BARRIERS TO IMPLEMENTATION OF THE (SA) NATIONAL CYBERSECURITY POLICY FRAMEWORK

Submission Date: 2016/07/21

Name: Sizwe

Surname: GWALA

Student Number: 955971

Dedications

I would like to dedicate this report to the Almighty God whom I couldn’t have completed this report without his guidance, I also want to send a special dedication to my beautiful and intellectual wife, to my handsome son who will grow up to be an incredible and highly influential leader in the future as well as to my entire family.

Acknowledgements

I would like to take this opportunity to send a special vote of thanks to Professor Anthoni Van Nieuwkerk who has provided me with great assistance in aligning the scope, focus and direction of this entire report.

DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements of the degree of Masters of Management (in the field of Security) in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other University.

_____

Sizwe GWALA

21 July 2016

TABLE OF CONTENTS **PAGE**

ABSTRACT

Technological advancement have seen South African government departments, state owned entities and private companies using cyberspace as a platform of interaction and the storage of information. Technological advancements have a positive impact due to the compression of space, time and thereby ensuring fast-paced interaction across borders. These technological advancements have, however resulted in most organisations, both private and public, becoming prone to cybercrimes and related incidents. In an initiative aimed at countering these threats, the South African government has passed various laws. The National Cybersecurity Policy Framework (NCPF) is a South African Policy framework aimed at countering an increase in the occurrence of cybercrimes and related incidents.

This research analyses the status in the implementation of the NCPF objectives allocated to the Department of Telecommunications and Postal Services (DTPS). Then the barriers in the Implementation are unpacked guided by the literature reviewed and finally recommendations on how to counter the identified barriers are provided post the data collection. The report firstly provides an outline of the global perspectives on cybersecurity which is followed by the regional cybersecurity measures, and then the national cybersecurity measures proposed by the South African Government department are outlined. The latter parts of the report focuses on the NCPF in terms of its scope, goals, objectives and stakeholders. Finally, focus is shifted to the DTPS as a chosen area of research wherein data was collected in a form of one-on-one, semi-structured interviews with relevant parties.

The results of this research are presented as a narrative description that is synthesised to develop the theoretical conjecture and empirical generalisation of the entire research. This research uncovered that there are numerous barriers in the implementation of the NCPF both within the DTPS as well as between the DTPS and various stakeholders entrusted with the implementation responsibility. The last chapter consists of general conclusions made by the researcher based on the research conducted which is then followed by recommended countermeasures which will be communicated to the DTPS as well as all stakeholders who will be affected by the proposed recommendations.

ACRONYMS AND ABBREVIATIONS

AU	African Union
ATM	Automated Teller Machine
CECC	European Convention on Cybercrimes
CERT	Computer Emergency response team
CRC	Cybersecurity Response Committee
CSC	Cybersecurity Centre
CSIR	Council for Scientific and Industrial Research
CSIRT	Computer Security Incident Response Team
DIRCO	Department of International Relations and Cooperation
DoD&MV	Department of Defence and Military Veterans
DoST	Department of Science and Technology
DoJ&CD	Department of Justice and constitutional development
DTPS	Department of Telecommunications and Postal Services
ECS	Electronic Communication Security
GCIS	Government Communication Information Services
ICT	Information and Communication Technology
IT	Technology
JCPS	Justice, Crime Prevention and Security Cluster
NCPF	National Cybersecurity Policy Framework
NT	National Treasury
SA	South Africa
SAPS	South African Police Services
SETA	Sector Education and Training Authorities
SITA	State Information Technology Agency
SOE's	State Owned Entities
SSA	State Security Agency
US	United States
USA	United States of America
WiFi	Wireless Fidelity

DEFINITION OF KEY CONCEPTS

Cyberspace: Nervous system, the control system of the country composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work (*Kuehl, nd*).

Cybercrime: Any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the internet or any one or more of them (Electronic Communication and Transaction Act, 2012)

Cybersecurity: The body of techniques, processes and practices designed to protect networks, computers, programs and data from attack, damage or authorised access (whatis.com, 2015).

Cyberpower: The ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power (Kuehl, nd).

CSIRT: A team of dedicated information security specialists that prepares for and responds to information security incidents. When an incident occurs, members of a CSIRT can assist its constituency in determining what happened and what actions need to be taken to remedy the situation (Grobler and Bryk, 2010).

Digital forensics: This is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing structured investigations (Technopedi, 2016).

Cloud computing: New and emerging invention that changes the way Information Technology (IT) architects solutions are put forward in terms of moving towards virtualisation of data storage, of local networks and softwares (Ramgovind, Eloff and Smith, 2010).

E-government: Governments use of technology, particularly web-based internet applications, to enhance the access to and delivery of government information and service to citizens, business partners, employees, other government departments , and government entities (Ngulube, 2007)

Information literacy: The persons' ability to recognise when information is needed and have the ability to locate, evaluate and use effectively the information needed (Ngulube, 2007).

New crimes: Crimes that can be committed solely with the aid or use of a computer (Herselman and Warren, 2012).

Information literacy: The persons' ability to recognise when information is needed and have the ability to locate, evaluate and use effectively the information needed (Ngulube, 2007).

Trojans: Malware masquandering as something the user may want to download or install, that may perform hidden or unexpected actions; spy ware transmits information gathered from a computer, such as bank details to an attacker (Osuagwu, Ogiemien and Okide, 2010).

WiFi: A local area network that uses high frequency radio signals to transmit and receive data over distance of a few hundred feet; uses ethernet protocol (whatis.com, 2015).

LIST OF ACTS AND REGULATIONS

- African Chatter on the Values and Principles of Public Service and Administration of 2011
- African Union Convention of Cybersecurity and Personal Data Protection of 2014.
- Electronic Communications and Transactions Act of 2002.
- European Convention on Cybercrimes of 2001
- Interception and Monitoring Prohibition Act no 27 of 1992
- Prevention of Organised Crimes Act no 121 of 1998

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Cybersecurity is defined as "…the body of techniques, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access" (whatis.com, 2015). These are all measures put in place to safeguard cyberspace users from cybercrimes and related incidents. The digitalisation of South African government departments has seen the gist of the interactions and information being stored in a virtual space. This has therefore resulted in cyberspace being vulnerable to cybercrime and related incidents.

Cybercrimes can be regarded as new forms of crime which adversely affects all societies throughout the world. Herselman, *et al* (2010) postulate that cybercrime can be any kind of crime, ranging from hacking to more serious damage to intellectual property. The results of such crimes often leads to organisations both in the private and public sector losing money, mainly through the usage of computers and similar devices which are connected to the internet.

There has recently been a drastic increase in cybercrimes and related incidents in South Africa (SA), a phenomenon which can be attributes to an increase in broadband access which has thus increased the number of internet users. The increase in internet accessibility has therefore resulted to vulnerabilities to cybercrimes as often times internet user do not adequately protect sensitive information thereby making them targets for cybercriminals. Cassim (2015) states that the lack of IT knowledge by the public and the absence of suitable legal frameworks to deal with cybercrime at national and regional levels has led to an increase in cybercrimes and related incidents.

The speed with which the exposure to cyberspace is increasing has left government departments and State Owned Entities (SOE's) vulnerable to cybercrime and with insufficient countermeasures to keep up with the fast-paced cyber threats. Cassim (2015) furthermore asserts that the face of cybercrime has changed recently as a result of new internet environment, organised cybercrime groups and the development of new viruses. This change is as a result of the development of new accessible technologies and therefore the expansion of the internet has led to the developments of new forms of criminal behaviour. This has led to an increase in the

vulnerability of the African cyberspace and more specifically SA and as such “Most African states are lagging behind in strengthening cybersecurity and fighting cybercrime, cybercriminals have recognised this vulnerability and are targeting the continent” (Tamarkini, 2015, p.1).

The fast paced rolling out of broadband accessibility in SA has led to most private and public organisations migrating to cyberspace as a medium of interaction and information storage. This advancement brings with it a number of vulnerabilities. Van Nieuwkerk (2015) furthermore states that the sophistication of and diversity of cyber-attacks are increasing and without proper cybersecurity measures the economic, political and social results of cybercrimes and cyber espionage can be devastating. The diversity of and fast speed with which new forms of cybercrimes are developing has therefore led to the South African government departments and SOE’s being vulnerable to cybercrimes as their cybersecurity measures cannot keep up with the ever-changing cyber threats .

As an initiative aimed at reducing and curbing the increasing cybercrimes and related incident, the South African cabinet approved the National Cybersecurity Policy Framework (NCPF) in March 2012. The NCPF is a government policy document which recognises that the state is charged with implementing a government led, coherent and integrated cybersecurity approach (National Cyber Security Policy Framework, 2012). The mandate to implement the NCPF was initially given to the State Security Agency (SSA), then it was handed over to the Department of Communication (DoC) whose name was changed to the Department of Telecommunications and Postal Services. The mandate was later in 2012 handed back to the SSA.

This research was conducted with the main intension of uncovering whether or not the NCPF objectives allocated to the DTPS have been effectively implemented as projected when approved in 2012. Secondly, to uncover the barriers affecting the DTPS in the implementation thereof and to thus make recommendations which will be communicated to the DTPS and all relevant stakeholders who will be affected by the proposed recommendations. The researcher selected the DTPS as a research setting and therefore the research was conducted in terms of assessing the status of implementation as well as the barriers of implementation of the three NCPF

objectives allocated to the NCPF namely; the establishment of a Cybersecurity Hub, the rolling out of a Cybersecurity Awareness Programme as well as to assist in the development of Sector Computer Security Incident Response Teams (CSIRT)s.

The researcher conducted semi-structured one-on-one interviews with officials employed at the DTPS as well as those officials stationed at the Cybersecurity Hub. Based on the research conducted, it emerged that there are barriers in the implementation of the NCPF objectives. Due to the borderless nature of cyberspace, the barriers identified are not limited to the DTPS. Some counter-measures recommended by the researcher will only be effective with assistance from various other stakeholders mandated by the NCPF. This report fully outlines all the barriers uncovered during the research as well as the recommendations made by the researcher. Prior to focusing directly on the DTPS, the researcher firstly provided an overview of various published sources in the cybersecurity arena which is followed by an in-depth overview of the NCPF and thereafter focus is shifted to the DTPS.

1.1 Background

SA has seen a digitalisation in the official interactions in government departments with cyberspace being the medium of communication and storing information. Cyberspace is gaining prominence in SA, as many geographical regions are incorporated into the global village in an attempt aimed at bridging the digital divide (Grobler, Van Vuuren and Leenen, 2007). This advancement brings various advantages to the faced-paced communication in government departments and private companies as technology has got the capability of compressing time and space. As much as there are advantages to the advancements in technology, there are equally vulnerabilities to the information stored in the cloud as adversaries see this as a loophole when attempting to disrupt the operation of certain organisations.

In an effort aimed at eliminating these vulnerabilities, the South African government has implemented various cybersecurity initiatives which will be discussed later in the report. The focus of this research report, however, is on the NCPF which was approved in 2012 and handed over to the former DoC whose name was in 2014 changed to the DTPS. The NCPF is one of South African policy documents which was approved by cabinet and holds various government departments, led by the JSCP cluster, accountable to implement measures aimed at securing the cyberspace (Grobler *et al*., 2007). This mandate was in August 2012 given to SSA with the JCPS cluster still providing the oversight role (Grobler *et al*., 2007).

The NCPF was developed with an intention of centralising the coordination of cybersecurity activities through relevant structures, policy frameworks and strategies in support of cybersecurity in order to combat cybercrime, to address national security imperatives and enhance the information society and knowledge based economy (Van Nieuwkerk, 2015). This research is therefore aimed at uncovering whether or not the NCPF is effective in achieving its objectives since implementation and if it has not successfully achieved its goals, to analyse the barriers to implementation. To achieve this, the researcher has posed three overall research questions which will analyse whether or not the objectives of the NCPF have been attained since implementation, to analyse the key factors affecting policy outputs and impacts, and finally to propose measures which will assist in the effective implementation thereof.

When analysing the status of the South African cyberspace, the researcher chose a time frame of a 10 year period, from 2005 to 2015. The chosen time-frame gives the researcher sufficient time to analyse the status of the cyberspace before the NCPF was developed thereby unpacking the reasons and the need for the policy, thereafter, a focus will be on the years after the implementation of the policy framework with an intention of analysing the effectiveness of the policy proposal. After analysing the effective implementation, the researcher was in a position of fully analysing all factors either impeding or strengthening the policy implementation.

Also of significance is the fact that the researcher chose to look at cybersecurity from three levels namely; international level, regional level and national level. This together with the chosen time-frame has enabled the researcher to fully outline and therefore thoroughly analyse cyberspace. This was done with an intension of assessing the status thereof prior to the implementation of the NCPF as well as the changes post the implementation thereof. As soon as all the factors have been outlined as well as the barrier in implementation have been unpacked, the researcher will then provide an outline of the comments and recommendations which are believed will assist in the effective implementation of the objectives outlined in the NCPF.

The researcher thus selected the DTPS as it is one of the key government department mandated with the responsibility of implementing the NCPF. The researcher in this instance conducted one-on-one semi-structure interviews with five officials currently working with or who have previously worked with the implementation of the NCPF. Various barriers were identified by the researchers which are reported on in chapter five of this research. The researcher furthermore proposed recommendations which will be communicated to various critical role-players are mandated by the NCPF. The key target is the DTPS as it was chosen as an area of research and therefore more barriers were uncovered therein. The researcher will in this instance compile a summary of the findings alongside the proposed recommendations, a copy of which will be sent to the department. The researcher will furthermore compile different short reports directed to relevant NCPF stakeholders who are affected by the barriers identified and who are required in the implementation of the proposed recommendations.

1.2 Problem Statement

The NCPF as implemented in South African government department has not been successful in achieving its objective, which is the reduction and elimination of the growing cybercrimes and related incidents SA. This is as government departments and State Owned Entities are currently faced with an increase in such crimes. Mtsweni (nd) postulates that over 80% of government websites around the world are vulnerable to common web-based attacks and furthermore that over 50 South African website were hacked in both the government and the private sector in the year 2015. This is due to website developers that are slow or ignore the implementation of available and appropriate security countermeasures proposed to their organisations (Mtsweni, nd).

There are various reasons which can be attributed to the lack of effectiveness in the implementation of the NCPF. The increasing bandwidth and use of wireless technology and infrastructure, high levels of computer illiteracy, and insufficient legislation to deal with cyber-attacks and threats are some of the factors which are barriers in the implementation of the NCPF (Grobler *et al.,* 2007). Such reasons and various others are seen to be creating more risks to the already vulnerable South African cyberspace.

This research is therefore aimed at uncovering the possible barriers in the implementation of the NCPF. The focus of this research is on those government departments which are the custodians of the NCPF with a specific focus on the DTPS. This research report provides feedback on the progress made since the NCPF was implemented on a national level, thereafter, the focus is shifted to the DTPS. The DTPS was chosen as an area of research due to it being the first national government department tasked with carrying out the NCPF mandate before the mandate was handed over to the State Security Agency (SSA) in August 2012. Furthermore, the DTPS is also responsible for the implementation of some of the cybersecurity initiatives outlined in the NCPF as stated in the introduction.

One of the critical government departments mandated with implementing the NCPF is SSA. The DTPS also had a huge role in the implementation process as it was the initial custodian of the said policy framework. The researcher is of the view that the DTPS played a significant role in the implementation of the policy framework and thus officials at the DTPS are in a better position to understand the policy framework as they are the key custodians thereof, hence it was chosen as an area of research. Finally, to avoid conflict of interest and to adhere to the professional SSA code of ethics, the researcher was unable to use SSA as an area of research due to current professional obligations and therefore the restrictions which limits the researcher in terms of the amount of data to be collected for research purposes.

This research has the capability of fully outlining the status of the South African cyberspace and also thoroughly uncovering the underlying barriers which are affecting the implementation of the NCPF as well as various other cybersecurity initiatives proposed by the South African government. Given the current status of the South African cyberspace, it can be agreed that there is not enough emphasis on the implementation of the proposals outlined in the NCPF. Various reasons can be provided for this and therefore this research will unpack all identified barriers. The literature review provides a solid starting point which will be verified by the data collected during the interview process.

1.3 Purpose Statement

The purpose of this research is in three forms, firstly it is to assess whether or not the NCPF was effectively implemented as intended and if not; to unpack and understand the barriers which are affecting the implementation thereof, and finally to make recommendations on how to effectively improve the implementation of the NCPF as well as various other policy proposals aimed at strengthening the South African cyberspace.

1.4 Research Questions

Due to the robustness and diverse nature of this research, the researcher made a decision to have three overall research questions as outlined below;

1. To what extent were the objectives of the NCPF attained since implementation?
2. What key factors strengthen or impede policy outputs and impacts?
3. What measures should be put in place to ensure the effective implementation of the NCPF?

1.5 Draft Outline of Chapters

Chapter one of this report provides an introduction to the research thereby setting a scene for the chosen research area in terms of the problem statement, research problem, research objectives as well as the three overall research questions which provide guidance to the entire research. This section unpacks the problem statement in detail and the purpose of the research. It is in this section that the researcher outlined the reasons for the development of the NCPF by the South African cabinet. Furthermore, the researcher, in this section also outlined the key custodians tasked with the implementation of the NCPF, as outline later in the report, as well as the JCPS being tasked to provide the oversight role.

Chapter 2 provides an overview of all sources consulted in the research area. The purpose of the literature review is to provide an overview of all publications in the chosen research area. The global status of cyberspace will be outlined, followed by an overview of the South African cyberspace, the report will provide an outline of the cybersecurity measures proposed internationally, regionally and nationally, and finally the barriers in the implementation of the proposed cybersecurity measures in the South African context will be unpacked. As the means of analysing the status of the implementation of the NCPF and the barriers identified, the researcher made use of the 5-C protocol which acts as a model to be followed when analysing policy implementation. The components of the 5-C protocol namely; content, context,

commitment, capacity, clients and coalitions are fully outlined in the introductory part of the literature review as they provide guidance towards policy analysis.

The third chapter of this report provides an overview of the research methodology which fully outlines the methodology followed by the researcher throughout the research. This research consists of a qualitative research methodology, the method of data collection is semi-structured interviews which were conducted at the DTPS. The researcher furthermore chose a non-probability sampling strategy with the purposive sampling method being chosen as the researcher deliberately decided to interview those individuals who are working in and around the implementation of the NCPF. A snow-ball sampling method was also utilised as the researcher also relied on referrals in terms of respondents to interview for data collection purposes.

Chapter three furthermore outlined the method and approach of data analysis with the thematic approach being seen as the appropriate method to be followed by the research. A deductive approach to analysis was followed as the researcher already had preconceived codes guided by the literature. The research then outlines the ethical issues in conducting this particular study and as such provides an in-depth analysis of issues of anonymity and confidentiality. The last part of this section provides an outline of the possible risks which can be associated with the study as well as how the researcher aims to eliminate the possibility thereof as well as how to react should such possible risks be manifested.

Chapter four focuses on the NCPF as the main focus point of the study. This chapter outlines the NCPF in terms of its goals and objectives, the stakeholders and role-players, the underlying goals and objectives, the structure of the NCPF, the role played by the Cybersecurity Hub and sector CSIRT's, and finally what elements are critical in the implementation of the NCPF. This section highlights the important role played by the JCPS Cluster in the implementation of the cybersecurity measures outlined in the policy framework through the JSCP implementation plan.

Chapter five focuses on the research findings gathered during the data collection phase conducted at the DTPS. The researcher, in this section, provides an overview of the responses gathered from the interviews which is followed by an analysis conducted by the researcher in an effort aimed at addressing the research question. The researcher in this section provides an analysis of the findings gathered which is

supported by the literature review conducted in chapter two of this report. Once completed with the analysis, the researcher moves on to chapter six which focuses on the conclusions and recommendations.

In chapter six, the researcher first makes conclusions based on the data gathered, it is in this section that the researcher outlines a total of eight barriers which are believed to be affecting the implementation of the NCPF according to the researcher. In the second part of this chapter, the researcher then makes recommendations which are aimed at addressing the identified barriers and which will be communicated to the DTPS as well as to relevant role-players as soon as the report has been authorised by the university. This is the only chapter which strictly consist of the researcher's viewpoints which are believed to be aimed at adding value to the current practice in terms of the implementation of the NCPF.

1.6 Significance of the research

The South African government department and State Owned Entities (SoE) are using the internet as a medium of communication. This has had a positive impact on the fast-paced and interactive nature of communication which has led to the establishment of open and interactive communication and thereby increasing public trust in the government. Cyberspace, as the platform used for such communication and the storage of information has seen drastic developments in the contemporary times and as such, there are more developments aimed at making it more effective and efficient.

As much as these advancements have a positive impact on the effectiveness of government departments and SoE's, the developments brought about by cyberspace and cloud computing have created vulnerabilities and therefore loopholes which cyber criminals perceive as opportunities to commit cybercrimes which can be in various forms. This research is aimed at conducting an in-depth analysis of the current status of the South African Cyber space with more focus on the DTPS. The researcher will in this instance fully analyse the intended objectives of the NCPF and furthermore assess if they were effectively implemented or not. The researcher will also analyse if there are any barriers in the implementation of the said policy

framework and finally make recommendations on the effective implementation thereof. The recommendations will be communicated to the DTPS as well as to other stakeholders working in and around the implementation of the NCPF. This will be done in two forms; firstly by sending a summarised copy of this report to the intended department which will be accompanied by a letter requesting to conduct a PowerPoint presentation outlining the research findings alongside proposed recommendations.

The researcher furthermore will assess and analyse how effective the DTPS has been in the implementation of those NCPF objectives of which were their responsibility. The researcher will in this instance analyse the effective implementation of measures such as the establishment of the of a national Cybersecurity Centre, the effective rolling out of a cybersecurity awareness program as well as the establishment of Sector CSIRTs since the approval of the NCPF in 2012. This section will then be followed by an analysis of the barriers in the implementation of the NCPF which will be followed by the recommendations which will be proposed by the researcher.

This research is aimed solely at adding value to the current status of the implementation of the NCPF, this is as the researcher intends sending a summarized copy of the report to the DTPS as well as to other stakeholders who are affected by the barriers identified and who the researcher believe are required in the implementation of the recommendations proposed at the end of this report. This report is highly valid as it is aimed at advising those departments involved in the implementation of the NCPF on how to effectively implement the policy proposal as projected.

1.7 Conclusion

This section of the report is an introductory section which has outlined the research purpose, problem statement, research questions, intended objectives and the significance of the research. The purpose of this research as outlined is to conduct an in-depth analysis of the NCPF with an intension of identifying the possible barriers in the implementation thereof and to furthermore make recommendation on how to

effectively implement it. To arrive at this however, the researcher will start by providing an international overview of the cyberspace which will be followed by a regional overview and finally a national overview which will be followed by an analysis of the barriers in implementation.

This section has provided a solid background behind the purpose and scope of the research, it has outlined the three purposes of this research which included assessing whether or not the NCPF was effectively implemented, assessing any barriers in its implementation and finally to make recommendations on the effective implementation thereof. Due to the diverse nature of cybersecurity, there are three overall research questions which have been formulated with an intention of providing a solid direction towards achieving the research objectives namely; to what extent were the objectives of the NCPF attained since implementation? what key factors strengthen or impede policy outputs and impacts? what measures should be put in place to ensure the effective implementation of the NCPF? And finally, what measures should be put in place to ensure the effective implementation of the NCPF?

The researcher then outlined the significance of this research which is highly significant as it is aimed at positively contributing towards making the NCPF more effective and finally towards assisting in curbing the growing cybercrimes and related incidents. The researcher furthermore intends making recommendations to stakeholders involved in the implementation of the NCPF on measures aimed at assisting in the implementation of the policy framework. The following chapter will provide an overview of various sources consulted in a form of a literature review. The purpose of this chapter is to provide an in-depth analysis of the secondary sources so as to ascertain what the view of various scholars on the subject of cybersecurity internationally, regionally and within SA.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Chapter two provides an outline of the sources consulted in the chosen research area. The researcher consulted various sources which have assisted in providing guidance on the focus and scope of the research. All sources consulted are believed to be providing a solid background on the status of cybersecurity in SA as well as a thorough explanation of the NCPF since its inception until recently. As much as the research is aimed at unpacking the barriers affecting the NCPF, the chosen time-frame is ten years, from 2005 to 2015, this is as the researcher believes that this period gives a clear picture of the South African cyberspace over an extended period of time.

The NCPF is a policy framework which was decided on by the JCPS cluster as part of its mandate and obligations under outcome three/output seven (Institute for Security Studies, 2015). The NCPF is intended to provide a holistic approach and is supported by the national cybersecurity implementation plan; the JCPS, working in consultation with various government departments oversees the realization of the implementation plan; the JCPS Cybersecurity Response Committee (CRC), chaired by the State Security Agency (SSA) has been established to ensure the implementation of output seven further supported by the Cyber Security Centres (CSC); and finally, in terms of NCPF an approved Cyber Crime Strategy needs to be presented by the South African Police Services as the lead department (Institute for Security Studies, 2015).

Approved in 2012, the overall objective of the NCPF is to centralise the coordination of cybersecurity activities through relevant structures, policy frameworks and strategies in support of cybersecurity in order to combat cybercrime, address national security imperatives and enhance the information security and knowledge based economy (Van Nieuwkerk, 2015). This section is primarily aimed at determining if the stakeholders tasked with the implementation of these policy proposals were effective in achieving their goals and objectives. This section will look at secondary data in forms of journal articles, books, research papers and various published dissertations with a focus on the subject matter.

This literature review will focus on the theoretical and academic discourse underlying the bodies of knowledge behind the status of the South African cyberspace between the chosen time-frame. Here the focus will be on how vulnerable the cyberspace is to cybercrime and related incidents. The second section will unpack various proposals made by the South African government departments in an effort aimed at curbing the growing threats to the cyberspace. Finally, the identified barrier in the implementation of such measures will be outlined. The 5-C protocol was chosen by the researcher as a model to be followed when analysing the effective implementation of the NCPF.

2.2 The 5-C Protocol

When analysing the effective implementation of the NCPF, the researcher followed the 5-C protocol which specifies the key elements in the policy implementation process. Policy implementation is regarded by Cloete and Wissink (2000) as not simply a managerial or administrative problem but rather a political process concerned with who gets what, when, how, where and from whom. The 5-C protocol can be regarded as an analytical framework which shapes the route which policy implementation should take. “Five such variables emerge which are important causal factors for a multitude of scholars adhering to otherwise divergent perspectives (top-down or bottom-up), working on differing issues (environment, education e.t.c), and in countries at various levels of economic development (Industrial or developing) (Cloete *et al*., 2000, p.178)

Content

The content of any policy proposed is crucial not only in the means it employs to achieving its ends, but also in its determination of the ends themself and also in how it chooses the specific means to reach the ends (Cloete *et al.,* 2000). This therefore means that the content of any given policy is highly important as it outlines clearly the purpose, focus and intended objectives which are to be achieved by all stakeholders concerned. When analysing the implementation of policies, it is therefore important to study the contents, purpose and goals of a policy proposed. This is furthermore emphasised by Lowi in Cloete *et al* (2000) who characterises policy content as distributive, regulatory or redistributive. A mandate outlining the

reason for a policy should be stated alongside the content of any given policy. Grobler *et al* (2007, p.3) asserts that "If the government is involved, there needs to be an appropriate and explicit mandate for any CSIRT establishing operations. Generally, if the mandate comes from the most senior position in government as far as possible, the better the chances to ensure a clear project mandate"

Context

Also of importance in the policy implementation process is the context within which the policy should be implemented. This refers to the institutional context which according to Cloete *et al* (2000) will necessarily be shaped by the larger context of the social, economic, political and legal realities in any given system. It is therefore important that there are effective working relations amongst all stakeholders involved in the implementation process in any given organisation, such effective relations often result from "bargaining, cajoling, accommodation, threats, gestures of respect and related transactions (Cloete *et al.,* 2000, p.180). It is thus believed by Grobler *et al* (2007) that cultural backgrounds and working environments are of importance when implementing a policy, some of the problems relates to the cost and logistics of travelling between countries, decision-making and openness with regards to mandate and agendas, and a political decision.

Commitment

As much as the policy, content and implementation context are of importance, what is also critical is the attitude of all stakeholders entrusted with the responsibility of policy implementation. Without any commitment from officials employed in an organisation or contracted with policy implementation, a policy will not be effectively implemented as intended. This is despite the appropriate content and environmentally suitable context. Cloete *et al (*2000) believe that commitment will influence and be influenced by all four remaining variables namely content, context, capacity and clients or coalitions. Management commitment and support is also of importance in this regard and as such "A key element for any successful project is to obtain management support within the organisation driving the project. Management support should last throughout the project: from the planning to the implementation,

through to project closure. In addition, it is important that management support be wide-ranging and displayed publicly in support of the project team" (Grobler *et al*., 2010, p.4).

Capacity

Capacity is seen by Cloete *et al (*2000, p.181) as "… the structural, functional and cultural ability to implement the policy objectives of the government…". This simply refers to the availability of and access to conserve both tangible and non-tangible resources to carry-out the tasks. The capacity factor is often a political matter as resource allocation deals with questions of who gets what, when, how, where and from who. The gatekeepers in any given organisation must ensure that the organisation is capacitated with all resources required in the policy implementation this include official equipment, staff members and moral support from organisational leaders. It is furthermore believed by Grobler *et al* (2010) that in addition to human resources, technical resources also play a key role in the policy implementation process. The project leaders establishing the national CSIRT should ensure that the team is able to purchase all needed equipments, accessories and systems, and finally there should be appropriate measures in place to monitor the progress of team members Grobler *et al* (2010).

Clients and Coalitions

Elmore in Cloete *et al (2*000, p.185) believes that "… implementation is affected, in some 'critical sense' by the formation of local coalitions of individuals affected by the policy to be one of the 'most robust' findings of implementation research". During the policy development phase, the policy developers should at all times consider the interests of the policy end-user. A policy must therefore be tailored in such a manner that it caters for the needs, interests and desires of such individual. The clients are thus of importance as they can determine the effectiveness of a policy or the lack thereof. The clients and coalitions are effective stakeholders which can assist in the determination of the status of cybersecurity. Such individuals can also oppose, and build strong resistance to the chances for successful implementation.

2.3 The global status of cyberspace

Cloud computing is a new and emerging invention that changes the way Information Technology (IT) solutions are put forward in terms of moving towards virtualisation of data storage, of local networks and softwares (Ramgovind, Eloff and Smith, 2010). The success of modern-day technology largely depends on the effectiveness of the world's norms, its ease of use and finally the degree of information security and control (Ramgovind et al, 2010). Cassim (2015) postulates that cybercrime is not bound by geographical boundaries, "it is unnecessary for the perpetrator and the victim to meet, as the unlawful actions committed by the perpetrator in one country may have a direct and immediate effect in another (Cassim, 2015).

The 2003 National Strategy to Secure Cyberspace defined cyberspace as "nervous (sic) systems- the control system of the country… composed of hundreds of thousands of interconnected computers, servers, routers, switches and fibre optic cables that allow our critical infrastructure to work" (Kuehl, nd). The concept of cybersecurity as defined earlier in the report is a global concept which is applied differently in various countries, however, the purpose being the same which is to secure the cyberspace. Incidents which occur on the cyberspace in any given time can have immediate effects in a country which is distant by geographical locations due to the compression of time and space which is brought about by the internet.

Creditcard.com, a compiler of credit cards statistics, published in 2005 that approximately 9.2 million United States (US) citizens reported a loss of credit card information, furthermore 42% of all identity theft cases in 2004 involved credit card fraud (Osaugwu, *et al*., 2010). In 2002/03 the British Crime Survey revealed that 18% of households with internet access stated that their computers have been affected by a virus, this had increased to 27% in 2003/04. Furthermore, the biennial Department of Trade and Industry Security Breaches Survey reported that 62% of UK businesses had a computer incident in 2006 (Osaugwu, *et al*., 2010).

The Philippines were also victims of cybercrimes and related incidents. The Philippine's failure to put cybercrime legislation in place resulted in a Philippine national inflicting damage during the 20th century without suffering any

consequences for this action (Cassim, 2015). The failure to have adequate legislations reverberated around the globe and illustrated the vulnerability of the modern network system. This therefore highlights that countries in both the developed and the developing states can at any point be affected by the cybercrimes and related incidents as such crimes are committed through the internet meaning therefore that they can be committed at a virtual point.

Internet connectivity has grown significantly throughout the world, in both the developed and developing state. Africa, in particular has seen a huge increase in the number of people connected to the internet on a daily basis. The table below shows the current status of global Internet users, as well as the status of Internet users within the African continent (estimation based on December 2009 figures). Although the penetration of the Internet into Africa is minimal, the 1,809.8% with which the number of African users has grown from 2000 to 2009 is considerable. Unfortunately, this tremendous growth may be the catalyst of numerous threats to cyber space. (Grobler *et al*., 2007).

Region	Africa	Rest of the world	**World total**
Population	991,002,342	5,776,802,866	**6,767,805,208**
% world population	14.6%	85.4%	**100.0%**
Internet users	86,217,900	1,716,112,557	**1,802,330,457**
Penetration	8.7%	29.7%	**26.6%**
Use growth (2000 - 2009)	1,809.8%	381.4%	**399.3%**
% users in world	4.8%	95.2%	**100.0%**

Table 1: Internet User Statistics for Africa

2.4 The status of South African cyberspace

Studies have shown that cybercrime is a recent addition in the list of crimes. This phenomenon, according to Herselman and Warren (2010, p.25), “was not directly prosecutable in South Africa until the enactment of the ECT act in July 2002”. Van Nieuwkerk (2015, p.1) asserts that “the introduction of ICT in the public and private realism is forcing governments to face the realities of the security challenges that accompany such advancements. The sophistication and diversity of cyber-attacks are increasing and without proper cyber security measures the economic, political and social results of cybercrime and cyber espionage can be devastating”.

Tamarkin (2015, p.1) states that African governments, the private sector and individuals increasingly rely on the internet to conduct sensitive transactions and store important data. This often results to cyberspace becoming vulnerable to cybercrime mainly due to that “Most African states are lagging behind in strengthening cybersecurity and fighting cybercrime; cyber criminals have recognised this vulnerability and are targeting the continent” (Tamarkin, 2015, p.1). This is despite the fact that more people are becoming exposed to the internet on a daily basis.

The increasing vulnerability in the cyberspace has been “…compounded by the fact that some bureaucrats and politicians view the ICT revolution as a highly political affair and not a technical challenge” (Ngulube, 2007, p.2). As the world is migrating to the digital era whereby information is stored in the cloud, this often results to an emergence of threats to most countries. Ngulube (2007, p.2) provides an overview of the challenges facing Sub-Sahara Africa, “They include infrastructure development, law and public policy, digital divide, e-literacy, accessibility, trust, privacy, security, transparency, interoperability records management, permanent availability and preservation, education and marketing, public sector and private sector partnerships, workforce issues, cost structures and benchmarking.

The draft African Union (AU) convention on the confidence and security in cyberspace stated that each AU member state has to undertake measures to develop capacity building measures, mainly in and around the cyberspace (Pieterse,2015). Various measures have been proposed in SA and as such some have been implemented while others are still in the planning phase. The status of the

South African cyberspace however still remains vulnerable to cybercrimes and related incidents.

As of January 2014, the internet penetration rate in Africa was 18%, which is a 5% increase from 2013, the majority of internet users are located in Egypt, Morocco, Nigeria and SA while in some communities the internet reaches less than 1% of the total population mainly due to the lack of affordable and accessible internet (Rezaire, 2014). SA's access to the internet is above the 18% average in the continent and had reached 41% of the total population in 2014, however, 80.2% of South African users use smartphones to access the internet whilst 19.5% still use traditional methods, namely; household connection, internet cafés or connecting though work or university (Rezaire, 2014). It is stated by Osaugwu *et al* (2010) that many small businesses and even large organisations do not know how to properly protect their sensitive data thus leaving the door open to criminals, more vulnerable remains the developing countries who are yet to develop new skills in computer forensic to tackle the menace.

Until recently, a term coined 'New Crimes' was introduced in SA following the growth of cybercrimes and related incidents. New crimes is regarded by Herselman, *et al* (2010 as "…crimes that can be committed solely with the aid or use of a computer". The most common of such crimes is hacking which has recently been criminalised following the enactment of the Electronic Communication and Transaction (ECT) Act of 2002. Another unique form is the denial of service attack (DoS) outlined in Section 86(5) of the same act. "This occurs when the perpetrator sets up a computer program (possible a virus) that exploits the handshaking routine of regression" Herselman, *et al* (2010).

Due to technological advancements, South African banks have recently been victims of cybercriminals. It is only in recent years that the focus is shifting to individuals, businesses and government. Herselman, *et al* (2010) indicated that banks have been exposed to cybercrime and it is expected that this trend will increase. Bank fraud has been in the region of 50% internal and 50% outsider and most of the international jobs have relied on insider assistance (Gordon in (Herselman, *et al*., 2010). More recently has been an incident wherein approximately 1600 fraudulent credit cards issued by Standard Bank were used to commit fraud in various

Automated Teller Machines (ATM) in Japan, the bank is believed to have incurred approximately R300 million in losses (Khoza, 2016). Furthermore, one of the reasons banks expect cybercrime to increase is that as the bank business and individuals move away from cash towards electronic transactions, physical crime will be less attractive and a move will be made towards cybercrime (Herselman, *et al*, 2010).

Due to the increasing connectivity which stems from broadband availability, information systems and networks are more prone to a growing number of cyber threats and vulnerabilities, this has furthermore resulted to hackers defacing more than 60 South African websites in the year 2003 (Herselman, *et al.,* 2010). More recently, however, a group titled Anonymous claimed responsibility for defacing approximately 200 South African websites. These hackers leaked classified information belonging to government employees while at the same time exposing them to cybercrime. This incident occurred in February 2016 and the same group has indicated its intensions of attacking various countries throughout the African continent (Mokati, 2016).

IT has brought about change in history that has been described using labels such as network age, information society and knowledge economy. Governments in the developing world, although prone to cybercrime, have been able to well respond to the problems being experienced, however, those in the Sub-Sahara Africa have not adequately restructured public bureaucracies in response to the demands of the information society (Ngulube, 2007). And as such had more vulnerabilities to the cyberspace with more cyber related incidents being reported in recent times.

Most South Africa government departments are making use of the internet as a medium of interaction, this is seen in terms of the interaction between government departments and the general public, a term known as E-government. This simply "Refers to governments use of technology, particularly web-based internet applications, to enhance the access to and delivery of government information and service to citizens, business partners, employees, other government departments , and government entities" (Ngulube, 2007, p.10). The E-governments have got the capability of promoting a better life characterised by representative and participatory democracy, transparent, open and collaborative decision making, close relations

between government, enhanced service delivery and a seamless government service (Ngulube, 2007).

In an effort aimed at rolling out such E-government, government departments were confronted with problems which have as a result affected the rolling out thereof as well as the security of such governments. These problems included infrastructure development, law and public policy, digital divide, e-literacy, accessibility, trust, privacy, security, transparency and records management (Ngulube, 2007).

Information literacy refers to the persons' ability to "recognise when information is needed and have the ability to locate, evaluate and use effectively the information needed" (Ngulube, 2007). This is also closely related to information security and awareness. The lack of such knowledge is one of the major problems facing SA in the contemporary times as the people lack the required skills and training in the information management as well as in the protection of sensitive information. African government departments have often been criticised for not focusing on cybersecurity measures and the training of relevant officials. Cassim (2015) postulates that "African countries are perceived to be preoccupied with attempting to be attending to issues such as alleviating poverty, the AIDS crisis, the fuel crisis, political instability, ethnic instability, and traditional crimes such as murder, rape and theft, as a result, the fight against cybercrime is lagging behind.

There also have been new and innovative forms of cybercrimes which ultimately affected SA government departments. An incident occurred at the Mpumalanga Department of Education where a suspected cyber hacker stole R5.5million from the department's bank account The North Gauteng High Court awarded a court order to seize the account of a person believed to be a suspect, only R1543 345.00 could be seized as the remainder was shipped off and disappeared without a trace (Cassim, 2015). This occurred as there were insufficient measures in place to secure the cyberspace and as such led to more vulnerabilities thereto.

Phishing is also seen as a new form of cybercrime which is heavily affecting banks in the country at large. Phishing is found to be the most common type of fraud which involves the online theft of internet user identities. "The South African Banking Risk Information Centre (SABRIC) has reported that the incident of phishing has more than trebled since January 2001" (Cassim, 2015, p.131). A report by the

TrendMicro, an ICT security company, concluded that Africa is becoming a cybercrime safe harbour because of increase internet availability at lower costs, a rapidly growing internet user base as a depth of cyber laws on the continent (Tarmakini, 2015). Cybercriminals are, according to Tarmakini (2015) developing more advanced and lucrative forms of cybercrimes which involves the use of botnets, remote access, Trojans and various malwares, African states on the other hand fail to adequately address the evolving cybercrime problems which adversely affects the national economy and national security.

Unlike physical crimes, the perpetrators and victims of cybercrime are not bound by geographical boundaries as all cybercrimes are committed on the internet. This is also emphasised by Tarmakini (2015) who postulates that the transnational nature of most crimes contributes to the complexities of sovereign, jurisdiction , extraterritorial evidence and international co-operation. Additionally, the issues faced also remains "extradition, mutual legal assistance, mutual recognition of foreign judgements, and information police-to-police cooperation" (Tarmakini, 2015, p.2).

Also adding to the vulnerability of the South African cyberspace is the increase usage of social network pages. Goredema (2012) made an observation that the primary sources of risks are also the increase in the number of people sharing information through internet facilitated social networking sites as well as the phenomenal growth in the use of computer devices in the form of smartphones. Data released by the International Data Corporation in 2014 indicted that the Global Sales of mobile phones have escalated from R1.391billion in 2010 to R1.546billion by the end of 2011, at that stage, there were R5.9bn mobile phone users and SA had approximately R42.3million contract subscribers.

The figures furthermore indicate that 65% of South African households have got access to a cellular phone on contract compared to only 20% who only have access to a landline, the highest of this population being in the Gauteng Province with 48%, followed by Western Cape with 43% and the lowest being in the Eastern Cape with 24% (Gorendema, 2012). The danger with the usage of these devices is that users are often not aware of the potential criminal uses of some of the information transmitted and therefore unwillingly provide adversaries with sensitive information thereby giving them leverage to commit crime.

Due to the global interconnectivity of the internet, its borderless nature, its anonymity, fastness and its ability to store high volumes of rich data such as financial data, personal information, military information and business information, cybercriminals can easily build complex systems aimed at stealing money and information thereby causing damage to the economy which is equivalent to more than that of counterfeit goods and/or narcotics trade (Tarmakini, 2015).

Furthermore, most developing countries, such as SA lack adequate laws which criminalise cybercrime, they lack the means to enforce existing statutes, have got few tools to investigate cybercrime and thus lack sufficient infrastructure for information sharing and international co-operation (Van Nieuwkerk, 2015). Until recently, cybercrimes were not directly prosecutable in SA and even after the cybercrimes have been prosecutable, it still remains a problem as law enforcement agencies are either not fully trained on how to respond to a cyber-incident or do not have the required technology to gather evidence where required.

The lack of knowledge has been seen as one of the other factors affecting SA in the modern era, this lack of knowledge leads to unsecure behaviour by internet users and as such this lack of the relevant knowledge has made the African population easy targets for hackers and botnet operators (Von Solms, 2015). Despite the low internet penetration rate, SA ranks third in the world after the United States of America (USA) and the United Kingdom (UK) in terms of the number of cyber-attacks encountered (Amit in Grobler et al., 2007).

Also to take note is the time delay between policy enactment and implementation, this is highlighted by Van Nieuwkerk as he states that “Due to the swift evolution in cybercrime techniques and advancements in ICT, policy makers must be quick to shorten the gap between development and efficient implementation of policy” (Van Nieuwkerk, 2015, p.1). The results of this are often that the policies are out-dated during their intended implementation phases. There are various reasons for such delays most of them often being administrative in nature and some often involving the lack of adequate resources to fully implement the policy.

Goredema (2012, p.1) believes that “the scope of activities which could fall within the definition of cybercrime is very broad ranging from purely malicious or intimidatory invasion of privacy, to the theft and abuse of personal identity particulars and the

fraudulent manipulation of electronic data to commit theft". An example of malicious invasion can be seen as hacking, which is defined by Herselman, *et al* (2010, p.254) as "the unauthorised access of a computer system or network". Osuagwu *et al* (2010, p.22) provide an overview of types of attacks to computers or computer networks.

Common types of malware works in four forms namely; viruses, which infects a computer and are passed by user activity; worms, self-propagate using an internet connection to access vulnerabilities on other computers and to install copies on them; Trojans are malware masquandering as something the user may want to download or install, that may perform hidden or unexpected actions; spy ware transmits information gathered from a computer, such as bank details to an attacker (Osuagwu *et al*., 2010, p.22).

Another critical problem facing SA is the absence of formalised organisations mandated to carry out cyber security. This is closely related to the context and commitment aspects of the analytical framework discussed earlier in this section. This is highlighted by Van Nieuwkerk (2015, p.2) as he states that "The absence of assigned agencies in many African nations to address issues of cybersecurity makes it unlikely for coordinated policy decisions to be made". There are however, other formalised organisations established which are not as effective as they are intended to be due to a lack of sufficient resources both human and non-human. This is furthermore emphasised by Cassim (2015, p.127) as he states that "African countries have also been criticised for dealing inadequately with cybercrime, as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure". The shortage of these critical resources can be attributed to a number of factors such as the lack of knowledge.

Another issue facing the South African government is the complications related to prosecuting cyber criminals, known as capacity in the 5-C Protocol. (Cassim, 2015, p.125) emphasises that "Criminal laws regulating cyberspace tend to result in few prosecutions due to the judicial difficulties and additional resources required in tracking down cyber criminals in different countries". History has proven that until recently, there have been a number of cyber criminals which were not prosecuted mainly due to a lack of applicable laws to prosecute cybercrime. With these identified

vulnerabilities, the South African government has proposed various counter measures, and the following section unpacks them.

2.5 Current cybersecurity measures

2.5.1 Internationally

Internationally, the European Convention on Cybercrimes (CECC) was signed in Hungary on 23 November 2001 and is aimed at encouraging countries to curb cybercrimes (Cassim, 2015). The main objective of the CECC is to advance a common criminal policy aimed at the protection of society against cybercrime more specifically by adopting appropriate legislation and fostering international co-operation (Cassim, 2015). This convention was signed by SA as it criminalises certain computer crimes such as the interception of non-public transmission of computer data, it establishes corporate liability, it calls for the production of stored computer data and recommends mutual assistance between countries in cybercrimes investigations (Cassim, 2015).

The CECC provide a sound basis for essential cross-border law enforcement co-operation which are required to combat cybercrimes; it serves as a purpose built mechanism on which countries can design their own domestic legislations and enhance international co-operation in relation to cybercrime (Cassim, 2015). As much as the CECC was signed by SA, it has however, not been ratified. The CECC can furthermore be regarded as the comprehensive powers to expedite preservation of stored computer data and partial disclosure of traffic data, its intentions are to make production orders, search computer systems, seize stored computer data, enable real time collection of traffic data and finally intercept the content of questionable electronic data (Pieterse, 2015).

According to Cassim (2015, p.126) “The CECC criminalises certain computer actions such as the integration of non-public transmission of computer data; establishes corporate liability; calls for the production of stored computer data; and recommends mutual assistance between countries in investigations”. The CECC was adopted by SA, it was however, not been ratified due to a number of factor most of being political in nature. It has however acted as a good guideline when public sector policies were developed in relation to cybersecurity.

The USA established the US/SA cyber working groups. These working groups identified areas of mutual interest and strengthened opportunities for cooperation (Pieterse, 2015). The focus of the US/SA cyber working groups is on the provision of technical assistance, capacity building, training and the sharing of best practices between the USA and SA. Also projected by the working groups is that future meetings held will also include private sector and civil society stakeholders. Since USA is more advance when compared to SA, they in this instance provide training in all areas of needs as determined by SA.

2.5.2 Regionally

Regionally, there have been various initiatives aimed at addressing the increasing cybercrimes and related incidents in SA. The AU has created the African Chatter on the Values and Principles of Public Service and Administration which speaks to issues of access to information and the role of ICT in the delivery of services (Van Nuewkerk, 2015). As part of its objectives, the AU African Chatter on the Values and Principles of Public Services and Administration aims to contribute to improving the working conditions of public service employees and to protect their rights (Yankey, 2013). The chatter furthermore strives to encourage efforts made by State Parties aimed at modernising the administration and the building of capacities in order to improve the quality of public services rendered (Yankey, 2013).

As an AU member state, SA adopted the AU convention of cybersecurity and personal data protection in 2014. The convention has however not been ratified and will only be ratified when it has been accepted by at least 15 AU member states out of a total of 56 member states, if adopted and ratified, it can play a critical role in improving cybersecurity in Africa (Von Solms, 2015). This factor displays a lack of commitment by stakeholders concerned as a critical factor in the 5-C protocol. This convention can be used by countries in various ways such as in conducting a self-assessment by a specific country against the specifications of a convention as well as in comparing a country with various AU member states to assess how they compare as far as the set requirements are concerned (Von Solms, 2015).

This convention was a culmination of the process which started with the Oliver Tambo Declaration at an extraordinary session of the AU in 2009, here the member states were required to jointly develop "…a convention on cyber legislation based on the continents' needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection" (Tarmakini, 2015, p.3). This convention was later adopted in June 2014.

The AU convention requires African States to adopt laws which criminalises attacks on computer systems (fraudulently accessing a computer system), computerised data breaches (fraudulently intercepting data), content-related offences (disseminating child pornography) and offences relating to the electronic message security measures (Tarmakini, 2015). This convention furthermore requires African States to establish appropriate institutions to combat cybercrimes and to offer training to those stakeholders tasked with countering cybercrime, this furthermore emphasises the importance of enhancing international co-operation to fight cybercrime (Tarmakini, 2015). Finally the AU convention requires African states to enact cybercrime offences that are punishable by effective, proportionate and dissuasive criminal penalties (Tarmakini, 2015).

2.5.3 Nationally

Cybersecurity has been a priority in the South African government since the early 1990's, this is evident as there are various legislations which have been passed from as early as 1992. Van Nieuwkerk (2015, p.3) states that these legislations consists of "(a) interception and monitoring prohibition act of 1992 which focuses on telephonic and postal communication and its legal interception; (b) prevention of organized crime act of 1998 introduced measures to help combat organised crime, money laundering and gang activity; (c) electronic communications and transaction act of 2002 which aims to facilitate and regulate electronic communication and transactions" Van Nieuwkerk (2015, p.3).

The Interception and Monitoring Prohibition Act no 27 of 1992 (IM) was approved with an intention of addressing the identified cyber threats. The purpose of this act is "To prohibit and intercept certain communication and the monitoring of certain

conversations; to provide for the interception of the postal articles and communications and for the monitoring of conversations in the case of a serious offence or if the security of the republic is threatened; and to provide for matters connected therewith (Interception and Monitoring Prohibition Act, 1992, p.1). This is one of the earlier policy proposals made in the country and was able to set the scene and following its implementation, more advance policies were proposed. This act was implemented in some aspect however it could not achieve all objectives set mainly due to amongst others, a lack of organisations to carry out the mandate.

Following the promulgation of the IM Act, there had been an increase in the use of advance telecommunication technologies including cellphones, satellite communications, emails and various other modes of electronic communication (Interception and Monitoring Prohibition Act, 1992). The IM, though effective, currently needs to be updated or to be supported with more modern policies in order to keep pace with the ever-changing cyberspace. This is due to the dynamic and ever-changing nature of the cyberspace as well as the more active and highly dynamic cybercriminals.

The Prevention of Organised Crimes Act (POCA) no 121 of 1998 is aimed at introducing measures aimed at combating organised crime, money laundering and criminal gangs, to prohibit racketeering activities, to provide for the prohibition of money laundering and for obligations to report certain information and to criminalise certain activities associated with gangs (Prevention of Organised Crime Act, 1998). POCA embodies an aggressive parliamentary stance against a rapid growing trend of organised crime, money laundering and criminal gangs (Prevention of Organised Crime Act, 1998). With regards to cybercrimes, this Act is not direct in the crimes covered, it merely refers to them as organised crimes. This Act was promulgated in 1998, it was less effective with regards to cybersecurity and as such more direct approaches needed to be established.

Various reasons can be provided for the lack of effectiveness in all the earlier Acts and policies proposed, Van Nieuwkerk (2015) believes that though these laws exist, their effectiveness have diminished overtime due to the insufficient training given to stakeholders entrusted with the implementation responsibility. This relates to the lack of the capacity aspect outlined in the 5-C protocol. What is therefore required in this

instance is to either amend the act or to formulate a policy which supports the actual implementation of the Acts outlined. Furthermore, the training of relevant officials should be made a key priority by all organisations concerned.

Also of significance, is the Electronic Communications and Transactions Act (ECTA) of 2002. The ECTA was promulgated in 2002 with the main objective being “To provide for the facilitation and regulation of electronic communications and transaction in the public interest” (Cassim, 2015, p.27). The act introduces new forms of crimes which are punishable under the law, crimes such as anti-cracking and hacking laws are introduced in the act, the latter being a law prohibiting the selling, designing or producing of anti-security circumventing technology (Cassim, 2015).

The objectives of the ECTA are to provide for facilitation/regulation of electronic communication/transactions to provide for the development of a national e-strategy, to promote universal access to electronic communication transactions, to prevent abuse of information systems and to encourage the use of E-government services (Pieterse, 2015). This act provides a legislative environment for secure electronic transactions in SA, it compels the Minister of Communications to have due regard for international best practices when it comes to electronic transactions matters, it introduced the concept of consumer protection by protecting consumers from unsecure communication, and furthermore sets out principles that govern the secure protection of personal information (Department of Telecommunication and Postal Services , 2009).

The Electronic Communications Transaction Act (ECTA) was enacted by the former South African president Thabo Mbeki in 2002. This act “repealed the previous computer evidence Act” (Herselman, *et al.,* 2010, p.254). This act according to Herselman, *et al* (2010, p.256) protects companies and individuals against theft, interception or interference of information; theft, fraud, forgery and extortion; aiding abetting cybercrime; and it also provides for penalties of contravening the act.

One of the definitions outlined in the act is that of access, which “includes actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access the data and still continues to use the data (Electronic Communication and Transaction Act, 2002). The actions of such an

individual are, according to the Act punishable under law and could lead to either a fine or imprisonment. The ECTA mainly protects companies and individuals against theft, interception, or interference of information; theft, fraud, forgery and extortion; aiding and abetting cybercrime; and the act also provides for penalties of contravention (Herselman and Warren, 2010). Crimes listed under the ECTA includes; unauthorised access, illicit tempering with files, or data, computer networks sabotage; use of information systems to commit or advance traditional crimes; computer-related espionage; violation against privacy by acquisition of computer data and the theft or damage of computer hardware or software (Herselman, *et al* 2010).

The Act furthermore created cyber-inspectors, those officials authorised to enter premises with an intention of obtaining information regarding cybercrimes (Cassim, 2015). As much as the cyber-inspectors are authorised to invade peoples properties with an intension of gathering data to be used as evidence when conducting an investigation, they are at times in conflict with the constitution as they are perceived as being in violation of section 14 and 25 of the South African constitution which deals with the right to privacy and the right to property respectively (Cassim, 2015).

The South African banking sector has seen the establishment of the South African Banking Risk Information Centre (SABRIC), a Non-Government Organisation aimed at combating crime in the banking sector. SABRIC according to Cassim (2015) provides the banking industry with crime the latest risk information management services and facilitates inter-bank initiatives to reduce the risk of organised bank-related crimes, through effective public-private partnership. SABRIC has created a platform for the police to collaborate with the banks and the IT industry in an effort aimed at combating cybercrime. Following the establishment of SABRIC, the South African banking sector has been very strict in terms of compelling banks to provide their clients with a safe and secure banking environment, failure to meet the set obligations could result to banks being held liable and therefore at times being sued for any losses incurred (Cassim, 2015).

The DTPS has got a responsibility of developing policies and industry standards concerning communication, the Department of Defence and Military Veterans is responsible for the implementation of cyber defence measures as it pertains to the

national defence mandate, and the Department of Science and Technology in the realm of cybersecurity Van Nieuwkerk (2015, p.4). All these departments work closely in terms of securing the South African cyberspace as well as in fighting the cybercrimes and related incidents.

The SA government has also partnered with academia in not only training its officials but also creating an awareness of cybersecurity in the public sector. In March 2014, the former Minister of SSA Dr Siyabonga Cwele provided a keynote address in a cybersecurity colloquium held at the WITS School of Governance. The colloquium was very successful in providing a platform for substantive discussion on the policy development management and capacity building issues in the arena of cybersecurity (The Cybersecurity Colloquium, 27 March 2014). One of the discussion points was the NCPF which is the focus of this research.

The NCPF was approved in 2012. The overall objective, according to Van Nieuwkerk (2015, p.3) being "…to centralise coordination of cybersecurity activities through relevant structures, policy frameworks and strategies in support of cybersecurity in order to combat cybercrime, address national security imperatives and enhance the information society and knowledge based economy". The NCPF outlined its purpose as being "…to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and understanding of cybersecurity in support of nation security imperatives and the economy (National Cyber Security Policy Framework, 201, p.15).

2.6 Reasons for ineffective cybersecurity measures in South Africa

It has been observed over the years that "Despite the time and effort put into the development of the policy framework, the process of implementation is still not complete" (Grobler, et al., 2007, p.1). There are various reasons which can be attributed to the failure thereof, most of them being administrative in nature often resulting to a lack of adequate resources required to effectively carry out the policy implementation. This section will unpack the reasons as published by various authors in the cybersecurity space.

The NCPF outlined in its milestones that it will establish the CSIRT and the CSERT at the end of March 2012, this however could not be achieved due to political will as there were mandate changes which resulted to the mandate being handed over to the DTPS Grobler *et al* (2010). This mandate was later on given to SSA. The results thereof led to there being a time-delay between policy development and policy implementation and as a result some of the measures proposed in the NCPF are currently not implemented as projected.

Another problem facing SA is the lack of adequate laws to make arrest and charge cyber criminals, this can also be regarded as a lack of capacity as outlined in the 5-C protocol Cassim (2015, p.125) states that "Police officials cannot prosecute cyber criminals unless countries have adequate laws in in place outlawing such criminal activities". Currently laws are being passed in SA, however they are not effective as law enforcement agencies do not have a thorough understanding of cybersecurity as well as various laws which are applicable. As alluded to earlier in the literature review, SA has adopted the CECC however, is has not ratified it.

Also related to the latter is the fact that there are currently weak penalties imposed on cybercriminals**.** The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects (McConnell International.2000). Also related to this is the fact that there are no measures in place to effectively prosecute a cybercriminal. This often leads to cybercriminals deliberately committing cybercrime often well aware that there will either be minor penalties imposed or no penalties all together, a practice termed impunity.

The diverse nature of the cybercrimes often leaves the governments' proposed cybersecurity measures outdated thereby unable to keep up with the ever-changing cybercrimes. Pieterse (2015) emphasises this aspect as he states that rapid developments and the exploitation of computers will continue to accelerate, with a concomitant increase in cybercrime threats and incidents and as such cyber criminals are becoming more sophisticated as they continue to develop new malicious software and also devising improved methods for infecting computers and networks.

A lack of awareness is also a factor affecting cyber security especially in government departments. Goredema (2012, p.2) furthermore postulates that “At this point, awareness of risks and how to mitigate them does not appear to be spreading as quickly as the escalation in the use of cyber-technology”. The SA government officials are exposed to the cyberspace on a daily basis, however, they are not well acquainted and therefore unaware of the threats they are exposed to as well as various countermeasures currently in place.

Also adding to the lack of awareness is the absence of African languages in cyberspace. The absence of African languages according to Grobler *et al* (2007) “has a direct impact on the vulnerability of the African cyberspace due to a lack of cognizance”. Most often, computer users willing to learn about cyberspace are restricted to do this, because African languages are used minimally in cyberspace (Grobler *et al*., 2007). This therefore often leads to these users unwittingly disclosing sensitive information which is often used by adversaries when committing cybercrime.

While the effects of cybercrime and all cyber related threats are well published globally, there is very little research currently available in SA especially within the government context. This is highlighted by Herselman *et al* (2010, p.256) as they postulate that “Research needs to be done on how badly South African companies are affected by cybercrime (if at all) and whether the newly promulgated laws will aid in preventing and prosecuting these crimes”. This often results in a lack of cybersecurity awareness. Also related to the lack of capacity by stakeholders tasked with the implementation of cybersecurity-related policies.

An effective law enforcement system is complicated by the transnational nature of and diversity of cyberspace, this is as the mechanisms of cooperation across national borders to solve and prosecute crimes are complex and as a result slow (McConnell International.2000). Cyber criminals are well aware of this deficiency and often deliberately defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources (McConnell International.2000). Such techniques drastically increase

both the technical and legal complexities of investigating and prosecuting cybercrimes.

Another problem is that the resources required in conducting a cyber-related investigation are often substantial while the crime may be high tech and as such investigating it often involves a substantial amount of traditional investigative work as well as highly technical skills which tends to be lacking in a country such as SA Pieterse (2015). This is the lack of commitment and capacity in terms of the 5-C protocol. There are also few organisations mandated to train such investigators and therefore often time the service is procured form international companies which is often highly expensive on the country and as such there is no consistency thereto.

2.7 Conclusion

This literature review has exposed the researcher to the current status of the South African cyberspace. When conducting research, the researcher was exposed to various threats in the SA government department as well as various measures introduced to curbs the spread of cybercrime. The focus of this research is on the barriers in the implementation of the NCPF, therefore, the researcher was exposed to common reasons for the ineffectiveness of the NCPF. This literature review exposed the researcher to a highly dynamic subject that is gaining prominence in SA as well the effectiveness of the NCPF in government departments.

The section of the research provided an in-depth overview of the sources consulted in the subject area. The researcher started off by presenting an international perspective on the status of cybersecurity whereby, the current impact of cybercrimes and related incidents on a global scale was provided with a focus on the US, UK and the Philippines. The researcher in this instance made mention of the growing impact of cybercrime in these countries with an intention of outlining that though developed, such countries are also victims of cybercrime.

The researcher also provided an outline of the international cybersecurity measures which SA is also party to. The researcher, in this instance made reference to two important international measures namely the CECC which is aimed at advancing the common criminal policy aimed at the protection of society against cybercrime more

specifically by adopting appropriate legislation and fostering international co-operation; the US/SA cyber working groups was also referred to as working groups which identifies areas of mutual interests and strengthened opportunities for cooperation.

Regionally, there are also various initiatives which are established with a common purpose of curbing and reducing the growing cybercrimes and related incidents. The AU African Chatter on the Values and Principles of Public Services and Administration was referred to as a chatter which is aimed at contributing towards improving the working conditions of public service employees and to protect their rights, this convention is also regarded as a convention which can be used by countries in various ways such as in conducting a self-assessment by a specific country against the specifications of a convention as well as in comparing a country with various AU member states to assess how they compare as far as the set requirements are concerned

Nationally, reference was made on various measures introduced by the South African government departments. Reference was made to the Interception and Monitoring Prohibition Act no 27 of 1992 (IM), the Prevention of Organised Crimes Act (POCA) no 121 of 1998, the Electronic Communications and Transactions Act (ECTA) of 2002., the South African Banking Risk Information Centre (SABRIC), and the NCPF of 2012 which is the focus of this research. The research clearly outlined the main reasons behind the formulation of these policies as well as their key objectives and finally how they intend reaching their objectives.

This section of the literature review ended with an analysis of the effectiveness of the South African cybersecurity measure as well as the reasons behind the barrier on implementation. To achieve this, the researcher consulted various sources who all have a common ground which states that there are barriers in the implementation of the NCPF. Various barriers are outlined and they range from administrative problem, political problems, capacity contains ineffective criminal justice system, unclear legal system as well as the lack of funding in some instances. The next chapter will focus on the methodology used during data collection.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The focus of this chapter is on the selected research methodology and the method of data collection. This research will follow a qualitative research design as the researcher intends to gather the first account of data through the usage of qualitative methods of data collection. The researcher in this instance gathered data directly from the respondents and as such the qualitative research design was seen as a suitable form of research design. This section of the report will fully outline the strategy which will be followed in arriving at answering the research question.

This is an interpretative research which is inductive in nature as the researcher will move from the specifics to the general and therefore the conclusions will be guided by the data inductively gathered during the data collection phase. Survey research has been chosen as a method of data collection with a specific focus on the DTPS as a case study. The researcher has in this instance conducted semi-structured interviews to available respondents at the DPTS. Appointments were confirmed prior with the respondents and each interview approximately 20minutes. The researcher reserved additional days to spend at the DTPS premises post the data collection and also communicated the dates with the respondents thereby inviting them in cases where there is additional information to be communicated to the researcher.

This research followed a non-probability sampling strategy as the respondents were included in the research because they were willing and available to participate in the study. A purposive sampling method was therefore used as the researcher's focus was on those business units dealing with the policies and strategy planning and implementation. The researcher was highly intentional in the selection of respondents as only those respondents exposed to and working around the implementation of the NCPF were selected to participate in the study. A snowball sampling method was used as the researcher also interviewed respondents referred to by other respondents.

This section of the report will therefore provide an in-depth overview of the methodology and methods followed in this research with a point of departure being the explanation of the research approach and design which will be followed by an overview of the sampling strategy and then an in-depth explanation of the data gathering phase.

3.2 Research Approach and Design

This is a qualitative research design as the researcher "strives to create a coherent story as it is seen through the eyes of those who are part of that story…" (Wagner *et al.,* 2012). The researcher's intention was to gather the first account of data as information was being provided by the recipients, and as such, the researcher was the main source of data collection. Therefore the qualitative research design was chosen as the appropriate research methodology due to "… the richness and depth of explorations and descriptions of data" (Wagner, et al., 2012, p.126).

This research is basic in its approach and it is motivated by the intellectual interests of the researcher in a phenomenon, it furthermore has as its main goals the extension of knowledge (Merran, 2009). The underlying objective of the research is to establish knowledge and understanding of the status and practice of cybersecurity in SA. The focus however, is on understanding the NCFP in terms of how effective it has been since implementation, if it has not been effective, to furthermore understand the factors which have contributed to it not achieving its main targets and finally to make recommendations on the effective implementation thereof.

The unit of analysis for the purpose of this study is the policy, and more specifically its implementation process. The researcher studied and analysed the process of implementation of the NCPF. To do this, the researcher made use of the 5-C Protocol as a guiding model. The researcher intended studying the effective implementation of the policy framework and as the literature review outlined that there was a lack of an effective implementation thereof, the researcher then studied the barriers in the implementation of the said policy framework and finally made proposals on how to effectively implement the NCPF as well as other cybersecurity-related policies.

This research was based on the collection of primary data and therefore the researcher was the primary instrument in the data collection and analysis processes. This is because the researcher could expand the current knowledge and understanding through non-verbal as well as verbal communication, processes and analyse data immediately, clarify any uncertainties, checking with respondents for any clarity when uncertain and finally explore unusual or unanticipated responses (Merriam, 2009). The interactive nature of the method of data collection furthermore enabled the researcher to establish relations with respondents thereby creating an open and interactive research climate. This therefore enabled the researcher to establish on-going relationship with respondents so as to continually study and thus make contributions to the chosen study area.

This research is mainly interpretative and highly inductive in its reasoning. Inductive reasoning is a form of reasoning whereby theory or the revision of theory is the outcome of the research, this therefore means that theory is drawn from the findings derived from data (Hewlett, 2015). This is a cross-sectional research as different samples are involved, separate in time, and the roles of the research was on identifying new factors or patters in the samples, to explore their effect in South African government departments (Ricttie and Lewis, 2003).

This research was based in two forms, firstly on a national and strategic overview whereby the researcher focused on the available secondary data mainly unpacking the NCPF on a national level. This section is based on the process of implementation as per the proposed plan. The second part is based on the the DTPS. The researcher believes that the DTPS will be the accurate government department as it was given the mandate to implement the NCPF as much as the mandate was later on transferred to the SSA. The researcher focused on the three main responsibilities of the DTPS as mandated by the NCPF namely; the establishment of a Cybersecurity Hub, the rolling out of a Cybersecurity Awareness Programme and to assist sectors in the establishment of Sector CSIRTs.

The researcher mainly asked the how and why questions and to avoid data saturation, the researcher used the literature to narrow the research interests to a

key topic or two, secondly the researcher examined closely a few key studies on the chosen topic of interest and finally identified the questions in those few studies to assess whether they conclude with new questions or loose ends for further research (Yin, 2014). Here the researcher consulted previous academic sources such as books, journal articles as well as scholarly research reports and dissertations.

The researcher made use of semi-structured interviews whereby questions were prepared prior and based on addressing the overall research question. The chosen form of interviews was the personal, one-on-one interviews whereby the researcher interviewed the respondent in the comfort of their office. The researcher, in this instance, asked a set of questions from a questionnaire in the same order, using precisely the same wording and recorded the answers given by the respondent and each respondent was provided (Wagner, et al., 2012).

Before the data could be gathered, the researcher firstly obtained authorisation from the head of institution to conduct the research at the DTPS and thereafter all targeted respondents were approached and requested to participate in the study. The researchers' ethics were highly crucial at this stage as the researcher asked the respondents to participate voluntarily in the study without expecting anything in return. What was promised by the researcher is the confidentiality of the responses should the respondents wish for their responses to be kept confidential as well as the copy of the findings once the research has been completed.

The researcher therefore requested to make use of a boardroom within the DTPS premises. Appointments were arranged prior with all respondents and each appointment was reserved for only 20 minutes. Data collection was reserved for a period of two weeks, after the researcher had left the DTPS premises. The researcher spent the two week at the DTPS premises mainly conducting interviews as well reviewing all DTPS documents which were not reviewed during the literature review stage and thereafter returned to his offices to conduct data analysis. The researcher also made use of a cell phone to make recordings of all interviews, permission to record was requested from the respondents prior to commencing with the interview and the researcher only recoded the interview when permitted by the respondent. The recorded data was used entirely for analysis purposes and was

copied into a memory stick which is safely stored by the researcher. The data kept in the cell phone was deleted and the data kept in the memory stick will be deleted after one year of submission of this report.

After the completion of the literature review and prior to the data collection phase, the researcher had already developed a proposition guided by the literature review. The proposition was that the NCPF has not been effectively implemented as per its intended plans. With this therefore, the researcher tailored the data collection plan in such a manner that it was directed at understanding what barriers are there in the implementation of the NCPF. This proposition was guided by various published authors which have been consulted at the literature review stage as well as by the observations made by the researcher in terms of the growing cybercrimes and related incidents in the previous 10 years, from 2005 to 2015.

3.3 Description of the study area

3.3.1 Sampling

This is a purposive sampling process and the sampling frame was all the employees of the DTPS at the national office based in Pretoria. The reason for the choice of the head offices is that it is where all strategic and policy decisions are made and as such the NCPF was handed to the officials based in that office, these officials are in a better position to have more knowledge regarding the NCPF when compared to those in regional offices. The accessible population, as alluded to prior, was furthermore be scaled down so as to make it possible for the researcher to gather primary data within the required time-frame. The sample size was therefore a total of seven respondents of which only five were interviewed the remaining two was unavailable to participate in the study. The study used semi-structured, one-on-one interview as the method of data collection.

The respondents were chosen from the business units which are working with the implementation of the NCPF namely the Cybersecurity Operations and the Cybersecurity Hub were also interviewed. Although currently stationed at the Cybersecurity Hub, these officials are accountable to the Chief Director:

Cybersecurity Operations who is in turn accountable to the DTPS Director General. These officials were responsible for the establishment of a Cybersecurity Hub, the rolling out of a cybersecurity awareness program, as well as the establishment of a platform of interaction for all stakeholders mandated to implement the NCPF.

The researcher approached all seven respondents who all committed to assisting with the research, only five respondents were available to being interviewed. The two outstanding respondents could not attend the interview on the first week of the data collection due to official commitment. The researcher then made arrangements to return to the offices on the second week of which the researcher attempted unsuccessfully for the entire week to secure appointments with the two outstanding respondents as they had busy schedules. The researcher then requested the respondents to contact him whenever they are available of which they did not. Furthermore, the researcher attempted to contact the respondents on week three, this was also an unsuccessful exercise. The researcher also requested an intervention from the Chief Director: Cybersecurity who was also unsuccessful. With this therefore, the researcher analysed the collected data and drew conclusions as a large proportion of the targeted audience responded to the interviews. Out of a total of seven respondents, five were interviewed and two were unavailable.

A non-probability sampling strategy was used as the “respondents were included in the sample because they are willing and available to participate in the study” (Wagner, et al., 2012). A non-probability sampling strategy was furthermore used as the researcher’s focus was on those departments dealing with the policies and strategy planning and implementation. A purposive sampling method was used. The researcher, in this instance, relied on previous research or ingenuity about the respondents to find participants in such a manner that they can be considered to be representatives of the population and usually uses specific criteria to identify the most suitable individuals (Wagner, et al., 2012). The criteria in this regard were based on their exposure and knowledge of the NCPF.

A snowball sampling method was another method used by the researcher as members of the population were difficult to locate (Wagner, et al., 2012). The researcher in this instance was referred to other members within the DTPS who

were interested in the study and were believed to possibly positively contribute thereto. Initially, the researcher met one official from the Cybersecurity Operations who introduced the researcher to two officials from the same unit. One official from the Cybersecurity Operations, then introduced the researcher to an official at the Cybersecurity Hub who in turn introduced the researcher to three other officials at the Cybersecurity Hub. The total number of respondents was therefore five who were all interviewed by the researcher on a face-to-face basis. Three of these officials are based at the DTPS head offices in Hartfield, Pretoria and the remainder are based at the Cybersecurity Hub which is located at the Council for Scientific and Industrial Research's (CSIR) offices in Pretoria.

3.3.2 Secondary Data

Secondary data is as important as primary data in any given research. As much as this research was based on the collection of primary data, the researcher also relied on secondary data. Secondary data has got the capability of exposing the researcher to the NCPF in its core, its implementation plan, the key stakeholders and role-players, the status of implementation and finally its successes and failures since implementation until recently.

The researcher approached secondary data in various phases. The first phase was to read and critically analyse the NCPF, this was done in an effort aimed at establishing an extensive understanding of the policy framework. Phase 2 involved the reviewing of all key policies in line with the NCPF, all policies listed alongside the policy framework were extensively reviewed, an example is the Cybercrimes and Cyber Security Bill, Electronic Communication Amendment Act, IM Act, POPI Act as well as other policies regarded as closely related to the NCPF.

Phase 3 consisted of the reviewing of all academic sources such as academic journals, books and all publications with a focus on the policy framework which the researcher came into contact with. This phase also consisted of the reviewing of all essential DTPS documents related to the DTPS, both internal and external DTPS documents were reviewed at this stage. Once all the phases were thoroughly undertaken, the researcher compiled a report which focused directly on the chosen

research area and thus provided direction and assistance in the data collection stage.

The researcher chose the secondary data to take this form as the cybersecurity field is fairly new in the South African context and there are therefore very few publications more specifically with the NCPF. The researcher is of the view that the choice of approaching research in this manner will expose the researcher to important data in an orderly form as this will be in a chronological order starting from 2005 to 2015. Most sources referred to in the literature review were able to provide the researcher with an extensive overview which was able to assist in developing the overall research questions as well as the interview questions used during the data gathering phase.

The following questions were used as guidelines when reviewing secondary data:

- What was the status of the SA cyberspace in 2005?
- How has the status of the cyberspace been since 2005 until 2015?
- How vulnerable is the SA cyberspace to cybercrime and all related incidents?
- What policies are in place to safeguard the SA cyberspace?
- What is the scope and focus of the NCPF?
- Who are the key custodians in the NCPF?
- How effective has the NCPF been since implementation?
- Are there any barriers and/or enablers in the implementation of the NCPF?
- What is the status of the SA cybersecurity since the implementation of the NCPF?
- What policies are currently in place at the DTPS in relation to the NCPF?

3.4 Data Analysis

A deductive approach of analysis was used during this research as the researcher was already familiar with the codes and therefore aimed to confirm or explain a phenomenon, based on several cases (Wagner et al., 2012). The researcher used codes which have already been identified from various studies conducted in the chosen research area. These codes have already been gathered during the literature

review stage and therefore were used as key words both in data collection as well as in data analysis. Deductive analysis according to Wagner et al (2012) calls for looking at the study from a general standpoint, then moving to the specific data gathered.

The researcher started conducting data analysis during the data gathering phase as this enabled the researcher to analyse the data as soon as it was received thereby ensuring the accurately thereof. With this practice, the researcher developed growing attention to analysis in proportion to the amount of data being collected and as soon as all the data was collected, the researcher then set aside a period of intensive analysis, this was when tentative findings were substantiated, revised and reconfigured (Merran, 2009). This practice enabled the researcher to have a comprehensive understanding of the data being gathered, it also limited the possibility of an error with regards to the accuracy of the data post analysis.

Thematic analysis is an analysis approach which was used by the researcher. This is an approach which involves identifying themes or patterns in the data with an intention of understanding some phenomenon by looking at how various participants experience the phenomenon (Wagner, et al., 2012) with an intention of answering the research question. The researcher in this instance wanted to understand some phenomenon by studying how various participants experienced a phenomenon and thus address the problem statement (Wagner, et al., 2012).When studying the responses gathered during the data gathering phase, the researcher identified units of analysis which were words, phrases and sentences that were mentioned by the respondents during the interviews, and labelled them with a code. Boyatzis in Wagner et al (2012) stated that a good code has got five elements, namely; a label, a definition of what the code concern, a description of how to know when the code occurred, a description of the qualifications and exclusion to the code and the listing of examples both positive and negative, to avoid confusion.

As soon as the researcher concluded with all interviews, the researcher first transcribed the interview in order to identify units of analysis which can be a word, phrase, sentence or couple of sentences and thereafter identified the topic being discussed or the subject of the unit. The transcribed interviews are presented in

chapter 5 of this research report. As each unit was being read, it was be labelled with a code. Thereafter the code were marked in the margins of a clean A4 paper and also highlighted with different colours, different codes had different colours. As soon as the codes were identified, the researcher then defined all the codes in order to illustrate what would be an appropriate entry for each code (Wagner, et al., 2012). Here, the researcher ensured that all elements of a code were included in a code.

Furthermore, a constant comparison method was also introduced. This was when the researcher compared new pieces of data with previous codes and labelled them with codes identified from the literature review (Wagner, et al., 2012). Once the first interview was concluded, the researcher moved to all interviews in the similar manner. Following this stage, the researcher then grouped the codes into categories of meaning. The researcher ensured that the categories were exclusive and therefore incorporates all key elements in the subject of the study. These categories were tailored in such a manner that they are mutually exclusive in the sense that each unit will be different to another and only fit into one category and thus reflect the same level of abstraction. Finally, these codes were selected in terms of how accurately they address the three overall research questions which guided the study.

3.5 Validity and Reliability

Reliability and validity are two concepts of critical importance in any given research. Reliability estimates the consistency of a measurement and validity involves the degree to which the researcher measures what they are required to measure (Wagner et al., 2012). To keep in tune and to be in line with the research, the researcher applied the concept of validity in research. Once the data was gathered, the researcher compared the findings with the published literature which was reviewed in Chapter to with an intention of either making connections or any disputing factors if they existed, a concept known as content validity.

This was the only element of validity which could be applied by the researcher as there was limited time to study the situation over time. The researcher will however, apply practices such as criterion validity which compares the measurement tool with

the relevant content (Wagner et al., 2012) as well as construct validity which will look at the extent to which the operationalization of the construct taps into actual theories (Wagner et al., 2012). These measures will however be applied at a later stage, as much as the report will be submitted for assessment purposes. The researcher will then arrange follow-up visits to the DTPS wherein a follow-up study will be conducted to first ascertain the effectiveness of the recommendations as well as to assist going forward.

3.6 Risk associated with the study

When planning for the research, the researcher was aware of a number of possible risks which if not planned for might interfere with the entire research process. The researcher pre-empted for the risks and then planned the countermeasures accordingly. The following section will provide an outline of the perceived risks as well as their counter-measures. The researcher in this instance identified four risks which will be associated with this particular study, counter-measures were also provided and as such the researcher planned ahead and therefore was not caught off-guard during the data gathering phase.

There was a possibility of respondents choosing not to participate in the study. To counter this risk, the researcher requests the office of the Director General to send the letter of request to the Chief Director of the targeted business unit. This made it much easier for the researcher when approaching the respondents as an endorsement was already given by the head of the institution and as such the letter of request was filtered down from the highest office in the DTPS. This procedure worked effectively and the researcher was well received and was able to effectively collect data as projected.

When requested by the Chief Director: Cybersecurity to participate in the study, all respondents agreed to assist the researcher, however, in the absence of the Chief Director, only five respondents participated in the study. The two outstanding respondents did not participate as they had busy schedules. The researcher therefore analysed the collected data as a larger proportion of the respondents had participated on the study and therefore conclusions were drawn on the findings gathered. There still exists a possibility that the outstanding respondents might have

provided different information of which might have affected the research findings, the outstanding respondents will be engaged when the researcher submits a copy to the department.

There was a possibility that the target institution only implemented few NCPF proposals as the mandate was later given to SSA and as such the officials could have limited information with regards to the subject area. To avert this risk, the researcher had prior engagements with officials from the SSA structures and they have confirmed that the DTPS plays a critical role in the implementation of the NCPF. There are however, a selected number of officials who are responsible for the functions related to the NCPF, it then became the responsibility of the researcher to ensure that the correct respondents are approached and that they agree to participate in the study.

The possibility of biasness and data saturation which might lead to skewed responses. Biasness was highly possible as the target audiences are from a single organisation and the subject of research is a policy which was at a later stage taken away from the organisation. Data saturation was highly possible as there are only few individuals currently working on the implementation of the NCPF and as such, it was rather challenging to gather data from a handful number of people. The researcher then tried to approach as much respondents as possible.

There was a possibility that respondents might provide incorrect information either deliberately or unintentionally when they were unfamiliar with the subject. To counter this risk, the researcher reserved a period of two weeks to spend in the DTPS for data collection. Ideally, all five respondents were interviewed within one week and as such, the researcher used the remaining week to verify any points of uncertainty and verified conflicting information. The researcher also used this remaining time to meet with those respondents who had more information to provide to the researcher as well as those who had more clarity seeking questions.

3.7 Ethical Considerations

The researcher's aim was to conduct the research in an ethical manner as studies which are not designed with care may unintentionally harm the participants. The researcher, in this instance clearly communicated the methodology, purpose of the

research, and any risk and benefits that may arise for the participants during the research process (Wagner *et al.,* 2012). The researcher established an open and interactive relationship with all respondents thereby ensuring that all uncertainties by the respondents are addressed throughout the research process.

3.7.1 Gatekeeping

First and foremost, the researcher sent a letter requesting to conduct the research to the Director General who then filtered the letter down to the Chief Director: Cybersecurity. In the letter, the researcher fully outlined the purpose of the research, scope of the research, duration of the research as well as what the needs are from the organisation. Once the permission was granted, various Directors of targeted business units were approached. The purpose here was to request the Directors to allow the researcher the space to conduct the research as well as to allow the respondents' time to participate in the study as the data was mainly gathered during official hours unless otherwise requested by a respondent. As soon as the research has been completed and the report has been compiled, the researcher will make the findings available to the Chief Director as well as all people who participated in the study.

3.7.2 Deception

This research is solely academic in nature, with the ultimate goal being the compilation of a research report for the Masters programme. The researcher honestly outlined, to the respondents, the purpose of the research as well as the only benefit of participating in the study which will be to be provided with a research report. The researcher did not make any promises to the respondents as the researcher was fully aware that those promises will never be materialised. The researcher therefore explained to the respondents that the purpose thereof is for the completion of the Masters Degree and therefore the respondents were only assisting the researcher with a motive of adding value to the research report by providing the relevant information.

3.7.3 Informed Consent

The researcher designed an informed consent document which explained to all respondents, the scope, duration, purpose, confidentiality and anonymity of the research, prior to an interview and if accepted, it was signed by the respondents. The researcher only proceeded with the research after the informed consent was signed. If the respondents were dissatisfied with the informed consent and therefore chose not to sign it, the research then could not proceed with the research. The respondents also afforded the respondents an opportunity to add any aspects which deemed necessary for the completion of the research, this was only accepted if it is in line with the research.

3.7.4 Anonymity and confidentiality

When compiling the research report, the researcher did not refer to the respondents in their original names. The respondents were referred to as; Respondent 01, Respondent 02, Respondent 03, Respondent 04 and Respondent 05. During an interview, respondents were afforded an opportunity to introduce themselves, if at any chance, they did not feel comfortable with their names being known, and they were referred to in professional means namely Mam or Sir". As outlined earlier in the proposal, the researcher also utilised cell phone to record the interview. The utilisation thereof depended on how comfortable the respondent was in the process and the recording was only activated after the respondents have introduced themselves.

3.8 Conclusion

This section of the report has outlined in detail how the researcher went about collecting data. This research report clearly unpacked the research methodology, research design and the method of data collection. This research is a qualitative research with semi-structured interviews as the methods of data collection. The researcher chose the qualitative research design as a researcher intended to collecting data through the usage of qualitative methods of data collection. Semi-

structured interviews were used as a method of data collection and as such, the researcher arranged 20minute interviews with the respondents before the actual data gathering stage.

This section then unpacked the sampling frame and strategy followed. The sampling frame for this research is a non-probability sampling frame with a purposive sampling being used as a method of sampling, a snowball sampling method was also used as the researcher also relied on referrals for respondents to interview. The researcher chose this method as the selection of respondents was directed at only those respondents who have either worked with or are currently working with the implementation of the NCPF. Furthermore, the researcher only chose those respondents who were both available and willing to participate in the study without expecting anything in return.

This section also referred to the importance of secondary data, which was seen as of importance as it has the capability of providing background information on the subject are as well as assisting in the formulation of research questions. The reviewing of and consultation of secondary data was approached, by the researcher in various stages as outlined in this report. When reviewing secondary data, the researcher was guided by various questions which provided solid background and narrowed the focus of the reviewing of secondary data.

The researcher then, in this section provided an overview of the method and approach of data analysis. The method of coding was used by the researcher as the method of data analysis. Here information obtained was categorised in various themes and codes of analysis. This was a method which assisted the research in fully analysing the research findings and ultimately in coming up with conclusions and therefore making recommendations which will be communicated to all stakeholders who were involved in the research.

The last part of this section looked into the aspect of reliability and validity which was followed by ethical considerations. The former refers to the researcher's adherence to the research ethical considerations which the researcher ensured that there was strict adherence thereto. With regards to ethical consideration, the researcher adhered strictly to the ethical aspects covered in this section which include gatekeeping, deception, informed consent, and anonymity and confidentiality. Above

all, the researcher at all times, strived to being honest and displayed integrity throughout the research.

CHAPTER 4: THE NATIONAL CYBERSECURITY POLICY FRAMEWORK

4.1 Introduction

Chapter four defines the NCPF as a government owned policy document which recognises that the state is charged with implementing a government led, coherent and integrated cybersecurity approach (State Security Agency, 2012). This section furthermore outlines the scope, purpose, focus and structure of the policy proposal as approved in March 2012. This section outlines the key objectives of the NCPF which includes amongst others, the centralisation of cybersecurity activities through the establishment of relevant structures and policy frameworks in support of cybersecurity.

This section then moves on to explaining the NCPF mandate changes which occurred after the implementation thereof. Thereafter, the report outlines the role of the JCPS cluster with regards to the NCPF in conjunction with government departments, which entails the overseeing of the implementation of the NCPF with the aim of ensuring a centralised approach in coordinating cybersecurity. This role is however made possible with the assistance of SSA as the lead department in the implementation of the policy proposal. This chapter then outlines the structure and component of the policy proposal with the SSA being the lead department and the JCPS cluster playing the oversight role.

This section furthermore outlines the purpose of a dedicated JCPS Cybersecurity Response Centre (CRC) which will be established within the JCPS Cluster with the intension of coordinating cybersecurity activities. This section also makes mention of the Cybersecurity Centre (CSC), Cybersecurity Hub, Electronic Communications Security Computer Security Incident Response Teams (ECS-CSIRT) and other CSIRT establishments in SA. The report then fully explains the roles and responsibilities of the CSIRTs within the South African context as established according to the NCPF with the main objective of outlining the purpose of the policy framework.

This section then outlines the stakeholders involved in the implementation of the NCPF alongside their roles and responsibilities. The role-players outlined are; Department of Justice and Constitutional Development (DoJ&CD), SSA, The South African Police Services (SAPS), DTPS, The Department of Defence and Military Veterans (DoD&MV), The Department of Science and Technology (DoST), the private sector and civil society. It is furthermore stated in this section that, for the effective implementation of the NCPF, all these department should adhere to the proposals as outlined in the NCPF. Although not mentioned alongside these stakeholders, the JCPS is the key role-player who is mandated with the role of overseeing the implementation thereof.

Finally, this section furthermore outlines the key elements involved in the implementation of the NCPF which are closely linked to the 5-C protocol. The factors which will be outlined involved: Political will; Established strictures (Capacity); The reduction of criminal opportunities and the increasing level of difficulties faced by the criminal; To encourage, lead and coordinate the education of professionals in the legal, economic and political arenas (Context and Capacity); The availability of trained staff and other resources (Capacity and Commitment); and a thorough understanding of the cultural and governmental differences (Capacity, Clients and Coalitions). Once all the factors are achieved, it is believed by the researcher that a NCPF can therefore be fully implemented and as such the objectives can be achieved.

4.2 The NCPF

The NCPF promotes a cybersecurity culture and demands compliance with minimum standards, strengthens intelligence collection, investigation, prosecution and judicial processes, it establishes public-private partnerships for national and international action plans, it ensures the protection of national critical information infrastructure and it promotes and ensures a comprehensive legal framework governing cyberspace (State Security Agency, .2012).

The rationale behind the national cybersecurity policy framework is to enable the safekeeping of a nations' constituency and the associated organisational, human, financial, technological and informational resources (Grobler *et al.,* 2007, p.1). With this therefore, the South African government through the DTPS approved the NCPF in 2012. According to the SSA Minister, Mr Mahlobo, SSA, in line with the NCPF, plans to "prioritise the establishment of cybersecurity centres and the repositioning of the current ECS-CSIRT to become a government CSIRT as securing that South Africa will ensure conditions of peace, security and development are enhanced (State Security Agency,2015).

To achieve its objectives, the NCPF will ensure the centralisation of cybersecurity activities through the establishment of relevant structures and policy frameworks in support of cybersecurity; it will foster co-operation between government, private sector and civil society through policy legislation and technology; it will promote international co-operation; it will develop requisite skills, research and develop capacity; it will promote a culture of cybersecurity and will promote compliance with appropriate technical and operational cybersecurity standards (State Security Agency, .2012).

SSA chairs the Cybersecurity Response Committee (CRC), a strategic body responsible for cybersecurity priority setting and overseeing the implementation of the NCPF once established (State Security Agency, 2015). Minister Mahlobo, in the 2015 budget vote speech also informed the general population of plans to strengthen the currently established cybersecurity initiatives such as the ECS-CSIRT. This is by means of making them fully capacitated and readily available to respond to any perceived threat and risk to the cyberspace.

The Systematic Corporation in 2013 published that cybercrime is increasing at a much rapid rate in Africa than in any other area in the world, and as such, expects estimate that 80% of personal computers in Africa are infected with a virus or other malicious software (United Nations, 2014). Africa and in particular South Africa has recently seen an explosive growth in Information and Communication Technology (ICT), making cybercrime to grow at a significant rate. There are, according to Globler *et al* (2007) Limited or inadequate actions and controls to protect computers and networks thereby making Africa a target of attack as well as a medium to attack other parts of the world.

The South African JCPS Cluster has adopted the NCPF as part of its mandate and obligations under Outcome three/Output Seven (Pieterse, 2015). The NCPF is aimed at providing a holistic approach and will be supported by the national cybersecurity plan. It seeks measures aimed at addressing national security threats in terms of cyberspace, at promoting the combating of cybercrime and trust in the secure of ITC; at developing , renewing and updating substation and procedural laws to ensure alignment (Pieterse, 2015). It is furthermore aimed at reducing the cybersecurity threats and risks with the ultimate aim of securing the South African Cyberspace.

According to the Pieterse (2015), the JCPS Cluster in conjunction with government departments is mandated with the function of overseeing the implementation of the NCPF with the aim of ensuring a centralised approach in coordinating cybersecurity measures. The JCPS CRC chaired by SSA, has been established to oversee the implementation of Output Seven also supported by the CSC. To fulfil this obligation, the JCPS cluster established the JCPS implementation plan which was established with the main aim of providing a monitoring plan, with deadlines used to monitor the progress made in the implementation of the goals and objectives as outlined in the NCPF.

The NCPF, according to Otoom and Atoum in Globler *et al* (2007) uses a strategic planning process consisting of the strategic formulation, strategic implementation and evaluation as its main strategy. The elements of the NCPF are; a detailed analysis of the policy strategy in manageable and understandable parts, a manageable structure responsible for the implementation of the strategy, strategic moves designed to achieve the different strategic goals and a set of applicable

strategic controls which should be deployed (Grobler *et al*., 2007). The main responsibilities of all stakeholders within the NCPF are therefore to ensure that the all the strategic elements of the NCPF are fully implemented and thus operational. To ensure the coordination of and effective working relations among all stakeholders, as per the 5-C Protocol.

The NCPF sets out the national cybersecurity proposals outlining the government approach to addressing cybercrimes and related incidents. It is aimed at implementing an all-encompassing approach pertaining to all role-players in relations to cybersecurity. The key strategic objectives of the NCPF are; to facilitate the establishment of relevant structures in support of cybersecurity; to ensure the reduction of cybersecurity threats and vulnerabilities to foster co-operation and coordination between the government and private sector; to promote and strengthen international cooperation on cybersecurity; to build capacity and promote a culture of cybersecurity; and to promote compliance with appropriate technical and operational cybersecurity standards (Grobler *et al*., 2007).

4.3 Structure of the NCPF

Approved in March 2012, the NCPF identifies areas of responsibility by a number of government departments with SSA being the key custodian (Grobler *et al*., 2007). It is worth noting at this point that the JCPS Cluster, in consultation with specific government departments involved in cybersecurity, oversees the implementation of the proposals outlined in the NCPF. According to the NCPF, a dedicated JCPS CRC is established within the JCPS Cluster with the intension of coordinating cybersecurity activities, to drive the implementation of the NCPF and to manage the implementation of Output Seven (State Security Agency, 2012).

Closely linked to the capacity aspect of the 5-C protocol, the role of the CRC is amongst others to ensure the achievement of NCPF policy objectives; to coordinate cybersecurity activities and to be a central point of contact on all cybersecurity matters of national interest; to identify and promote areas of intervention and promote focused attention and guidance where required; to promote, guide and coordinate activities aimed at improving cybersecurity measures by all role players;

and to oversee and guide the functioning of the CSC, Cybersecurity Hub, South African Government ECS-CSIRT and other CSIRT establishments in SA (State Security Agency, 2012).

4.4 Cybersecurity Hub and CSIRT's

The Cybersecurity Hub was established by the DTPS with an intension of establishing a platform of facilitating interaction between key role players involved in cybersecurity. The Cybersecurity Hub is therefore a platform that coordinates the interaction between the JCPS cluster, government departments, private sector and civil societies on matters related to cybersecurity. With regards to the analytical framework, this factor is linked to the clients and coalitions. This is a platform established as per the NCPF, whereby all cybersecurity incidents are reported and interventions by relevant role-players are made to counter all threats and risks against the cyberspace.

The responsibilities of the Cybersecurity Hub, as outlined in the NCPF includes; to coordinate cybersecurity activities in consultation with JCPS CRC as well as stakeholders in the private and public sector; to disseminate relevant information to other sector CSIRTs, vendors, technology experts on cybersecurity; to provide best practice guidance on ICT security for government, businesses and civil society; to initiate cybersecurity awareness campaigns; and to encourage and facilitate the development of appropriate additional sector CSIRT (State Security Agency, 2012).

The CSIRT, according to Grobler *et al* (2007) consists of a team of dedicated information security specialists that prepares for and responds to any information security incident. The CSIRT was established based on the premise that developing countries such as SA do not have proper skills and organisations in relation to cybersecurity incidents and as such, they are vulnerable and a major risk for other countries as well (Grobler *et al.,* 2015). The establishment of the CSIRT in SA is mainly based on the increasing threats and risks against the vulnerable cyberspace. The stakeholders in the CSRITs are fully equipped with the necessary skills required to counter any cyber security threats and risks.

According to Grobler *et al* (2010) a CSIRT consist of a team of dedicated information security specialists and as such when an incident occurs, the members of a CSIRT

can assist its constituency in determining what happened and what actions need to be taken to remedy the situation. The officials can furthermore immediately report any cybercrime incident to law enforcement agents and an investigation can immediately be conducted. As a CSIRT is a 24 hour point of contact whereby cybersecurity incidents can be reported as they occur, all stakeholders mandated to form part of the CSIRT as per the NCPF, are required to be available on an on-going basis and respond to any cybersecurity incident as it occurs.

Figure 1 below consists of general services rendered by a CSIRT in any given country such as SA. According to the table below, the CSIRT consists of both proactive and reactive services. The proactive services mainly consist of services related to the general monitoring of cyberspace and therefore countering any cyber-crime from manifesting. The reactive services are often those which occur after an incident has occurred such as incident response and analysis. The main goal of a CSIRT is the rendering of proactive services.

CSIRT

Reactive services	Proactive services
Alerts and warnings	Announcements
Incident handling	Technology watch
Incident analysis	Security audits or assessments
Incident response on site	Configuration and maintenance of security tools, applications and infrastructures
Incident response support	
Incident response coordination	Development of security tools
Vulnerability handling	Intrusion detection services
Vulnerability analysis	Security-related information dissemination
Vulnerability response	
Vulnerability response coordination	**CSIRT service categories to prevent cyber crime**
Artefact handling	
Artefact analysis	
Artefact response	
Artefact response coordination	

Figure 1: Services rendered by a CSIRT

4.5 Stakeholders in the NCPF

There are various stakeholders which are mandated to form part in the implementation of the NCPF. All stakeholders mandated as per the NCPF play a critical role in the implementation thereof and ultimately the securing of the cyberspace. This section will provide an outline of all such stakeholders.

The DoJ&CD is mandated, as per the NCPF, to lead the implementation process, in consultation with the JCPS cluster for the review and alignment of cyber laws and is required to submit progress reports to the cluster on a continuous basis and in accordance with the JCPS implementation plan (State Security Agency, 2012). Simply stated, its role is to ensure that all laws are aligned with the policy framework and create an integrated cybercrime legal framework and prosecution in the country. Therefore, the DoJ&CD must ensure that all security laws do not overlook the importance of the cyberspace and thus take into consideration the proposals made in line with the NCPF.

SSA is mandated to take the overall responsibility and accountability for the coordination, development and implementation of cybersecurity measures in the country (State Security Agency, 2012). SSA is mandated to ensure that the JCPS cluster is fully capacitated and well able to carry out its duties; to ensure the establishment of the CRC, cybersecurity centres and the proper existence of the CSIRTs; to initiate and lead a process for the development and approval of guidelines and national security norms and standards; and to provide information assurance and secure information and communication technology of importance in support of national security. Simply stated, SSA is the key role-player mandated with the overall implementation of the NCPF, this however, does not give SSA more superiority over other stakeholders as all departments listed in this sections each have got a huge role to play in the effective implementation of the NCPF.

The SAPS, in terms of the NCPF, is responsible for the prevention, investigation, and combating of cybercrime in the country; the roles of SAPS includes; the development of cybercrime policies and strategies; the collaboration with appropriate stakeholders; the development and maintenance of enforcement capabilities and the impartment of basic understanding of cybercrime within SAPS. The SAPS, through the Cybercrimes bill, has the responsibility of developing policies aimed at curbing

and reducing cybercrime. Furthermore, SAPS has the power to make arrest if an individual or institution is alleged to have committed a cybercrime or related incident.

The DTPS is responsible for the development and implementation of policies, regulations and industry standards regarding ICT in general and to assist in the provision of strategic direction and coordination on local and international cybersecurity measures (State Security Agency, 2012). The DTPS is also responsible for the establishment of the National Cybersecurity Advisory Council (NCAC) which is responsible for advising the minister of the Telecommunications and Postal Services on policy and technical issues as well as other matters related to cybersecurity (State Security Agency, 2012). Finally, the DTPS is also responsible for the establishment of the cybersecurity hub as well as the facilitation of any other sector CSIRT. The researcher therefore tested the progress made by the DTPS in terms of its responsibilities in the implementation of the NCPF, this was done in a form of a case study which is reported on in the latter part of the report.

The DoD&MV has the sole responsibility for the coordination, accountability and implementation of cyber defence measures in SA as an integral part of its national defence mandate (State Security Agency, 2012). The DoD&MV furthermore has got the role of border security as per its mandate and therefore, it is also responsible to ensure defensive security in that regard. With that therefore, the DoD&MV is furthermore mandated to establish secure cyber defence measures to protect the South African territory from adversaries from foreign countries, both internationally and regionally. Furthermore, the DoD&MV must be able to advise all stakeholders accordingly should a threat arise specifically from outside the perimeters of the country.

The DoST has the responsibility of the development, coordination and implementation of the national capacity development program, furthermore, it is responsible for developing and facilitating the implementation of the national cybersecurity research and development agenda for South Africa (State Security Agency, 2012). The DoST has got the responsibility of assisting other role-players within the cyberspace in developing innovative cybersecurity hardware and software which will assist in making the South African cyberspace more secure. The role of the DoST is therefore to constantly conduct research and thus provide advisory

service on an on-going basis with an aim of positioning the South African Cyberspace in a more secure space.

The private sector and civil society are also key role players with regards to the NCPF. The former is responsible for the implementation of information security measures which are equivalent to those implemented in government departments. The latter is required to ensure that each and every computer, cell phone or any other device at their disposal connected to an internet is protected by a sufficient malware protection which is fully functional and constantly updated. Furthermore, these role-players also have the responsibility of reporting any cybersecurity incident as it arises to the national CSIRT or any other sector CSIRT. Figure 2 below consist of an organogram outlining the role-players involved in cybersecurity (Grobler *et al*., 2007). This organogram only outline key stakeholders as per the NCPF mandate namely; SSA and DTPS with the JCPS cluster providing an oversight role. This organogram furthermore outlines the structures which these departments mandated to establish in the process of implementing the NCPF.

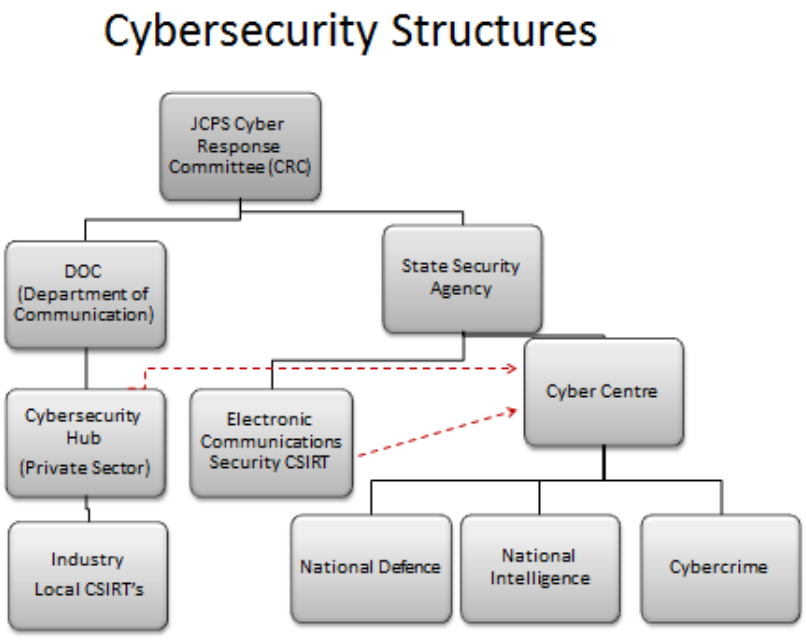

Figure 2: South African Cybersecurity Structure

4.6 Critical Elements in the implementation of the NCPF

Approved in 2012, the NCPF was intended to be implemented according to the JCPS implementation plan. This section of the research report will unpack the key elements required in the implementation of one of the proposals outlined in the NCPF, specifically the Cybersecurity Hub, also known as the CSIRT. In an effort aimed at making the research more researchable and therefore practical, the researcher chose to conduct field work at the DTPS. As per the NCPF, the DTPS is responsible for the implementation of the cybersecurity hub and as such, the researcher, when conducting research focused on analysing whether the DTPS was successful in its goals of establishing a cybersecurity hub and if it was not, the researcher therefore unpacked the barrier in implementation.

This section of the report will therefore unpack some of the elements required in successfully implementing a CSIRT. The 5-C protocol outlined and the following elements will be followed by the researcher when analysing the status of implementation of the NCPF. The results of the research conducted will be outlined in the following chapter.

First and foremost, political will is required when implementing a CSIRT. The national leadership, according to Grobler *et al* (2007) is highly imperative as both an individual and an organisational relationship is required in ensuring the effectiveness of cybersecurity policies. The NCPF is as such aimed at ensuring that various government departments and the private sector participate in ensuring the security of the cyberspace. Senior political leaders as they are the most prominent figures in the leadership of a country such as SA are required to first understand the objectives of any given policy and as such endorse a policy because their assistance is required in all aspects both financially and non-financially.

Secondly, there should be established strictures which should sustain effective cybersecurity solutions for individuals, organisations and government agencies (Grobler *et al*., 2007). A CSIRT can as such be considered the most prominent organisational structure in the coordination of computer networks and information systems. It is also of utmost importance to identify accurate proactive and reactive measures as individuals and groups are highly dependent on data (Grobler *et al*.,

2007). Ghernouti in Grobler *et al* (2007). proposed that cybersecurity actors should be classified in specific roles such as the protector, protected, or the criminal, this will make it much easier to identify any threats thereto and as such, the multiplicity and automation of cybersecurity is becoming more prominent to maximise output and minimise the element of human error.

The third element should be the reduction of criminal opportunities which should be perceived as an effective measure which will be made possible by the effective implementation of the NCPF. The foundation for an adequate security system according to Grobler *et al* (2007) is twofold: to raise the level of risk taken by a criminal as well as to raise the level of difficulties faced by the criminal. The ultimate goal of cybersecurity measures is to ultimately reduce cybercrimes and related incidences, this might take longer to achieve, therefore while working towards achieving the goal, cybersecurity measure must therefore achieve the two objectives listed above.

Organisations, both private and public, should also encourage, lead and coordinate the education of professionals in the legal, economic and political arenas in an effort aimed at strengthening cybersecurity in various aspects. The lack of cybersecurity awareness has been seen as one of the factors which are contributing to the increasing vulnerabilities in the cyberspace. Some of the cyber users fall prey to cybercriminals as they unwillingly give information to cybercriminals which they are often not aware that such information is sensitive and as such it can be used to commit cybercrime. It is therefore of outmost importance that organisations involved in cybersecurity establish programs which will assist in the uplifting and development of the cyber awareness.

The availability of trained staff and other resources is also seen as a key element in the effective implementation of the NCPF. Oftentimes, the activities involved in the NCPF involve professional expertise and as such, it is crucial that that those people involved in these projects possess those skills or are trained immediately after they are hired (Grobler *et al*., 2010). According to Grobler *at al* (2010) excellent IT knowledge and the willingness to learn new things are good characters in the recruitment process with regards to officials who will be implementing the

recommendations as outlined in the NCPF namely the establishment of the cybersecurity hub.

Finally, it is also of importance that all role-players involved in the implementation of the recommendations outlined in the NCPF have a thorough understanding of the cultural and governmental differences within the country as well as among various countries both internationally and regionally. A good understanding of various inter-governmental policies and mandates will give government departments an ability not to overstep other terrains and as such to make a certain department to operate within its mandate. Internationally, it is also of importance to fully understand the governmental difference as “Cultural backgrounds and working environments may differ greatly between different countries” (Grobler *at al.,* 2010).

4.7 Conclusion

The section above has outlined the NCPF in terms of its objectives, structure and purpose as approved in March 2012. This section of the report also outlined the key objectives of the NCPF which included amongst others, the centralisation of cybersecurity activities through the establishment of relevant structures and policy frameworks in support of cybersecurity. Furthermore, this section also defined the NCPF as a government owned policy document which recognises that the state is charged with implementing a government led, coherent and integrated cyber security approach (State Security Agency, 2012).

The research report outlined the NCPF mandate changes which occurred after the implementation in 2012. This section furthermore, outlined SSA as the key custodian of the NCPF, the JCPS cluster as the overseer of the policy framework, the DoJ&CD as mandated to lead in terms of the review and alignment of cyber laws and is required to submit progress reports to the cluster on a continuous basis; SSA is mandated to take the overall responsibility and accountability for the coordination, development and implementation of cybersecurity measures in the country; SAPS is responsible for the prevention, investigation, and combating of cybercrime in the country; the DTPS is responsible for the development and implementation of policies, regulations and industry standards regarding ICT in general; the DoD&MV

has the sole responsibility for the coordination, accountability and implementation of cyber defence; and the DoST has the responsibility of the development, coordination and implementation of the national capacity development program

The private sector and civil society have got the responsibility of abiding to the transcripts as set out in the NCPF. Finally, this section furthermore outlined the key elements involved in the implementation of the NCPF, which involved among others, political will, trained officials etc. A conclusion was therefore drawn by the researcher that these key elements are required in order for the NCPF to be effectively implemented as the absence of any of the factors can lead to the policy not being effectively implemented.

CHAPTER 5: DATA PRESENTATION AND ANALYSIS

5.1 Introduction

Chapter 5 of this report focuses on providing a presentation and an analysis of the data gathered by the researcher during the data gathering phase. This chapter is divided into two sections. The first section provides a presentation of the transcription of the raw data gathered during the data collection phase, this section provides the transcribed responses given by respondents during the data gathering phase with no analysis conducted by the researcher. The researcher only transcribed the raw data so as it make it easier to read without making changes to the actual responses provided by the respondents. During the note taking-practice, the researcher was constrained by the short-ness of time and attention as the main attention was on the conducting the actual interview and as such the notes were fragmentary, incomplete and cryptic (Yin, 2011). This therefore necessitated the need to revise the field notes to convert them into a more formal set of notes which are included into the research report.

The transcribed responses gathered during the data gathering sessions are presented in three groups thereby addressing the three overall research questions. These responses are categorised in terms of the three overall research questions namely; To what extent were the objectives of the NCPF attained since implementation? What key factors strengthen or impede policy outputs and impacts? What measures should be put in place to ensure the effective implementation of the NCPF? In presenting the findings, the researcher provides a feedback of the responses provided by respondents to all questions which were posed by the researcher. Responses are presented under the relevant research question and as such are presented in a sequence from the first respondent to the last one. To emphasise its responsibilities, the DTPS was only mandated to implement cybersecurity measures outlined on the NCPF namely; the establishment of a Cybersecurity Hub, the rolling-out of a Cybersecurity Awareness Programme, and to assist in the establishment of Sector CSIRTs.

As soon as the responses are presented, the researcher then provides an analysis of these responses with an intension of addressing the problem statement as well as answering the three overall research questions. When conducting data analysis, the researcher followed a deductive approach of analysis as the researcher was already familiar with the codes and therefore aimed to confirm or explain a phenomenon. The researcher used codes which have already been identified from various studies conducted in the chosen research area. These codes have already been identified during the literature review and therefore were used as key words in the data collection stage. Unlike the presentation of the findings which is divided into three segments, data analysis will only be presented into one segment, namely, the barriers in the implementation of the NCPF. This is as the main purpose of this study was to fully uncover the barrier in implementation of the NCPF.

5.2 Data Presentation

- To what extent were the NCPF objectives allocated to the DTPS attained since implementation?

In addressing the first research question, **Respondent 01** first defined the NCPF as a policy document which provides guidance to legislatives in the South African cybersecurity domain. The objectives of the NCPF which were allocated to the DTPS, according to Respondent 01 were the establishment of the Cybersecurity Hub, the establishment of the CSIRT and various Sector CSIRTs, the establishment and operationalization of the Cybersecurity Centres as well as the rolling out of the cybersecurity awareness program. Respondent 01 stated that the CSIRT is established, however the end goal is a fully functional CSIRT which is currently being developed. According to Respondent 01, most NCPF objectives have been achieved and there are currently attempts being made by the DTPS to achieve the remainder.

Respondent 02 stated that the NCPF is a policy which intends to bridge the gap that currently exists and to deal with duplications of similar functions in various government department. The NCPF according to Respondent 02, is aimed at establishing a single policy which will have a by-in from all stakeholders. The role of the DTPS according to Responder 02 is to deal with softer issued rather than the

hard issues in IT Security and furthermore the NCPF is one policy which covers all role-players in the cybersecurity environment. The objectives of the NCPF have not been fully achieved according to Respondent 02. Although established, the Cybersecurity Hub was delayed due to financial constrains which is still a problem as the Cybersecurity Hub is unable to being a one stop cybersecurity contact centre as there are limited funds.

According to Respondent 02, the rolling out of a cybersecurity awareness programme is currently underway and the DTPS is working closely with the GCIS. There are already cybersecurity electronic billboards erected on major highways in and around Pretoria, there is also a brochure which has been distributed to the public, this brochure is designed to cater for different audiences, there is one for young people and another for the elderly. As much as these cybersecurity initiatives have been implemented, the impact is currently not seen, this according to Respondent 02 is because the cybersecurity concept is an international concept which is relatively new in SA and therefore only known by limited individuals.

Respondent 03 defined the NCPF as a policy framework that sets out how SA should deal with cybersecurity matters, it is an all-encompassing policy document which includes the economy, social security and cybersecurity as a whole. The NCPF according to Respondent 03, mandated the DTPS to establish a Cybersecurity Hub which is a platform to pull together the public and private sectors in information security. According to Respondent 03, the coordination of all stakeholders in the cybersecurity environment is not yet done, what has been achieve however, is the establishment of the Cybersecurity Hub which is currently operational. The second responsibility of the DTPS is to roll out a cybersecurity awareness program, this is currently been done by the department. The awareness program therefore engages the public in cybersecurity matters.

According to Respondent 03, there has also been an establishment of and installation of electronic billboards which are currently up in major roads in Pretoria. Furthermore, there is also a cybersecurity brochure which has been printed and distributed to the general public. According to Respondent 03, the objectives of the

NCPF have been preliminarily achieved, there is however more work to be done to ensure the full implementation.

According to **Respondent 04**, the NCPF is a strategy document which foresters or classifies the roles which should be played by government departments in cybersecurity. The NCPF according to Respondent 04, sets a roadmap of the country on securing the cyberspace. Respondent 04, informed that they are more advanced as compared to other government departments in the implementation of the NCPF, this is with regards to the establishment and operationalizing of the Cybersecurity Hub. Although the objectives of the NCPF have not been fully implemented, Respondent 04 believes that the DTPS has achieved a 30% implementation of the objectives of the NCPF.

Respondent 04 also stated that that there are various other structures within the DTPS who are assisting in the implementation of the NCPF objectives namely; the Legal department assist in the establishment of IT disclaimers, the Human Resources department assist in the recruitment of personnel, the Supply Chain Management department assist in the procurement of equipment's. The CSIR as a sister department of the DTPS which has also been mandated by the NCPF is also assisting in the implementation of the NCPF, according to Respondent 04. The CSIR has deployed two officials in the Cybersecurity Hub which are assisting in providing technical knowledge.

Respondent 05, defined the NCPF as a policy document which facilitates the formation of a curriculum which deals with the establishment and operationalization of the CSIRTs. According to Respondent 05, it also compels the Department of Education (DoE) to develop a cybersecurity curriculum with assistance from the DTPS which will be rolled out to the general public. Respondent 05 informed that the DTPS's Gender and Disability Unit has developed a policy on online child protection which aims to protect children against cybercrime. This Unit has conducted awareness briefings in various schools and has partnered with Google and the film and publication board (FPB). NEMISA, an intermediary of the DTPS has been established to assist in the development of technical skills and knowledge in rural communities throughout the country, it has partnered with GCIS.

According to Respondent 05, there has also been a distribution of cybersecurity awareness booklets which has been given to the general public. It was also stated by Respondent 05 that a lot has been done with regards to cybersecurity awareness, due to political restrictions and mandate changes, there is however, some objectives which could not be implemented. Finally, Respondent 05 informed that the NCPF is not clear on the responsibilities of role-players as well as the time-frames wherein the objectives should be met. It is therefore hard to determine whether or not the objectives were met.

- What key factors strengthen or impede policy outputs and impacts in the DTPS?

With regards to the factors impeding the implementation of the NCPF, **Respondent 01** stated that, although the Cybersecurity Hub was established 09 months ago, there is currently a shortage in the skills required to operate a fully functional Cybersecurity Hub. Secondly, Respondent 01 also stated that the Cybersecurity concept is a cross border phenomenon and therefore it is rather challenging for the DTPS to achieve the set objectives as there is no communication with international cybersecurity players. With regards to the factors which strengthen the implementation, Respondent 01 alluded to the growing interest in the cybersecurity space which has had a positive impact in terms of people adhering to the cybersecurity measures communicated by the DTPS.

Respondent 02 stated that the factors strengthening the implementation of the NCPF in the DTPS is due to there being good working relations among stakeholders mandated by the NCPF and therefore a common understanding by all players. Furthermore, Respondent 02 stated that the DTPS has established working relations with the European Council (EU) in terms of the development of cybersecurity skills by the EU to South African government departments. Respondent 02 also mentioned that the relations which currently exist between SA and various African states in namely the AU and the South African Development Community (SADC) regions have assisted in the implementation of the NCPF. What is impeding the implementation for the NCPF, according to Respondent 02 is the lack of understanding of cybersecurity by the general population, the lack of cybersecurity

skill in SA as a whole has resulted in the department not moving at a desired pace, and finally the lack of funding is also regarded as a major impeding factor.

When looking at the factors impeding and strengthening the implementation of the NCPF, **Respondent 03** stated that it is hard to determine the progress made in the implementation as there is no transparency among stakeholders mandated by the NCPF, such organisations are not working together as required, the Cybersecurity Hub is supposed to be a platform that such interaction takes place, however, it is currently not being utilised. Respondent 03 furthermore stated that sensitive information is often being given to irrelevant people often through a telephone or email which is also vulnerable to cybercrime. Finally, Respondent 03 stated that the current protocols which are followed in decision making often makes it impossible to proactively respond to a cyber-threats. Respondent 03 however, stated that relevant parties to provide accurate responses are those in operational structures and therefore since Respondent 03 is not employed as a cybersecurity operative, he was unable to provide a response.

Respondent 04 stated that the factors which strengthen the implementation of the NCPF is the research conducted by the CSIR which has provided guidance in the governance framework by identifying the international best practices and aligning then to the specific need of the country and then providing advice to the DTPS. With regards to factors impeding the implementation of the NCPF, Respondent 04 stated that there is a lack of support from other stakeholders mandated by the NCPF, there are currently few officials employed at the Cybersecurity Hub who are expected to service the entire country and finally, there has been a lot of criticism against officials employed at the Cybersecurity Hub and this has negatively affected the staff deployed at the Hub.

When responding to the question on the factors impeding the implementation of the NCPF, **Respondent 05** stated that there has recently been conflict between the Cybersecurity Hub and the Directorate for Priority Crime Investigation Unit also known as the HAWKS who have criticised the DTPS of interfering with evidence when analysing information received informing of a cybercrime, this according to Respondent 04 has had a negative impact as officials in the Hub ended up being

uncertain of their roles and responsibilities as mandated by the NCPF. Secondly, Respondent 04 stated that the competition in various sector; namely banks, has affected the establishment of Sector CSIRT as there was a lack of a Memorandum of Understanding (MoU) with regards to the sharing of information in a Sector CSIRT.

Respondent 05 furthermore stated that there is currently a problem with regards to whose responsibility it is to monitor the State Information Technology Agency (SITA) as the SSA is mandated thereto however, it is not carrying out the function. Furthermore, Respondent 05 stated that there are no working relations among stakeholders highlighted in the NCPF. Respondent 05 also believes that the support from the Minister of the DTPS has greatly assisted in the implementation of some of the objectives of the NCPF, such as in the establishment of the Cybersecurity Hub.

- What measures should be put in place by the DTPS to ensure the effective implementation of the NCPF?

When requested to recommend measure to be put in place in assisting in the implementation of the NCPF, **Respondent 01** stated that a cybersecurity skills development programme should be developed within the framework of the Sector Education and Training Authorities (SETA), SETA's should in this instance be approached to prepare standardised cybersecurity approaches in courses which will be attended by both the public and private sectors. Respondent 01 also recommended that minimum standards for the cybersecurity space should be jointly established by all role-players in the cybersecurity space so as to create an enabling environment. Furthermore, Respondent 01 recommended that more cybersecurity awareness should be done to the public in educating them about cybersecurity. Finally, Respondent 01 stated that the NCPF involved all relevant stakeholders.

When asked to make recommendations on measures to be implemented in ensuring the effective implementation of the NCPF, **Respondent 02** stated that more officials should be employed at the Cybersecurity Hub as there is currently 03 officials appointed. Respondent 02 also recommended that more funds must be allocated to activities working on the implementation of the NCPF. Respondent 02 recommended that the Cybersecurity Hub should either be moved to a much bigger space or the

current space be extended as they are the only Hub servicing the entire country which is currently occupying a small space.

Respondent 02 recommended that the DTPS should build relations with various regional and international counter-parts thereby establishing cross-border relations as cyberspace is borderless. Furthermore, Responder 02 recommended that the officials working at the forefront must have an extensive understanding of cybersecurity and thus improve on the current communication with stakeholders in the NCPF. Respondent 02 also highlighted the importance of the involvement of the private sector in the implementation of the NCPF also more specifically in the rolling out of the Sector CSIRTs. Additionally, Respondent 04 recommended that a programme should be established to train 'Cyber Police' whose responsibility will be the policing of the cyberspace, these positions should be occupied by the unemployed graduates. Finally, Respondent 04 recommended that SA should consider producing its own IT equipments rather than importing, this is as there is a possibility of the imported equipment's to be bugged even though we secure them.

In providing recommendations to assist in the effective implementation of the NCPF, **Respondent 03** stated that there must be more funding allocated to the implementation of the NCPF, furthermore, Respondent 03 stated that there must be programs in place to provide cybersecurity training to officials mandated to implement the NCPF. Finally, Respondent 03 recommended that there must be a single Cybersecurity Hub established wherein officials from all stakeholders will be deployed, the permanent deployment of officials from different departments will enable the Cybersecurity Hub to promptly respond to an incident as there will be an immediate analysis and dissemination of information.

When requested to provide recommendations in the effective implementation of the NCPF, **Respondent 04** stated that all stakeholders mandated to ensure the implementation should work together despite their differences and the JCPS cluster should be more involved in operational matter as they currently are not involved. Respondent 04 stated that the management must be trained on cybersecurity matters so as for them to have an understanding of the core function. Respondent 04 recommended that SITA should be contacted to provide IT security infrastructure

and furthermore be involved in the overall implementation of the NCPF. Respondent 04 thus recommended that more cybersecurity awareness programmes must be rolled out so as to educate the general population on cybersecurity measures such as the secure use of the cyberspace. Finally, Respondent 04 stated that the Department of Agriculture and Forestry should have been included in the NCPF as it has the capability of communicating with rural communities across the country.

As a recommendation in the effective implementation of the NCPF, **Respondent 05** stated that the cybercrimes bill should urgently be passed in parliament and thus be enforced so as to act on cybercriminals. Respondent 03 thus recommended that all departments with overlapping mandates should develop a MoU which will deal with the mandate clashes as well as creating an effective environment to carry out the duties and thus establish a working manual with responsibilities which must be approved by heads of departments. Respondent 05 could not provide more recommendations in the effective implementation of the NCPF as it is believed by Respondent 05 that the implementation depend on a huge number of factors some of which have been addressed in preceding questions.

5.3 Data Analysis: Barriers in the implementations of the NCPF

Thematic analysis is a general approach to analysing qualitative data which involves these or patterns derived from the raw data (Wagner et al., 2012).Thematic analysis was applied in this research as the researcher intended assessing the status of implementation of the NCPF by means of interviewing various individuals in the DTPS. Following data collection, the researcher transcribed the interviews and thereafter identified units of analysis which were thereafter labelled with a code. The codes identified will be presented in the section below and will be integrated in the relevant sections.

A total of five officials employed by the DTPS were interviewed by the researcher when conducting research on the barriers of implementation of the NCPF. Prior to the collection of the data, the researcher conducted a literature review whereby various academic sources including books and journals, policies and regulations, acts of parliament and various cybersecurity-related documents were consulted. This

was done with an intension of first establishing a solid understanding of the NCPF in terms of its goals and objectives, its stakeholders, the status of implementation, its effectiveness or lack thereof, and finally the barriers of implementation. During this exercise, the researcher uncovered that the NCPF was not effectively implemented as projected when approved in 2002. With that therefore, the researcher then conducted this study with an intension of uncovering the reasons why the NCPF has not been effectively implemented as projected and to thus make recommendations which will be communicated to all relevant stakeholders in the NCPF.

All respondents interviewed agreed that the DTPS has moderately achieved its obligations in terms of implementing the objectives of the NCPF. Respondent 01 mentioned that the Cybersecurity Hub has been established, however the end goal is a fully functional National CSIRT which is currently being established. Respondent 02 stated that, although established, the Cybersecurity Hub was established late due to financial constraints. Respondent 03 on the other hand stated that as much as the Hub is active and fully functional, it is not serving its core function, which is the contact 24-hour point of contact for all role-players as mandated by the NCPF, this is however disputed by Respondents 04 and 05 who state that the Hub is constantly used by other stakeholders, there however tends to be clashed in terms the responsibilities with some stakeholders often criticising officials at the Hub of tampering with evidence often when sensitive information is reported. The codes identified were the lack of coordination and cooperation by stakeholders.

Another DTPS responsibility is the rolling-out of a cybersecurity awareness programme as per the objectives of the NCPF. This is according to Respondents 01, 02, 03 and 05 was achieved as there is currently a cybersecurity awareness program being rolled out by the DTPS. The code identified was commitment by DTPS officials. Respondent 01 stated that the cybersecurity awareness program is an on-going program which has already been launched by the department. Respondent 02 on the other hand stated that there has been electronic billboards erected on major highways in and around Pretoria, there is also a brochure which has been distributed to the public. Respondent 03 concurred with Respondent 02 and furthermore made mention of the electronic billboard as well as the awareness booklet which are currently being rolled out.

In addition to this, Respondent 05 also mentioned the role played by the DTPS's Gender and Disability Unit, this unit has developed a policy on online child protection which is entirely aimed at the protection of children against cybercrime. This Unit has conducted awareness briefings in various schools and has furthermore partnered with Google and the FPB. Respondent 05 furthermore mentioned the role played by NEMISA in partnership with the Government Communication Information Services (GCIS) in terms of the development of technical skills and knowledge in rural communities throughout the country. When compared to other role players, Respondent 04 believes that the DTPS has achieved most of the objectives set, according to Respondent 04, the DTPS has achieved approximately 30% of the objectives as out lined on the NCPF.

As much as the DTPS has implemented the objectives of the NCPF which were their responsibility, their impact is not yet seen in the country at large due the late rolling out of a cybersecurity awareness programme as stated by Respondent 02. Although established, this awareness programme does not cater to all individuals in the country as it is not designed in all South African official languages. Code derived from this data is that of a lack of understanding by some officials and also a lack of resources to roll-out a successful cybersecurity awareness programme. This factor was also mentioned by Grobler *et al* (2007) as they stated that the absence of African languages has a direct impact on the vulnerability of the African cyberspace due to a lack of cognizance, this is as computer users often willing to learn about cyberspace are restricted to do this, because African languages are used minimally in cyberspace. Once such individuals have an exposure to cyberspace, they tend to be vulnerable as they often display sensitive information which adversaries may use to commit cybercrime.

The shortage of skilled cybersecurity officials is one of the major factors currently acting as barriers in the implementation of the NCPF objectives and more specifically, the establishment of the Cybersecurity Hub. A Code in this regard is the shortage of skills. Respondent 01 outlined the shortage of skills as a major problem that the DTPS is currently confronted with, this aspect was furthermore emphasised by Respondent 02 who in turn stated that the lack of cybersecurity skills in SA as a

whole has resulted in the DTPS not moving at a desired pace as projected when implementing the NCPF. This factor was also highlighted by Van Nieuwkerk in chapter 02. Van Nieuwkerk (2015) believes though these laws exist, their effectiveness has diminished overtime due to the insufficient training given to stakeholders entrusted with the implementation responsibility. What is therefore required in this instance is to either amend the act or to formulate a policy which supports the actual implementation of the Acts outlined.

The time-delay between policy development and implementation is also seen as one of the factors negatively affecting the implementation of the NCPF. This was also made evident with the delayed establishment of the Cybersecurity Hub, the code derived in this regard was a lack of accountability. The time-delay can be attributed to a number of factors one of them being mandate changes, as the NCPF implementation mandate was initially, in March 2012, given to SSA and then later in 2012 given to the DTPS (Globler, et al., 2007), the same mandate was later on given back to SSA. Additionally, political interference was also identified as a code in this regard. This then resulted to the delay in the policy implementation. Currently the main custodian entrusted with the overall implementation of the NCPF is the SSA who is accountable to the JCPS cluster. This is not the true case in reality as the main point of contact for cybersecurity operations is the Cybersecurity Hub which currently has officials from the DTPS and the CSIR who all report to the Minister of the DTPS who is in turn accountable to the JCPS Cluster.

Sensitive information received in the Cybersecurity Hub is currently unsecure and there are possible vulnerabilities which adversaries can utilise as weak points when attempting to commit cybercrime. All officials deployed at the Hub are not vetted and therefore not security cleared by SSA; all officials deployed in the Hub are not trained in the secure handling of SA’s sensitive information in factors such as information classification, information control, information storage and information destruction; And there is currently no official from the security cluster deployed at the Hub or in constant communication with the Hub to provide direction in the secure protection of sensitive information as per the South African legislations. The code identified by the researcher in this regard is security deficiencies.

Respondent 03 cited the lack of coordination by stakeholders as a major problem in implementing the NCPF objectives. This factor was emphasised by Respondent 04 who stated that there is a lack of support from other stakeholders mandated by the NCPF. Respondent 05 concurred with both these respondents and also cited the lack of stakeholder coordination as a major factor which is negatively affecting the achievement of the NCPF goals and objectives. Although mandated to work jointly in achieving a secure cyberspace and thus fully implement the objectives of the NCPF, various stakeholders are currently not working together with a common purpose thereby not sharing the necessary information which might positively assisting in both implementing the NCFP as well as in establishing a safe and secure cyberspace.

Due to its global nature, it is believed by Respondent 02 that cybersecurity is an international concept which is relatively new in SA and therefore only known by limited individuals. There is therefore very little research in the subject area and as such, Herselman, *et al* (2010, p.256) proposed that more research needs to be conducted in terms of how badly South African companies are affected by cybercrime and whether the newly promulgated laws will be effective in combating cybercrime. A code derived from this was a lack of prioritisation by the South African government. The limited nature of this research has resulted in there being insufficient cybersecurity awareness measures readily available which can be applied by various individuals, private companies as well as government departments. Furthermore, due to the borderless nature of the cyberspace, SA thus relies on various countries both regionally and internationally to strengthen its cybersecurity as well as to effectively implement the NCPF.

5.4 Conclusion

This chapter focused entirely on the presentation of the data gathered as well as the analysis thereof. This data was gathered at the DTPS and a total of five officials were interviewed. The researcher conducted one-on-one semi-structure interviews with questions pre-determined prior to an interview. Where necessary, the researcher asked probing questions which were in relation to the study. This section

was aimed at presenting the findings gathered by the researcher in two forms, firstly by means of providing a transcription of the data gathered as well as by providing an analysis of the responses gathered by the researcher.

The first part of this chapter provides a transcription of the findings gathered during the data collection stage. Here, the researcher transcribed the responses provided by the respondents with an intension on re-writing the responses without changing the meaning conveyed. The presentation of the findings is divided into three parts based on the three overall research questions which guided the study namely; To what extent were the objectives of the NCPF attained since implementation? What key factors strengthen or impede policy outputs and impacts? What measures should be put in place to ensure the effective implementation of the NCPF? The responses to these questions were provided under a question in a sequence from the first to the last respondent.

The second part of this chapter focused on the actual data analysis. This section however, focused on the main focus point of this research which is on understanding the barriers of implementation. The researcher in the section analysed all responses gathered with an intension of understanding how the respondents understand the implementation of the NCPF recommendations as well as on the barriers which the respondents believe are affecting the implementation of the highlighted cybersecurity measures as outlined in the NCPF. As per the responses gathered, the DTPS is far ahead when compared to other stakeholders with regards to the implementation of the NCPF. The objectives allocated to the DTPS namely; the establishment of a Cybersecurity Centre, the rolling out of a cybersecurity awareness program and to assist in the establishment of sector CSIRTs have been primarily achieved according to all respondents interviewed.

Based on the responses gathered and various sources consulted during the literature reviews, it is believed by the researcher that the DTPS has performed significant in implementing the NCPF objectives allocated to them as compared to various other stakeholders, there are however various barriers which are currently affecting the effective implementation of the entire objectives as the effective implementation is largely dependent on a number of factors such as stockholders

coordination, international and regional inter-relations as well as the understanding by the target audience.

Based on the data collected and the literature reviewed, it can be concluded that the key barriers in the implementation of the NCPF are not only within the DTPS but rather on the coordination of all key stakeholders as outlined on the NCPF, this is as there is currently no coordination of such role-players in the cybersecurity hub which was developed to be a 24 hour central point of contact which is currently not being utilised as such. Furthermore, the shortage of skills was seen to have featured prominently as a problem which is currently facing the DTPS and as such, acting as a key barrier in the implementation of the NCPF. The next chapter will focus on the conclusions made by the researcher based on the entire research conducted, the conclusions will then be followed by a number of recommendations which will be communicated to all key stakeholders mandated by the NCPF.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

As a concluding chapter, this chapter is based on outlining the conclusions made by the researcher based on the data gathered throughout the entire research. This chapter is divided into two sections, section one outlines the conclusions drawn by the researcher based on the entire research conducted and the second section provides recommended measures which the researcher believes can assist in the effective implementation of the NCPF objectives by relevant stakeholders. The researcher believes that there is a total of eight barriers which are affecting the implementation of the NCPF.

Most of these barriers are within the DTPS, however, some are those barriers which are across-sector whereby more than one stakeholder is affected by a single barrier. The barriers outlined are amongst others; the lack of trained cybersecurity officials, the lack of funding for cybersecurity projects, the lack of coordination by NCPF stakeholders and the lack of security cleared officials in the Cybersecurity Hub who are also trained on the secure handling on the states' sensitive information. As much as these barriers were uncovered during a research which was conducted at the DTPS, a possibility arises that there are some stakeholders with similar challenges.

To counter the barriers identified, the researcher formulated recommendations which are believed to be effective measures aimed at addressing the identified barriers. Included in the proposed recommendations is the rolling out of a skills development program by the DTPS, to establish a more intensified cybersecurity awareness programme, to ensure a more coordinated and well managed Cybersecurity Hub, to involve the Department of International Relations and Cooperation (DIRCO) to assist in the establishment of international and regional relations with regards to cybersecurity and to ensure that security cluster officials play a vital role specifically in the Cybersecurity Hub as they are trained on the security of the country. As a point of departure, the conclusions by the researcher are outlined.

6.2 Conclusions made by the Researcher

As much as some officials interviewed believed that there is generally support from their management in particular the Minister of the DTPS, and as a result most projects are successfully executed. There are however, some officials within the organisation who believe that there are elements of favouritism which are largely affecting the organisation, this is as there are some projects which tend to be given more preference over other projects often with the same level of importance, urgency and amount of funds required. Although this factor cannot be used to draw conclusions with regards to various other projects within the DTPS due to the small number of the respondent, the selected sample is only effective in terms of drawing conclusions with regards to the implementation of the NCPF as all the respondents interviewed are either currently working with or have previously worked with the implementation of the NCPF.

Based on the research conducted, it can be concluded that the objectives of the NCPF are not implemented as projected when it was approved in 2012. This therefore means that there exist barriers in the implementation of the NCPF. Based on the research conducted, it is believed by the researcher that there is a total of eight barriers which are largely affecting the implementation of the NCPF. The barriers identifies are not solely within the DTPS as they are similar among most stakeholders identified within the NCPF. Some barriers are believed by the researcher, to be overlapping inter-departmentally as various government departments are dependent on each other for the implementation of the NCPF. As per the 5-C Protocol, it emerged that all respondents interviewed are committed to fulfilling their official obligations, the factors which are acting as barriers are administrative and operational.

Based on the data gathered, it has emerged that there is no common understanding of the NCPF in terms of its definition, purpose, scope and objectives. The respondents interviewed had differing views with regards to the actual definition of the NCPF. The purposes, scope and objectives of the NCPF was largely different among all respondents. Furthermore, as much as most stakeholders believed that key role-payers were included in the NCPF, there were some stakeholders who

believed that some critical stakeholders were excluded thereto such as the Department of Agriculture which has the capacity to communicate with the rural community. With this therefore, it can be concluded that there is generally no common understanding of the NCPF by the main officials tasked with the implementation responsibility within the NCPF. The officials interviewed do not understand the definition of the NCPF, its goals and objective, its stakeholders and finally its purpose. It is highly important that there is a common understanding of a policies in any given organisation, this factor is furthermore emphasised in the 5-C Protocol as Cloete *et al (*2000) postulate that the content of any policy is highly crucial not only in the means it employs to achieving its ends, but also in its determination of the ends themself and also in how it chooses the specific means to reach the ends.

The lack of skilled cybersecurity operatives was seen to be one of the main problems currently facing the DTPS which has acted as one of the barriers in the implementation of the NCPF. Although established, there are currently few trained cybersecurity officials deployed at the hub. The majority of officials currently employed are specialists in various other fields and were pulled in to assist in the Hub with the provision of the strategic direction, there is currently a shortage of skilled technical operators in the DTPS as well as in various other stakeholders outlined in the NCPF. This shortage of skills has led to some stakeholders either implementing the objectives late or not implementing them at all. This factor can be linked to the 5-C protocol, more specifically the capacity factor which according to Globler *et al* (2010) relates to human and technical resources which play a key role in the policy implementation process. The absence of these factors can result to a policy not being effectively implemented.

The implementation of the cybersecurity initiatives is a highly expensive excise which requires huge amounts of funds from the government. There has recently been a shortage of such funds in the DTPS and as such the implementation of most of the NCPF objectives has been delayed. This was evident with the delayed establishment of the Cybersecurity Hub as well as the delayed rolling out of the Cybersecurity Awareness Program. Furthermore, the shortage of skills is also negatively affecting the employment of skilled cybersecurity officials as such officials are often being

provided with higher salaries by the private sector, it is therefore highly challenging for government departments to provide competitive salaries for trained cybersecurity officials to convince them to join government departments. This factor refers to challenges in the institutional context as per the 5-Protocol. (Cloete et *al* (2000) postulate that the institutional context is the larger context of the social, economic, political and legal realities in any given organisation.

The DTPS which was chosen as a case study for this research has started with the implementation of the NCPF. This has been evident with the rolling out of a cybersecurity awareness program which includes the construction of digital billboards along major roads in Pretoria as well as the printing and distribution of information broachers to various communities. This awareness program has been successfully rolled out by the DTPS and has been spread to selected communities in the Gauteng Province. The impact of this awareness program is however not yet seen in the country at large, a number of factors can been attributed to this namely; the awareness programmes are not aggressive enough to be known by every citizen of the country, the messages are only communicated in English thereby no catering for local South African Languages and as such leaving out a high number of individuals, information brouchers are only distributed to a selected number of people and communities, billboards are in certain areas of Pretoria thereby only visible to local people and only people driving by and therefore excluding a high proportion of South Africans.

The Cybersecurity Hub as one of the NCPF objectives has been established and activated. It currently has a total of two officials deployed with two managers who report to the Chief Director: Cybersecurity at the DTPS. One official at the Hub is from the CSIR and is deployed at the Hub to provide technical assistance. There have recently been three interns recruited to provide assistance. As much as it is fully functional, there are a number of deficiencies identified. All officials stationed at the Hub are not vetted and therefore not security cleared by SSA and yet they handle sensitive state information, officials deployed at the Hub have not been trained on the secure handling of the states' sensitive information, the interns are exposed to sensitive information however they are not security cleared by the SSA,

and finally there are currently no officials from the security cluster deployed at the Hub to provide direction on information security.

Although established as the 24 hour point of contact for all stakeholders to report cybersecurity incidents as well as to proactively react to cyber-treats as they emerge, the cybersecurity Hub is currently not being utilised as such by stakeholders. Cybersecurity stakeholders currently do not work together as outlined in the NCPF, there is currently no sharing of information as is supposed to be happening in the Hub. Furthermore, there are often clashes of mandates with regards to sensitive information, this has been evident with regards to whose responsibility it is to handle sensitive information between the SSA, the HAWKS or the DTPS as the officials mandated to manage the Hub which is the point of reporting cybersecurity incidents. This confusion has therefore led to some organisations working in isolations and thereby individually attending to their own cybersecurity challenges as they emerge. According to the 5-C Protocol during the policy development phase, policy developers should at all times consider the interests of the policy end-user (Cloete *et al.,* 2000). The lack of interactions in the Cybersecurity Hub confirms that there is a lack of solid relations among clients and coalitions where ought to be strengthened prior to the implementation of the NCPF.

Also closely related to the above factor is the late implementation of the NCPF which was affected in part by the mandated changes which led to the implementation mandated being initially given to the DTPS in 2012 then later on handed over to SSA with not reasons communicated to the officials in the DTPS. The mandate changes have negatively affected policy implementation with some objectives being implemented late such as the late establishment of the cybersecurity Hub. Currently the key custodian of the NCPF is the SSA with the JCPS cluster as tasked with providing an oversight role, the DTPS and various other stakeholders are equally important as they all are tasked to each contribute significantly in the implementation of the objectives.

As cybersecurity is a global concept, the implementation of the NCPF is largely dependent on various international and regional countries. There is however, currently no such interaction and as such SA is attempting unsuccessfully to

implement such recommendations. It is rather challenging for a country to successfully implement any cybersecurity policy or any related document in the absence of any international coordination. As much as there are relations which currently exists namely; with the EU, SADC and AU, there is no constant interaction more specifically with operational matters specifically with advises on decision making. Finally, there is a lack of trust which has led to SA often not sharing information with a believe that they are safeguarding the county's sensitive information, this is a good initiative while at the same time it is disadvantaging the country in terms of the sharing of skills.

6.3 Proposed recommendations

The NCPF is one of the South African government initiatives aimed at curbing and reducing the growing cybercrimes and related incidents in the country. This research has outlined that the NCPF has not been effectively implemented as projected when the framework was approved in 2012 due to a number of factors which have been outlined in the previous section. This section will therefore provide a list of recommended measures which will be communicated to the DTPS as well as all stakeholders highlighted in the NCPF. This chapter will be summarized into a shorter document and therefore sent to the departments concerned and more specifically the DTPS, alongside a request to conduct a PowerPoint presentation of the findings and recommendations. Below are the recommendations provided by the researcher.

DTPS employee empowerment programs

An information awareness session should be organised by the Chief Director: Cybersecurity. All officials responsible for the implementation of the NCPF should be invited to form part of the discussions on factors in relation to the NCPF. A presentation outlining the NCPF should be provided by the head of the department and thus a progress update should be given in terms of the progress made since 2012. This information session should be tailored in a manner that it assists officials in terms of the definition of the NCPF, its scope, focus, goals and objectives. Furthermore, this information session should also establish short-term objectives with due dates and a review session should be held in six months following the first

session. If the session is successfully executed, it is then that all officials within the DTPS can be involved to form part of future sessions.

Skills Development Programs

The DTPS should establish a skills development programs which must include all officials working within the cybersecurity space. There are various options currently available which can be exploited by the DTPS. The DTPS can sign a MoU of training with various SETAs for cybersecurity programmes which can be funded by the Department of Education. The DTPS can also enter into a training agreement with various institutions of higher learning such as the University of Pretoria, University of Johannesburg and the WITS University for short-term certificates on cybersecurity. The DTPS can also enter into a training agreement with various private companies such as Wolfpackrisk and ISACA who can create short-term courses which caters for cybersecurity needs, and finally a MoU with regards to cybersecurity training can be signed with the South African Defence Force or the State Security Agency to assist in the training of cybersecurity skills. Officials already employed by the DTPS and working with the implementation of the NCPF can be taken on these courses. The DTPS can also recruit unemployed graduates in various sectors and immediately take them on these courses and once completed they will then be ready to fully operate under supervision.

Significance of operational funds

The training of cybersecurity officials as well the implementation of various other objectives outlined on the NCPF is a highly expensive. This therefore requires a solid understanding of the need for the implementation thereof in proportion to the funds required. The DTPS should develop a good proposal and address it to the National Treasury requesting finances to fund the implementation of the NCPF. In the proposal, the DTPS should outline the need for cybersecurity, the need for technical expertise, the need for technical equipments as well as the implications for the lack of effective implementation of the NCPF objectives. This proposal should also be made available to other stakeholders tasked with the implementation of the NCPF objectives thereby creating a platform for the sharing of information in the Hub. The

DTPS should thereafter create a cybercrime incident record linked to the SAPS cybercrime database which must be submitted to the National Treasury (NT), this report will quantify to the NT the impact of an effective, fully-funded Cybersecurity Hub in a country.

Stakeholder involvement in the Cybersecurity Hub

The Cybersecurity Hub was established as a 24 hour point of contact by all key stakeholders highlighted in the NCPF. This is an area where all cybersecurity threats are supposed to be reported and the relevant stakeholders proactively respond before it intensifies. This however is not the case as there is currently no sharing of information by stakeholders. A stakeholder committee should be established consisting of all stakeholders highlighted on the NCPF, this committee should consists of senior officials with the capacity to make decisions, and therefore have meetings on a regular basis. In addition to the committee, there should be a secure communication line created with analysts from various department having access thereto. This therefore means that, as much as they are not formally stationed at the Cybersecurity Hub, they will have virtual access to the hub. There should however be limitations to this access namely; the analyst can only access their own portal, can only receive information once processed by the Hub and communication from the virtual analysts can only be received by the most senior official in the Hub who is security cleared.

Security Vetting of officials in the Cybersecurity Hub and the involvement of security cluster operatives

All officials working with the implementation of the NCPF should be vetted and therefore security cleared to Top Secrete by the State Security Agency. These officials should furthermore sign a declaration of secrecy which binds them not to disclose any sensitive state information. The vetting of officials is necessary as such officials will be dealing with sensitive state information which might be used for sensitive operations and might furthermore be exposed to secrete state operations. Additionally, an information security awareness program must be rolled out by officials in the security cluster such as the SANDF, SSA or the SAPS Crime

Intelligence. This awareness program will train all officials in terms of the secure handling of the states' information in terms of document classification, control, access, storage and disposal. Finally, these officials should have constant visit to the Hub to assist in the adherence to the information security rules by officials.

A more aggressive and direct cybersecurity awareness program

Although rolled out, the impact of the cybersecurity awareness program is currently not effective. This is as the messages contained are only accessible to a selected number of individuals mainly those in close proximity to the DTPS offices. The DTPS should adopt a more aggressive approach with regards to its cybersecurity awareness program with regards to the utilisation of the social media which is where most cybersecurity breaches occur, here cybersecurity awareness messages can be sent out to users of sites such as Facebook, Twitter, Instigram and WatsApp. The DTPS can also enter into an agreement with the South African Broadcast Services (SABC) to negotiate affordable rates and then run awareness messages which can reach a wider audience in televisions and radios. Instead of using digital billboards which are more expensive, the DTPS can print traditional smaller billboards which can be distributed to more communities. The DTPS can also enter into an agreement with various municipalities who are rolling out free Wireless Fidelity (WiFi) throughout the country, their role will mainly be to send cybersecurity awareness messages to user of the free WiFi platform.

Additionally, the DTPS can also conduct a cybersecurity awareness road-show targeting various schools across SA. These road-shows will be educating leaners on a safe and secure conduct in the cyberspace and more specifically in the social network sites. A pilot study can be launched whereby five schools from each province are selected and a team is established from the DTPS to visit all these schools in a period of six months. Once the pilot study is successfully executed, a fully-fledged project can be launched and more schools can be targeted. Furthermore, the DTPS can also send awareness messages directly to officials in various government department trough intranet messages. To start-off this process, the messages can only be sent out to officials employed by the organisations identified as critical NCPF stakeholders and after a considerable time, more

government department can be included. As soon as all the government departments are included, the State owned Entities and the Private companies can also be included.

The involvement of the Department of International Relations and Cooperation (DIRCO)

DIRCO should also be included as a stakeholder in the NCPF. The role of DIRCO should solely be the establishment of international and regional relations with countries particularly in terms of strengthening SA's relations with regards to cybersecurity. DIRCO should be included as their line function involved international and regional stakeholder coordination, therefore it will be much easier for them to connect the head of the DTPS with the organisations dealing with cybersecurity in the country which the DTPS believe can add value to SA. Furthermore, DIRCO has got a much deeper understanding of the bilateral and multilateral relations as well as the sanctions which have been imposed in some countries. This will therefore assist in the DTPS not entering into an agreement with a country which has been barred from operating with SA.

6.4 Conclusion

Chapter six of this report has provided concluding remarks made by the researcher based on the entire research conducted with the motive of understanding the barriers which are affecting the implementation of the NCPF. The latter part of this chapter focused entirely on the recommended measures which the researcher believes the DTPS, as the chosen case study, can adopt to strengthen its strategy towards the implementation of the NCPF objectives. As much as some officials believe that there generally is positive support from the senior officials within the organisation, namely the minister of the DTPS, there is a total of eight barriers that the research identified as the main ones which are affecting the implementation of the NCPF by the DTPS.

The researcher, in this chapter concluded that there is generally a lack of common understanding of the NCPF by those officials responsible for its implementation. The

researcher also concluded that as much as the cybersecurity awareness program is being rolled out, it is not as effective as required and it is not reaching the required audience. The researcher also concluded that there tends to be clashes of mandates amongst stakeholders tasked with the implementation of the NCPF. The researcher furthermore concluded that there is a general lack of skilled cybersecurity officials specifically in the cybersecurity hub and those officials in the hub are not security cleared. The researcher also concluded that officials stationed in the Hub are not trained on the secure use of state information by the security cluster, and there is no visibility of security cluster officials in the hub. Finally, the researcher concluded that there is generally no stakeholder coordination among all role-players tasked with the implementation of the NCPF.

Based on the above conclusions, the researcher made recommendations which will be communicated to the DTPS as well as to other relevant stakeholders as outlined in the DTPS. The communication of the recommendations will be tailored in different forms and will be written in a summary form addressed to a specific department with the barriers affecting that department directly alongside the recommendations. Most of the recommendations outlined in this report will be communicated to the DTPS as it was chosen as the case study and interviews were conducted to officials employed by the DTPS. As soon as the report has been approved by the university, the researcher will send a summarized copy to the DTPS and furthermore send a letter requesting to conduct a PowerPoint presentation of the findings and recommendations.

The researcher, in this chapter recommended that, the DTPS should adopt a much more aggressive approach to cybersecurity awareness and directly address a much wide audience. The researcher recommended that the DTPS should develop a skills development program and enter into agreements with various institutions namely, SETAs, institutions of higher learning and private companies to train all officials currently working within the cybersecurity space and furthermore recruit unemployed graduates who must be immediately taken on various causes prior to working. The researcher recommended that all officials working in the Cybersecurity Hub be vetted and therefore security cleared by SSA, furthermore, these officials should also be trained on the secure use of information security. The researcher recommended

that the DTPS should engage the NT in terms of the request for more funding for the implementation of the NCPF and exercise more transparency thereto. Finally, the researcher recommended that the DTPS includes DIRCO with regards to its expertise when forging international and regional relations.

This chapter conclude the research conducted on the barriers in the implementation of the NCPF. Based on the research conducted, it was uncovered that there exists barriers which are affecting the implementation of the NCPF. The researchers individually unpacked all the barriers alongside recommended counter-measures. As much as most of the barriers identified are directly within the DTPS as it was chosen as a case, the implementation of the NCPF is largely dependent on all stakeholders mandated by the NCPF. It was thus uncovered that the barriers in the implementation of the NCPF are not solely limited within the DTPS, however, they are across all stakeholders tasked with the implementation thereof as such all stakeholders should jointly work together to ensure effectiveness in the implementation of the NCPF objectives.

APPENDIX A: LIST OF REFERENCES

Cassim, F. (2015). Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. The comparative and International Law Journal of Southern Africa, 44 (1), 123-138

Cloete, F & Wissink, H. (2000). Improving Public Policy (1st Ed). South Africa: Van Schaik Publishers

Electronic Communication and Transaction Act, South African Statutes. (2002)

Grobler M & Van Vuuren JJ. (2007) Combating cyberspace fraud in South Africa [slides] from Council for Scientific and Industrial Research

Grobler M & Bryk H. (2010) Common challenges faced during the establishment of a CSIRT. Pretoria: CSIR

Goredema, C. (2012). Predatory Cyber Crime in South Africa: Current Risks and Realities. Cape Town: Institute for Security Studies

Herselman, M & Warren, M. (2010). Issues in information and technology: Cyber Crime Influencing Business in South Africa. http//www.informationscience.org Accessed: 2 August 2015

Hewlett, L.(2014) Qualitative Research Methods [Slides] Johannesburg: Wits School of Governance

http//:www.whatis.com. Accessed: 12 February 2016

Interception and Monitoring Prohibition Act, South African Statues. (1992)

Khoza LM. (2016). Standard bank confirms R300m lost in credit card scam. Retrieved from: http://ewn.co.za/2016/05/23/standard-Bank-confrims-R300m

Kuehl DT. (nd). From Cyberspace to Cyberpower: Defining the Problem.

Merran, SB. (2009). Social Research Methods: *Qualitative and Quantitative Research Methods.* San Francisco: Jossey-Bass

Mokati N. (2016). Panic hits as Anonymous hacks SA sites. Retrieved from: http://www.iol.co.za/news/politics/panic-hits-as-anonymous-hacks-sa-sites

Ngulube, P. (2007). The Nature and Accessibility of E-Government in Africa. International Review of Information Ethics, 7 (9), 1-13.

Neuwman, WL. (2001). Social Research Methods: Qualitative and Quantitative Approaches (6th Ed). USA: Pearson

Osuagwu, O, Ogiemien, T, Okida, S. (2010). Deploying Forensic Science & Technology for resolving national cyber-security challenges. Journal of Mathematics and Technology,3, 2078-0257

Pieterse, P.(2015). Is South Africa geared up for new cyberspace challenges? *Transnational Treats and International Crime Division [Slides]. Retrieved from*http://www.iss.com/presentations/cybercrime/cybercrimes-challenges

Prevention of Organised Crime Act, South African Statutes. (1998)

Ramgovind S, Eloff M, Smith E. (2010). The Management of Security in Cloud Computing. Pretoria: University of South Africa

Rezaire, T. 2014. Afro cyber resistance. *South African Internet Art,* 12, 2-3.

Ricttie L, Lewis J. (2003). Qualitative Research Practice: *A guide for Social Science Students and Researchers.* London: Sage

State Security Agency. (2012). National Cybersecurity Policy Framework for South Africa: No. 3947. South Africa: Government Gazette

State Security Agency. (2016, February 4) Budget Vote Speech. Retrieved From State Security Agency Website: hptt://www.ssa.gov.za/budgetvotespeech

Tamarkin, E. (2015). The AU's cybercrime response. *A positive start, but substantial challenge ahead*. , Policy brief 3. Pretoria: Institute for Security Studies

Techno Pedi. (2016). Digital Forensics. Retrieved from: https://www.twchnopedia.co/definition/27805/digital-forensic

The Cybersecurity Colloquium, 27 March 2014.

United Nations Report on Cybercrimes risks in South Africa. Retrieved from: http://www.unitednations.com/cybercrimeincidents/southafrica2013

Van Nieuwkerk, A. (2015). Cybersecurity capacity building workshop: "Good practices in developing Cybersecurity and Cybercrime Strategies". Johannesburg: University of Witwatersrand

Von Solms SH. (2015). A Maturity Model for Part of the African Union Convention on Cyber Security. South Africa: University of Johannesburg

Wagner, C., Kawulich, B., Garner, M. (2012). Doing Social Research: *A global context.* London: McGraw-Hill.

Yankey, A. (2013). African Union Perspectives on Cybersecurity and Cybercrime Issues: The AU Draft Convention on Cybersecurity and related Activities. [Slides]. Yaoundé: AU

Yin, R. (2014). Case Study Research: *Design Methods (5th Ed).* Los Angeles: SAGE

APPENDIX B: INTERVIEW QUESTIONS

Interview Session: 20-30 Minutes

Ice Breakers

- The interviewer will first introduce himself and thereafter outline the purpose, scope and duration of the interview and deal with the informed consent, thereafter, the following ice breaker questions will be asked prior to the actual interview questions.
    - How are you today?
    - Please tell me about yourself in terms your official duties as well as how long you have been in this specific position.

SEMI-STRUCTURED INTERVIEW

1. To what extent were the NCPF objectives allocated to the DTPS attained since implementation?

    1.1 Please provide me with your understanding of the NCPF
    1.2 To what extend do you understand the NCPF in terms of its aims and objectives?
    1.3 What role does the DTPS and more specifically your business unit play in the implementation of the NCPF?
    1.4 Apart from your business unit, which other unit within the DTPS are involved in the implementation of the NCPF?
    1.5 What progress has the DTPS made, in terms of achieving the objectives set out in the NCPF?

2. What key factors strengthen or impede policy outputs and impacts by the DTPS?

    2.1 What factors, according to your understanding are strengthening the achievement of the NCPF objectives by the DTPS?
    2.2 What factors, according to your understanding are impeding the achievement of the NCPF objectives by the DTPS?

2.3 Apart from the ones outlined above, are there any other factors which either strengthen or impede cybersecurity-related policies outputs within DTPS?

3. What measures should be put in place to ensure the effective implementation of the NCPF by the DTPS?

3.1 What measures can be implemented by the DTPS to ensure the effectiveness of the NCPF?

3.2 What measures should be put in place jointly by all stakeholders involved in the NCPF to achieve the effective implementation of the NCPF?

3.3 Apart from the role-players involved in the implementation of the NCPF, which other stakeholders do you think should have been involved in the therein and what role do you think they should play?

3.4 What cybersecurity measures do you think the South African government should introduce in order to reduce the current cybercrimes and related incidents?