention: Theory, evidence, and policy. In Brandon, C., Welsh, D. & Farrington, P. (Eds.), *The Oxford handbook of crime prevention* (pp. 354-383). New York: Oxford University Press.

Edure, A.A. & Adio, E.O. 2018. Biometric technologies for secured identification and personal verification. *Biostat Biometric Open Access Journal*, 6(2), 1-4.

Enokela, J.A. & Tyowuah, M.N. 2014. An electronically controlled automatic security access gate. *Leonardo Journal of Sciences*, 25, 85-96.

Enterprise Solutions. 2009. Integration is the future. *Hi-Tech Security Solutions*, 15(8): 60-63. Available at: http://www.securitysa.com/article.aspx?pklarticleid=5742 Accessed on: 01July 2018.

Erich, R. & Norman, V. 2015. *State of the art report (1): Urban critical infrastructure systems*. Brussels: European Union.

ESKOM. 2015. *Kusile and Medupi coal-fired power stations under construction.* COP 17 Fact Sheet. ESKOM: Megawatt Park.

European Academy. 2011. National critical energy infrastructure protection in Europe Seminar. 29 to 30 September. Maritim Proarte Hotel, Berlin, Germany.

Fay, J.J. 2010. *Contemporary security management*. Oxford: Butterworth-Heinemann.

Fay, J. & Patterson, D. 2018. *Contemporary security management*. 4th edition. Oxford: Elsevier.

Federal Republic of Germany. 2009. *Report on elections to the federal government*. Germany: Office for Democratic Institutions and Human Rights.

Felson, M. & Clarke, R.V. 1998. *Opportunity makes the thief: Practical theory for crime prevention*. London: Home Office.

Fennelly, L.J. 2013. *Effective physical security*. Amsterdam: Elsevier.

Fin24. 2015. Eskom shuts down. *Fin24.* 25 March. Available at: https://www.fin24.com/Economy/Eskom-shuts-down-Medupi-over-strike-action-20150325 (Accessed on: 09 September 2018).

Fisher, R.J., Halibozek, E. & Green, G. 2008. *Introduction to security.* 8th edition. Boston: Butterworth-Heinemann.

Flick, T. & Morehouse. 2010. *Securing the smart grid: Next generation power grid security.* Amsterdam: Elsevier.

Flick, T. & Morehouse. 2011. *Threats and impacts in securing the smart grid.* Amsterdam: Elsevier.

Fowler, H.R. & Aaron, J.E. 2010. *Little, brown handbook: The 12th edition*. London: Pearson.

Fritzon, A., Ljungkvist, K., Boin, A. & Rhinard, M. 2007. Protecting Europe's critical infrastructures: Problems and prospects. *Journal of Contingencies and Crisis Management*, 15(1), 30-41.

Gaiser, l. 2018. European critical infrastructure protection: The need for a regional approach and a cyber-constant contact strategy. *National Security and the Future*, 1-2(19), 45-63.

Giannopoulos, G., Filippini, R. & Schimmer, M. 2012. *Risk assessment methodologies for critical infrastructure protection Part 1: A state of the art*. Luxembourg: Office of the European Union.

Gibson A. 2017. On the face of it: CCTV images recognition evidence and criminal prosecutions in New South Wales. DPhil Thesis, University of Technology, Sydney, Sydney.

Greggo, A. 2011. *Retail security and loss prevention solutions.* Boca Raton, CA: Auerbach Publications.

Gritzalis, D. & Theoharidou, M. & Stergiopoulos, G. 2019. *Critical infrastructure security and resilience: Theories, methods, tools and technologies.* New York: Springer International Publishing.

Guest, G., Namey, E.E. & Mitchell, M.L. 2013. *Collecting qualitative data: A field manual for applied research*. Thousand Oaks, CA: Sage.

Gul, S.K. 2009. An evaluation of the rational choice theory in criminology. *Journal Social & Applied Science*, 4(8), 36-44.

Hammerli, B. & Renda, A. 2010. *Protection critical infrastructure in the EU: CPS Task Force Report.* Brussels: Centre for European Policy Studies.

Hazzi, O.H. & Maldaon, I.S. 2015. A pilot study: Vital methodological issues. *Business: Theory and Practice,* 16(1), 52-62.

Heino, O., Takala, A., Jukarainen, P., Kalahti, J., Kekki, T. & Verho, P. 2019. Critical infrastructures: The operational environment in cases of severe disruption. *Sustainability*, 11(838), 1-18.

Hemme, K. 2015. Critical infrastructure protection: Maintenance is national security. *Journal of Strategic Security*, 8(3), 25-39.

Henage, R.T. & Henage, D. 2013. Physical security: The weak link in internal control design? *American International Journal of Contemporary Research*, 3(10), 83-86.

Hi-Tech Security Solutions. 2007. Securing national key points. Available at: http://www.securitysa.com/news.aspx?pklnewsid=25593 (Accessed on: 21 September 2018).

Holmgren, A. 2004. Vulnerability analysis of electrical power delivery networks. PhD Thesis, Royal Institute of Technology, Stockholm, Sweden.

Hsieh, M.L. & Wang, S.Y. 2018. Routine activities in virtual space: A Taiwanese case of an ATM hacking spree. *International Journal of Cyber Criminology*, 12(1), 333-352.

Ibrahim, A.M. 2012. Thematic analysis: A critical review of its process and evaluation. *West East Journal of Social Sciences*, 1(1), 39-47.

Ishmail, N., Kinchin, G. & Edwards, J.A. 2018. Pilot study, does it really matter?

Learning lessons from conducting a pilot study for a qualitative PhD thesis. *International Journal of Social Science Research,* 6(1), 1-17.

Izuakor, C.O. 2016. Critical infrastructure asset identification: A multi-criteria decision system and aviation case study. DPhil thesis, University of Colorado, Colorado Springs.

Jacobs, J. 1961. *The death and life of Great American Cities.* New York: Random House.

Johnsen, S.O. & Stene, T. 2016. *Use of CCTV in remote operations and remote support of oil and gas fields to improve safety and resilience.* Human factors in organisational design and management – XI, Nordic Ergonomics Society Annual Conference, 46, 305-309.

Johnson, S.D. & Bowers, K. 2010. Permeability and burglar risk: Are cul-de-sacs safer? *Journal of Quantitative Criminology,* 26(1), 89-111.

Jugder, N. 2016. The thematic analysis of interview data: An approach used to examine the influence of the market on curricular provision in Mongolian higher education institutions. PhD thesis, Leeds: University of Leeds.

Kallio, H., Pietila, Johnson, M. & Kangasniemi, M. 2016. Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72(12), 2954-2965.

Karabacak, B. & Ozkan, S. 2009. Critical infrastructure protection status and action items of Turkey. International Conference on eGovernment Sharing Experiences. Available at: https://fuse.franklin.edu/facstaff-pub/40

Kashiefa, A. 2014. iStore robbery was a nightmare. *iOL News*. 23 August. Available at: http://www.iol.co.za/news/crime-courts/istore-robbery-was-a-nightmare-1.1739875 (Accessed on: 22 June 2018).

Katina, P.F. & Hester, P.T. 2012. Systemic determination of infrastructure criticality. *International Journal of Critical Infrastructure*, 10(10), 1-13.

Kelly, H., Clare, J., Wuschke, K. & Garis, L. 2019. Opportunity and rationality as an

explanation for suspicious vehicle fires: Demonstrating the relevance of time, place and economic factors. *Crime Science,* 8(8), 1-11.

Kimiecik, R.C. 1995. *Loss prevention guide for retail businesses.* Hoboken, NJ: John Wiley & Sons, Inc.

Kjolle, G.H., Utne, I.B. & Gjerde, O. 2012. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering and System Safety*, 105, 80-89.

Kole, O.J. 2015. Partnership policing between the South African Police Service and the Private Security industry in reducing crime in South Africa. PhD Thesis, University of South Africa, Pretoria.

Kumar, R. 2011. *Research Methodology: A Step-by-Step Guide for Beginners*. 3rd edition. Thousand Oaks, CA: Sage.

Kumar, R. 2014. *Research Methodology: A Step-by-Step Guide for Beginners*. 4th edition. Thousand Oaks, CA: Sage.

Kumar, R. Kelly, H., Clare, J., Wuschke, K. & Garis, L. 2019. Opportunity and rationality as an explanation for suspicious vehicle fires: Demonstrating the relevance of time, place and economic factors. *Crime Science,* 8(8), 1-11.

Kurdi, H.A. 2014. Reviews of closed circuit television (CCTV) techniques for vehicle traffic management. *International Journal of Computer Science & Information Technology,* 6(2), 199-206.

Kusile and Medupi Power Stations. 2017. *Heavy lifting project, 2013-2018*. Isando, Kempton Park: Freyssinet.

Lani, J. 2009. Dissertation Statistics Help. Available at: https://www.statisticssolutions.com/wp-content/uploads/kalins-pdf/singles/dissertation-statistics-help.pdf

Liebenberg, A.S. 2018. Examining the significance of modus operandi information in copper theft investigation. MTech Dissertation, University of South Africa, Pretoria.

Lee, J., Park, S. & Jung, S. 2016. Effect of crime prevention through environmental design (CPTED) measures on active living and fear of crime. *Sustainability*, 8(872), 1-16.

Leedy, P.D. & Ormrod, J.E. 2010. *Planning and design*. 8th edition. Upper Saddle Rivier, NJ: Pearson Prentice Hall.

Leventakis, G., Nikitakos, N. & Sfetsos, A. 2017. Risk assessment for interconnected critical infrastructure: The case of ship-port interface. Proceedings of the 52nd ESReDA Seminar, May 30-31, Lithuanian Energy Institute & Vytautas Magnus University, Kaunas, Lithuania.

Lutchminarain, N. 2015. Safety as a priority at shopping centres in Gauteng: An assessment of existing security measures. MTech Dissertation, University of South Africa, Pretoria.

Mahambane, M.A. 2017. Safety and security of consumers at retail stores in the Gauteng Province: An assessment of security measures. MA Dissertation, Pretoria: University of South Africa. Available at: http://uir.unisa.ac.za/bitstream/handle/10500/24500/dissertation_mahambane_ma.pdf?sequence=1&isAllowed=y. Accessed on: 07 October 2018.

Mäkinen, J. 2016. Cyber threats against critical infrastructure – Is there a need for national programme? Degree Programme in Security Management at LAUREA University of Applied Sciences, Leppävaara, Finland.

Mbalula, F. 2017. Mbalula wants new police budget, better security at key points. Available at: https://www.polity.org.za/article/mbalula-wants-new-police-budget-better-security-at-key-points-2017-06-07. Accessed on: 28 July 2020.

Melchiorre, T. 2018. *Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security*. Vilnius: NATO Energy Security Centre of Excellence.

Melville, S. & Goddard, W. 2001. *Research Methodology: A practical guide*. Thousand Oaks, CA: Sage.

Minimum Information Security Standards. 1998. Available at: https://www.right2info.org/resources/publications/laws-1/SA_Minimum%20Information%20Security%20Standards.pdf Accessed on: 07 October 2018.

Mouton, J. 2001. *How to succeed in your master's and doctoral studies: A South African guide and resource book*. Pretoria: Van Schaik.

Moyo, S. 2019. Evaluating the use of CCTV surveillance systems for crime control and prevention: Selected case studies from Johannesburg and Tshwane, Gauteng. MTech dissertation, University of South Africa, Pretoria.

Musonza, D. 2016. *The implementation of integrated security systems: Case study of the industrial sector of Harare-Zimbabwe*. MTech dissertation, University of South Africa, Pretoria.

MyHR. 2014. Human resources for the B.C. Public Service. Available at: http://www2.gov.bc.ca/myhr/content_hub.page?ContentID=ea3328ba-7d38-5d2c-2818-f4fd2a64db33 Accessed on: 20 June 2018.

Narayan, R. 2013. Session five: Reducing copper theft in telecommunications and electrical industry. Available at: http://www.iceweb.com.au/ElectricalWeb/Earthing/Reducing%20Copper%20Theft%20.pdf

Nkwana, M.J. 2015. Protection of security information within government departments in South Africa. MTech Dissertation, University of South Africa, Pretoria. Available at: http://uir.unisa.ac.za/bitstream/handle/10500/19897/dissertation_nkwana_mj.pdf?sequence=1&isAllowed=y (Accessed on: 20 September 2018).

Nowell, L.S., Morris, J.M., White, D.E. & Moules, N.J. 2017. Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16, 1-13.

Oforis, G., Hindle, R. & Hugo, F. 1996. Improving the construction industry of South Africa: A strategy. *Habitat International*, 20(2), 203-220.

Parahoo, K. 2006. *Nursing research: Principles, process and issues*. 2nd edition. New York: Palgrave Macmillan.

Pathak, A. & Intratat, C. 2012. Use of semi-structured interviews to investigate teacher perceptions of student collaboration. *Malaysian Journal of ELT Research*, 8(1), 1-10.

Peters, D. 2011. Make cable theft a serious crime. Media Briefing by the Minister of Engergy, 9th August 2011. Available at: https://www.polity.org.za/article/make-cable-theft-a-serious-crime-peters-2011-08-19 (Accessed on: 26 May 2020).

Pothier, M. 2013. The National Key Point Act. Briefing Paper, Cape Town: Parliamentary Liaison Office.

Poustourli, A., Ward, D., Zachariadis, A. & Schimmer, M. 2015. An overview of European Union and United States critical infrastructure protection policies. Proceedings of the 12th International Conference "Standardization, Prototypes and Quality: A means of Balkan Countries' Collaboration", Kocaeli University Foundation, Turkey, 549-557.

Pretorius, W.L. 2012. A criminological analysis of copper cable theft in Gauteng. MA dissertation, University of South Africa, Pretoria.

Private Security Industry Regulatory Authority Act No. 56 of 2001. Available at: https://www.saps.gov.za/resource_centre/acts/downloads/juta/a56of2001.pdf (Accessed on: 19 July 2018).

Purpura, P. 2011. *Security: An introduction.* Boca Raton, FL: CRC Press.

Purpura, P. 2013. *Security and loss prevention: An introduction*. 6th edition. Oxford, UK: Butterworth-Heinemann.

Queiros, A., Faria, D. & Almeida, F. 2017. Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies,* 3(9), 369-387.

Rakoma, R. 2018. Personal communication. 15 April.

Rantao, J. & Bailey, C. 2011. Bheki Cele's recipe for the fight against crime. *The Star.* 15th September. Available at: http://www.iol.co.za/the-star/bheki-cele-s-recipe-for-the-fight-against-crime-1.1137942 (Accessed on: 01 June 2018).

Rehak, D., Hromada, M. & Novotny, P. 2016. European critical infrastructure risk and safety management: Directive implementation in practice. *Chemical Engineering Transactions*, 48, 943-948.

Rehak, D., Markuci, J., Hromada, M. & Barcova, K. 2016. Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. *International Journal of Critical Infrastructure Protection,* 14, 3-17.

Rehak, D., Senovsky, P. & Slivkova, S. 2018. Resilience of critical infrastructure elements and its main factors. *Systems*, 6(21), 1-13.

Reynald, D.M. 2014. Environmental design and crime events. *Journal of Contemporary Criminal Justice*, 31(1), 71-89.

Right2know. 2015. A*nalysis: The National Key Points list has been released. Now What?* Salt River, Cape Town: Right2know. Available at: https://www.r2k.org.za/2015/02/03/analysis-national-key-points-way-forward/ (Accessed on: 23 June 2020).

Robles, R.J., Choi, M.K., Cho, E.S., Kim, S.S, Park, G.C. & Lee, J.H. 2008. Common threats and vulnerabilities of critical infrastructures. *International Journal of Control and Automation*, 1(1), 17-22.

Rouse, M. 2014. Physical security. Available at: http://searchsecurity.techtarget.com/definition/physical-security (Accessed: 17June 2018).

SA, see South Africa.

Sabhanayagam, T., Ventatesan, P. & Senthamaraikannan, K. 2018. A comprehensive survey on various biometric systems. *International Journal of Applied Engineering Research*, 13(5), 2276-2297.

Sadeghi, A., Jabbari, M., Alidoosti, A. & Rezaenian, M. 2017. Vulnerability and

security risk assessment of a thermal power plant using SVA technique. *Journal of Integrated Security Sciences*, 1(1), 16-28.

Sango, I. 2013. An investigation of communal farmers' livelihood and climate change challenges and opportunities in Makonde rural district of Zimbabwe. PhDThesis, University of South Africa, Pretoria.

Sanjari, M., Bahramnezhad, F., Fomani, F.K., Shoghi, M. & Cheraghi, M.A. 2014. Ethical challenges of researchers in qualitative studies: The necessity to develop a specific guideline. *Journal of Medical Ethics and History of Medicine*, 7(14), 1-6.

Sapori, E., Sciutto, M., Sciutto, G. 2014. A quantitative approach to risk management in critical infrastructures. *Transport Research Procedia*, 3, 740-749.

Sastry, T.S.N. 2013. The significance of research methodology in human rights: A bird's eye view. *Delhi Law Review,* 32, 105-114.

Savard, D.M. 2018. A routine activity approach: Assessing victimization by gender in transit environmental and other public locations. *Advances in Applied Sociology*, 8, 56-75. Available at: https://doi.org/10.4236/aasoci.2018.81004. (Accessed: 16 June 2020).

Schneidhofer, B. & Wolthusen, S. 2015. *A case study in critical infrastructure interdependency*. London: Royal Holloway.

Schneidhofer, B., Wolthusen, S. 2016. Multigraph critical infrastructure model. In: Rice M. & Shenoi, S. (Eds.), *Critical infrastructure protection XI*. 11th IFIP WG 11.10 International Conference, ICCIP 2017, Arlington, VA, USA, March 13-15, 2017, Revised Selected Papers (Accessed: 18 April 2020).

Shared Narrative. 2014. *Critical 5: Forging a common understanding for critical infrastructure.* Dartmouth, Canada: Public Safety Canada.

Shariati, A. 2017. An assessment of the role of crime prevention through environmental design (CPTED) in campus safety. DPhil Thesis, Florida International University, Miami, FL.

Shuping, P. 2018. *Copper cable theft syndicate sentenced to lengthy jail terms*. Free State: NPA Media Statement, 31 January 2018.

Sienko, P. 2015. Methods of securing and controlling critical infrastructure assets allocated in information and communications technology sector companies leading European Union countries. *Securitologia*, 22(2), 107-123.

Simon, M.K. & Goes, J. 2013. *Dissertation and scholarly research: Recipes for success*. Seattle, WA: Dissertation Success LLC.

Singh, T., Chetty, N. & Karodia, A.M. 2016. An investigation into the impact of absenteeism on the organizational performance of a private security company in Durban, KwaZulu-Natal. *Singaporean Journal of Business Economics and Management Studies*, 4(11), 105-159.

South Africa [SA]. 1980. National Key Points Act 102 of 1980. Pretoria: Government Printer.

South Africa [SA]. 1998. *Minimum information security standards*. 2nd edition. March 1998. Available at: http://www.right2info.org/resources/publications/laws-1/SAMinimum%20information%20Security%standards.pdf (Accessed on 13 December, 2016).

South Africa [SA]. 2001. Private Security Industry Regulation Act 56 of 2001. Pretoria: Government Printer.

South Africa [SA]. 2007a. Strategic Installations Bill [Notice 432 of 2007]. Pretoria: Government Printer.

South Africa [SA]. 2007b. The National Key Points Act 102 of 1980: Government Gazette, 31 July 2007. Pretoria: *Government Printer*. Available at: https://www.saps.gov.za/resource_centre/acts/downloads/juta/a102of1980.pdf Accessed on: 18 July 2018.

South Africa [SA]. 2015. Protection of Critical Infrastructure Bill, 2015. Pretoria: Government Printer.

South Africa [SA]. 2018. Annual report for Department of Energy, 2018/19. Pretoria:

Department of Energy.

South Africa [SA]. 2019a. Roadmap for ESKOM in a reformed electricity supply industry 2019. Pretoria: Department of Public Enterprise.

South Africa [SA]. 2019b. Annual report for 2018/2019. Pretoria: Department of Public Enterprise.

South Africa [SA]. 2019c. Critical Infrastructure Protection Act 8 of 2019. Pretoria: Government Printer.

Sovacool, B. & Rafey, W. 2011. Snakes in the grass: The energy security implications of Medupi. *The Electrical Journal*, 24(1), 92-100.

Spellman, F., & Bieber, R.M. 2010. *Energy infrastructure protection and Homeland security.* New York: Rowman & Littlefield.

Steele, W., Hussey, K. & Dovers, S. 2017. What's Critical about Critical Infrastructure? *Urban Policy and Research*, 35(1), 74-86. DOI: 10.1080/08111146.2017.1282857

Tabansky, L. 2011. Critical infrastructure protection against cyber threats. *Military and Strategic Affairs*, 3(2), 61-78.

Torkar, G., Zimmermann, B. & Wilbrand, T. 2011. Qualitative interviews in human dimensions studies about nature conservation. *Varstvo Narave*, 25, 39-52.

Tweneboah-Koduah, S. & Buchanan, W. 2018. Security risk assessment of critical infrastructure systems: A comparative study. *The Computer Journal*, 61(9), 1-18.

UNISA, see University of South Africa.

United Nations Security Council. 2018. *The protection of critical infrastructures against terrorist attacks: Compendium of good practice*. New York: United Nations Office of Counter-Terrorism.

University of South Africa [UNISA]. 2016. *Policy on research ethics.* Pretoria: UNISA.

Van Der Watt, M., Van Graan, J. & Labuschagne, G. 2014. Modus operandi, signature and fantasy as distinctive behavior: Fundamental considerations in the case linkage of child rape cases. *Child Abuse Research: A South African Journal*, 15(1), 61-72.

Van Jaarsveld, L. 2011. An Investigation of safety and security measures at secondary schools in Tshwane, South Africa. MTech Thesis, University of South Africa, Pretoria.

Van Niekerk, A.M. 2015. The analysis of a cell phone record as a source of intelligence in the investigation of copper cable theft. MTech dissertation, University of South Africa, Pretoria.

Van Niekerk, B. 2011. Vulnerability assessment of modern ICT infrastructure from an information warfare perspective. PhD dissertation, University of KwaZulu-Natal, Durban.

Van Niekerk, B. & Manoj, M.S. 2011. Relevance of information warfare modes to critical infrastructure protection. *South African Journal of Military Studies*, 39(2), 52-75.

Visser, B.L. 2015. *The significance of physical surveillance as a method in the investigation of insurance fraud: A Discovery Life Perspective.* MTech Dissertation, University of South Africa, Pretoria.

Zaballos, A.G. & Jeun, I. 2016. *Best practices for critical information infrastructure protection (CIIP): Experiences from Latin America and the Caribbean and selected countries*. Washington, DC: Inter-American Development Bank.

Zaballos, A.G. & Jeun, I. 2016. *Best practices for critical information infrastructure protection (CIIP): Experiences from Latin America and the Caribbean and selected countries*. Washington, DC: Inter-American Development Bank.

ANNEXURE A: INTERVIEW SCHEDULE

SCHOOL OF CRIMINAL JUSTICE

DEPARTMENT OF CRIMINOLOGY AND SECURITY SCIENCE

INTERVIEW SCHEDULE

TOPIC: AN EVALUATION OF SECURITY THREATS AND VULNERABILITIES AT A NATIONAL KEY POINT (CASE STUDY OF MEDUPI POWER STATION).

Dear Mr/Ms ……..

My name is Elias Motha Thoka, I am an MTech student at University of South Africa (UNISA) and I am conducting a study on "**An Evaluation of security threats and vulnerabilities at the Medupi Power Station".** For this reason, I would like to ask you some questions relating to the topic. Participation in this study is voluntary and the information you provide is private, confidential and anonymity.

The information will only be used for the purpose of the study and none of the information will be shared with a third party. This research is not funded by any organization. You may withdraw from the interview at any time of the interview without any consequences. This interview will take +-45 minutes. A tape recorder will be used to assist the researcher in transcribing the interview at a later stage. If you have any questions about the research, please feel free to contact Elias Motha Thoka@ 078 709 3603, and ThokaME@eskom.co.za.

1. **SECTION A** (Demographic details)

The following questions are for statistical purposes only.

1.1 Gender:

Male	1	

Female	2	

1. Age:

18-22 years	1	
23-27 years	2	
28-32 years	3	
33-37 years	4	
37-42 years	5	
48-52 year	6	
53+	7	

1.2 Marital status:

Single	1	
Married	2	
Unknown	3	
Divorced	4	
Widowed	5	

1.3 Educational qualification:

Degree	1	
Advanced diploma	2	
Diploma(3 years)	3	
Certificate	4	
Standard 10/Grade 12	5	
Other	6	

SECTION B

QUESTIONS	PROBES
1. What types of crimes occurs at Medupi power station?	*What, Who, When, Why, Where and How?*
✓ How would you describe criminal activities that are taking place? ✓ How would you describe modus operandi of crime? ✓ Describe how you manage to reduce crimes on-site?	
2. What type of security threats and vulnerabilities at Medupi?	*What, Who, When, Why, Where and How?*
✓ How would you describe how to identify threats on-site? ✓ How would you describe how to reduce threats and vulnerabilities around Medupi? ✓ How would you describe your security measures around Medupi?	
3. How can power station security officers combat criminal activities at Medupi?	*What, Who, When, Why, Where and How?*
✓ How would you describe your experiences of combating crime? ✓ What is your role in combating crime? ✓ Are there any methods or strategies that you are using to combat crime? ✓ What resources are you using to combat crime? ✓ What are the challenges experienced when combating crime? ✓ What are the best practices of combating crime?	
4. What are the causes of the security threats and vulnerabilities to power station?	*What, Who, When, Why, Where and How?*
✓ How would you describe the causes of security threats and vulnerabilities to power station? ✓ What is your understanding of those causes?	
5. What type of security measures is needed to reduce security threats and vulnerabilities?	*What, Who, When, Why, Where and How?*
✓ In your opinion, describe an ideal of security measures that you see fit in this station? ✓ How would you describe your role in your proposed security measures mentioned above?	
6. In closing, do you have anything further comments or questions?	

Thank you for agreeing to participate in this study. Your input will be very valuable to my study Medupi to improve the role of security measures at Medupi Power Station. It will assist me to make recommendations to management to improve security measures around Medupi.

ANNEXURE B: EDITING CERTIFICATE

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 EVALUATION OF SECURITY THREATS AND VULNERABILITIES TO A NATIONAL KEY POINT: CASE STUDY OF MEDUPI POWER STATION

By ELIAS MOTHA THOKA

Barbara Shaw

25/03/2021

ANNEXURE C: LETTER OF PERMISSION TO CONDUCT RESEARCH

Eskom

Mr. Elias Thoka
Security Supervisor
Medupi Power Station
LEPHALALE

Date:
22 March 2019

Enquiries:
Lesley Baloyi
Tel 27 14 762 6193
Fax +27 86 665 9516

Dear Mr. Thoka

APPROVAL TO CONDUCT RESEARCH STUDY AT MEDUPI POWER STATION (NKP)

Permission is hereby granted to Mr. Elias Thoka to conduct research study at Medupi Power Station. Medupi Power Station has been declared a National Key Point and thus the following conditions will apply:-

Conditions:-

1. The information gathered will be used for the study purposes only.
2. Information will only be used for what it was intended for.
3. The report compiled will be approved by the Risk Management Manager before external submission.
4. Information divulged should not put Eskom in disrepute or cause any form of security breach.

The above conditions must be strictly adhered to. Disobeying National Key Point rules bears serious consequences.

Yours sincerely

Lesley Baloyi
RISK MANAGEMENT GROUP MANAGER
MEDUPI POWER STATION

Generation Division – Coal New Build Unit
Management Department (Medupi Power Station)
Steenbokpan Road, Onverwacht
Private Bag X9003, Lephalale 0555 SA
Tel+27 14 762 2154 www.eskom.co.za
Eskom Holdings SOC Ltd Reg No 2002/015527/30

ANNEXURE D: UNISA ETHICAL CLEARANCE LETTER

UNISA university of south africa

UNISA CLAW ETHICS REVIEW COMMITTEE

Date 20181109

Reference: ST100 of 2018
Applicant: EM Thoka

Dear Mr Thoka

Decision: ETHICS APPROVAL
FROM 9 NOVEMBER 2018
TO 8 NOVEMBER 2021

Researcher(s): Elias Motha Thoka

Supervisor(s): Prof K Pillay
Prof AdV Minnaar

An evaluation of security threats and vulnerabilities to a national key point: Case study of Medupi power station

Qualification: MTech (Security Management)

Thank you for the application for research ethics clearance by the Unisa CLAW 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 9 November 2018 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision was ratified by the committee.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.
3. The researcher will conduct the study according to the methods and procedures set out in the approved application.

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

4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. No field work activities may continue after the expiry date of 8 November 2021. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:
The reference number ST100 of 2018 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

PROF N MOLLEMA

Chair of CLAW ERC

E-mail: mollen@unisa.ac.za

Tel: (012) 429-8384

PROF CI TSHOOSE

Executive Dean: CLAW

E-mail: tshooci@unisa.ac.za

Tel: (012) 429-2005

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: RESEARCH PERMISSION LETTER

Mr Martin Strauss (Acting Executive Security Division)
Eskom

Dear Mr Strauss

RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH FOR AN MTECH DISSERTATION

Mr **Elias Motha Thoka,** (UNISA Student Number:**33789169**), is currently a Masters student at the University of South Africa (UNISA), busy with his research studies for a Masters' degree (MTech in Security Management).

The title of his research topic is: An evaluation of security threats and vulnerabilities to a National Key Point (case study of Medupi Power Station).

Elias Motha Thoka has obtained ethical clearance from the UNISA College of Law Research Ethics Review Committee (#ref: ST100 of 2018) to proceed with his fieldwork research (see attached letter dated from 09 November 2018 to 08 November 2021 as per decision of ethical committee.

Accordingly we would like to request permission for him to undertake fieldwork research and conduct interviews with Security Staff and Contracted Security Company renders services on-site.

DESCRIPTION OF THE RESEARCH PROJECT

The research project will examine the evaluation of the current effectiveness of the existing security measures at the Medupi power station.

The primary aim of the research is to evaluate the effectiveness of the legislation regulating national key point.

A further objective of this research being that research results and recommendations will be submitted to station management and board of directors for perusal and possible approval of the findings and the study will be used to make recommendations

The public, referred to in the questionnaires shall mean to add value in the security outlook of the power station.

The questionnaires have three sections, namely:

i) demographic information;
ii) Interviews
iii) Site observation

All the information that is received from the participants/respondents will be treated with the utmost confidentially (i.e. respondents will remain anonymous and no reference will be made to their identity or to the organisation for which they work). Neither organisation nor names of individual respondents/participants will be used in the resulting research report (i.e. identities will remain unknown and protected).

Participation in the research interviews/survey questionnaire will also be on a voluntary basis.

The final dissertation (research report) once accepted will be placed in the UNISA library and therefore in the public domain and can be accessed by interested parties.

Attached for your information, is a detailed research proposal and a draft set of interview questions and a survey questionnaire.

If any confirmation or other information is needed, Mr Elias Motha Thoka can be directly contacted at the following:

Tel: 014 762 6454
Cell: 078 709 3603
Email:ThokaME@eskom.co.za

Alternatively, Prof K Pillay, Mr Thoka's study supervisor, can also be directly contacted (see below for contact details).

Once permission is granted to [insert your name] to commence his field research at your workplace please inform him accordingly. EM Thoka will then be in touch directly with you or a representative for the scheduling of any interviews or administering of the research questionnaire with relevant staff.

Regards

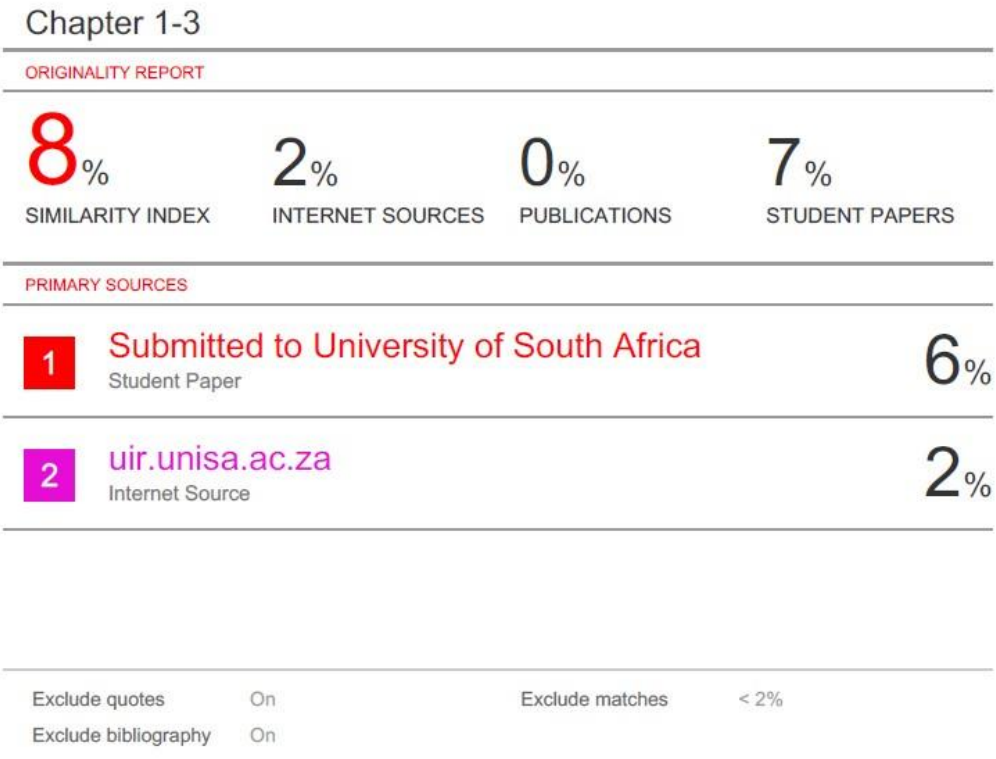
_____ (Prof)
K Pillay
Supervisor
Department of Criminology & Security Science
School of Criminal Justice, College of Law, University of South Africa
Email: cpillay@unisa.ac.za Cell: 082 883 7334 Tel: 012 433 9419

_____ (Mr)
Elias Motha Thoka
MTech Student (Student number: 33789169)
Work details: Medupi Power Station
Tel: 014 762 6454
Cell: 078 709 3603
Email:ThokaME@eskom.co.za

Date: 20 November 2018

ANNEXURE F: TURNITIN REPORT

Chapter 1



Chapter 1-3

ORIGINALITY REPORT

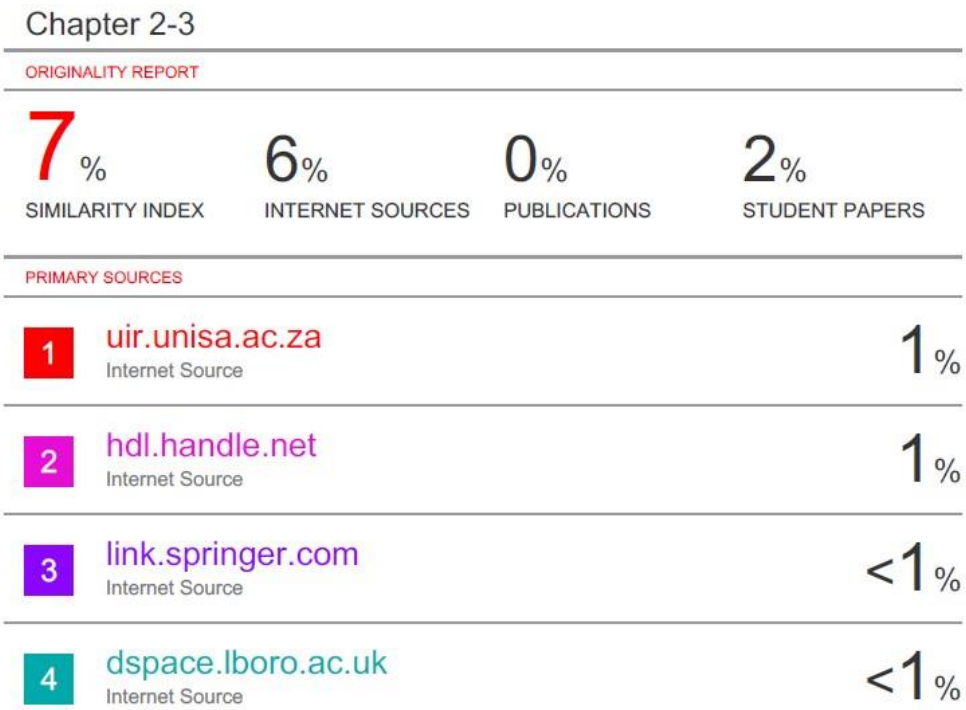
8%	2%	0%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of South Africa Student Paper	6%
2	uir.unisa.ac.za Internet Source	2%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		

Chapter 2



Chapter 2-3

ORIGINALITY REPORT

7%	6%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	uir.unisa.ac.za Internet Source	1%
2	hdl.handle.net Internet Source	1%
3	link.springer.com Internet Source	<1%
4	dspace.lboro.ac.uk Internet Source	<1%

Chapter 3

Chapter 3-2

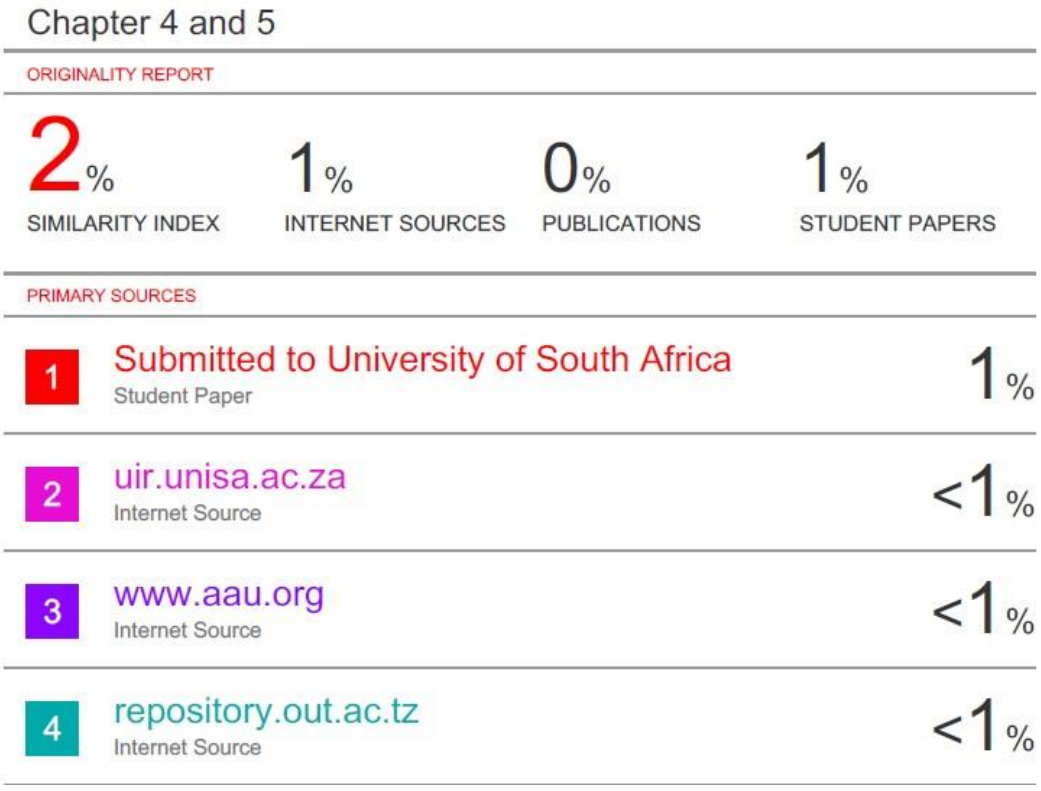
ORIGINALITY REPORT

9%	7%	4%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.homeoffice.gov.uk Internet Source	2%
2	www.annualreviews.org Internet Source	1%
3	Åsa Fritzon, Kristin Ljungkvist, Arjen Boin, Mark Rhinard. "Protecting Europe's Critical Infrastructures: Problems and Prospects", Journal of Contingencies and Crisis Management, 2007	1%

Chapter 4 & 5



Chapter 4 and 5

ORIGINALITY REPORT

2%	1%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of South Africa Student Paper	1%
2	uir.unisa.ac.za Internet Source	<1%
3	www.aau.org Internet Source	<1%
4	repository.out.ac.tz Internet Source	<1%