

Aligning the constitutional rights of citizens with cybersecurity measures in South Africa

D.M. Molwantwa

 [orcid.org/ 0000-0001-8682-6142](https://orcid.org/0000-0001-8682-6142)

Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Masters of Arts in Development and Management* at the North-West University

Supervisor: Dr BL Prinsloo

Graduation: May 2019

Student number: 22001824

DEDICATION AND ACKNOWLEDGEMENTS

I would like to dedicate this study to my family for their encouragement and support.

I would also like to express my gratitude to the following:

My supervisor, Dr Barend Prinsloo, for his unwavering academic insight and guidance throughout this academic undertaking;

The NWU (Potchefstroom campus) for the financial assistance;

Christel Claudine Matthews for her understanding, care, and patience;

Karabo Motaung, Kabelo Rapoo, and Mandisi Faku for their support and assistance and

God for making this a reality.

ABSTRACT

The growth of Information and Communication Technologies (ICT) and the internet (referred to as cyberspace) have enabled the world to be more connected than ever before. Moreover, the increased number of people accessing cyberspace has enabled people to access information and services instantly at increased levels. However, along with the growth of cyberspace came malevolent actors and threats that threatened the well-functioning of computer networks, financial markets, and governments' services and security. As a result, many countries have taken measures to curb cyber threats. Likewise, South Africa has also enacted a number of cybersecurity measures to thwart cyber threats and create a secure cyberspace for itself. However, cybersecurity measures taken by states, may have implications on the constitutional rights of their citizens. South Africa is no exception in this regard as this study demonstrates. This study assesses and highlights the cybersecurity measures in South Africa and how these measures impact on the constitutional rights of South Africans, especially the right to privacy. The study indicates that such impacts are more likely to happen if the state introduces cybersecurity measures from a realist approach-driven and state security-centric perspective. Finally, recommendations were provided to align cybersecurity measures in South Africa with the constitutional rights of its citizens.

Keywords: Constitutional rights; Constitutional democracy; cybersecurity; cyberspace; state security; human security

ACCRONYMS

APC – Association for Progressive Communications

CIO – Central Intelligence Organisation

DoD – Department of Defence

ECTA – Electronic Communications and Transactions Act

ICT – Information Communications Technology

IRERC - Institutional Research Ethics Regulatory Committee

NGO – Non-governmental Organisation

NCC – National Communications Centre

NSTF – National Science and Technology Forum

OIC – Office of the Interception Centre

SARS – South African Revenue Service

SSA – State Security Agency

USA – United States of America

TABLE OF CONTENTS

DEDICATION AND ACKNOWLEDGEMENTS	I
ABSTRACT	II
ACCRONYMS.....	III
CHAPTER 1: ORIENTATION, PROBLEM STATEMENT AND METHODOLOGY.....	1
1.1 INFORMATION AND COMMUNICATION TECHNOLOGIES IN SOUTH AFRICA.....	1
1.1.1 The constitutional rights and cybersecurity governance in South Africa.....	2
1.2 PROBLEM STATEMENT	4
1.3 RESEARCH QUESTIONS.....	4
1.4 RESEARCH OBJECTIVES	4
1.5 CENTRAL THEORETICAL STATEMENT.....	5
1.6 RESEARCH METHODOLOGY	6
1.6.1 Methodological Approach	6
1.6.2 Data Collection Instruments.....	7
1.6.3 Strategy For Data Analysis	8
1.7 ETHICAL CONSIDERATIONS	8
1.8 LIMITATIONS OF THE STUDY.....	8
1.9 SIGNIFICANCE OF THE STUDY	8
1.10 LAYOUT OF CHAPTERS	9
CHAPTER 2: CYBERSECURITY IN THE CONTEXT OF SOUTH AFRICA'S CONSTITUTIONAL DEMOCRACY.....	10
2.1 INTRODUCTION	10

2.2	WHAT IS CYBERSECURITY?	10
2.2.1	Cybersecurity seen through Realism perspective	14
2.3	WHAT IS A CONSTITUTIONAL DEMOCRACY AND WHY SOUTH AFRICA IS ONE?	16
2.3.1	Constitutional democracy of South Africa	17
2.3.2	Cybersecurity in constitutional democracies and non-democracies	18
2.4	The meaning of cybersecurity in South Africa	21
2.5	CONCLUSION	25
CHAPTER 3: CYBERSECURITY REGULATIONS INSTITUTED AND PROPOSED BY THE SOUTH AFRICAN GOVERNMENT AND THEIR COMPATIBILITY WITH THE CONSTITUTIONAL RIGHTS OF CITIZENS		27
3.1	INTRODUCTION	27
3.2	THE CONSTITUTIONAL RIGHTS OF SA CITIZENS IN TERMS OF PRIVACY AND PROTECTION FROM THE STATE.....	28
3.3	PROTECTION OF PERSONAL INFORMATION ACT	29
3.3.1	The purpose of the POPI Act.....	30
3.3.2	The constitutionality of POPI Act and Protecting Privacy	32
3.4	REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATIONS ACT (RICA)	34
3.4.1	The Constitutionality of RICA and its impact on privacy	36
3.4.1.1	Office for Interception Centres	36
3.4.1.2	The duplication of duties by the National Communication Centre and its unconstitutionality	38
3.4.1.3	Problems with blanket and indiscriminate retention of metadata.....	38
3.4.1.4	Technological devices used to intercept communication.....	39

3.5	THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT	39
3.5.1	Cybercrimes under the ECT Act	41
3.5.2	Problems with the ECT Act.....	42
3.6	CYBERSECURITY AND CYBERCRIMES BILL IN SOUTH AFRICA	42
3.7	OFFENCES UNDER THE BILL.....	43
3.7.1	Financial and personal information and data related offences	43
3.7.2	Unlawful access offences	44
3.7.3	Unlawful interception of data.....	45
3.7.4	Terrorist activities using computers offences	45
3.7.5	Espionage by computers and unlawful access to restricted data and information.....	46
3.8	OTHER IMPORTANT ASPECTS OF THE BILL	46
3.8.1	Establishment of 24/7 Point of contact and structures to deal with Cybercrimes	47
3.8.2	Conflict of the Bill with the Constitution	49
3.8.2.1	State centric approach to cybersecurity by the Bill	49
3.8.2.2	No express emphasis on the protection of the right to privacy	50
3.8.2.3	Sharing of information and entering into agreements with foreign states	50
3.9	CONCLUSION	54

CHAPTER 4: RECOMMENDATIONS AND CONCLUSION - APPROPRIATE CYBERSECURITY REGULATIONS THAT CAN BE ALIGNED WITH THE CONSTITUTIONAL RIGHTS OF CITIZENS		55
4.1	INTRODUCTION	55
4.2	THE THEORETICAL CONTEXT OF CYBERSECURITY IN SOUTH AFRICA'S CONSTITUTIONAL DEMOCRACY	55

4.2.1	Realism and cybersecurity measures and constitutional rights	57
4.2.1.1	Central theoretical statement and its application to the study.....	58
4.3	CYBERSECURITY MEASURES IN SOUTH AFRICA THAT ARE NOT ALIGNED WITH CONSTITUTIONAL RIGHTS OF CITIZENS	58
4.3.1	The POPI Act and constitutional rights	60
4.3.1.1	Aligning POPI with constitutional rights.....	60
4.3.2	The ECT and constitutional rights	61
4.3.2.1	Aligning ECT with constitutional rights	61
4.3.3	The impact of RICA on SA's citizens constitutional rights	62
4.3.3.1	Aligning RICA with the constitutional rights.....	64
4.3.4	Cybercrimes and Cybersecurity Bill and constitutional rights	65
4.3.4.1	Aligning the Cybercrimes and Cybersecurity Bill with constitutional rights	66
4.4	GENERAL RECOMMENDATIONS	66
4.5	CONCLUSION	68
5.	BIBLIOGRAPHY	69
6.	ADDENDUMS: LETTERS FROM LANGUAGE EDITORS.....	80

LIST OF TABLES

Table 2.1: Discourses influencing the understanding of cybersecurity	13
Table 2.2: Government departments involved in cybersecurity in South Africa.....	23
Table 3.1: Summary of the cybersecurity measures and their constitutionality	52

LIST OF FIGURES

Figure 3.1: Memorandum of Understanding between SSA and CIO	33
---	----

CHAPTER 1: ORIENTATION, PROBLEM STATEMENT AND METHODOLOGY

1.1 INFORMATION AND COMMUNICATION TECHNOLOGIES IN SOUTH AFRICA

With the advent of globalisation, the world has witnessed an unprecedented spread and use of Information and Communication Technologies (ICT). The usage and dependence on ICT has penetrated both the private and public sectors. This widespread usage of ICT has been made possible by the ever declining costs of ICT making it easy for people across the world, particularly in the African continent, to gain access and connect with the rest of the world (Kiboi, 2015:1). This rise in ICT and the penetration of cyberspace has become crucial to the operation and smooth running of both governments and businesses (United States General Accounting Office, 2004). For a country such as South Africa, ICT and cyberspace have become important parts of the government and the public sector (Mokhele & De Beer, 2007:61). For example, some of the South African government services to the public are now provided electronically. Such services include, *inter alia*, government employment information; the South African Revenue Services' (SARS); National Treasury; and the Department of Home Affairs' emigration services (Mutula, 2010:39).

While the increased usage and permeation of the internet in South Africa does benefit the South African government and its citizens with regard to service delivery, communications, and easy access to information, cyberspace also poses challenges and security threats to people and governments (Kiboi, 2015:3). The threats emanating from cyberspace include cyber-attacks and hacking (Paalman, 2013:9). As protection measures are usually taken at the level of the state, South Africa is no exception and has prioritised cybersecurity, its regulation and governance (State Security Agency, 2014). To achieve that end, the South African government has put in place a number of policies, strategies, regulations and laws related to cybersecurity with the intent of combating cybersecurity threats. These include the following:

- Cybercrimes and Cybersecurity Bill (CAC) (2015);
- Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) (Act 70 of 2002);
- Protection of Personal Information Act (Act 4 of 2013) (POPI);
- The Electronic Communications and Transactions Act (Act 25 of 2002); and
- National Cybersecurity Policy Framework (NCPF) (2015) (ECTA) (Research ICT Africa, 2015; State Security Agency, 2014; Right2Know, 2016).

These numerous cybersecurity measures can be seen as the “securitization of cyberspace” by the South African government. Securitization is when an issue is given an extraordinary attention as it is presented in such a way that it is under a serious threat and requires extraordinary measures to be protected (Collins, 2007:109). This move towards the securitization of cyberspace by the South African government can be understood through a realists’ perspective. This perspective posits that states are the primary actors in international system that is anarchic and has no overarching government. In this system, it is the primary responsibility of states, like South Africa, to ensure its security, safeguard its territorial integrity, and interests (Sorensen & Jackson, 2007: 49; Burchill & Linklater, 1996:30). While realism holds that states seek to maximise their benefits and gains in the international system, like from the spread of ICT and the penetration or usage of cyberspace, the South African government also has to thwart the cybersecurity threats (Phahlamohlaka *et al.*, 2011:1). Given the several policies, strategies and laws put in place in relation to cybersecurity (as mentioned above), it can thus be concluded that cyberspace has been or is being securitized in South Africa.

With these several measures in place to curb cybersecurity threats by the South African government, it is worth noting that cybersecurity threats do not only affect the state (Kaiser, 2015:12; Laughlin, 2016:348). According to Kaiser (2015), cybersecurity threats confront not only states but also citizens, individuals and private organisations. This point made by Kaiser (2015) then negates the realists’ perspective that makes the state the sole referent object of security (Cawthra, 2009:7). Therefore, with the recent increase cybersecurity measures in South Africa, this study seeks to uncover the threats posed by increased cybersecurity measures to the constitutional rights of South Africans. Moreover, the study seeks to investigate whether the cybersecurity measures in South Africa augment the constitutional rights of its citizenry (as guaranteed in the Constitution of the Republic of South Africa)(Constitution of the Republic of South Africa, 1996) and human security, or whether the measures only amplify the security of the state. This is because, there have been dissenting voices internationally on the hostile implications cybersecurity measures can have on human rights, privacy and the activities of civil movements (Hart *et al.*, 2014: 32; Rigoglioso, 2014: 28). The Constitutional rights of SA citizens is discussed next.

1.1.1 The constitutional rights and cybersecurity governance in South Africa

In recent years, a number of civil society movements, human rights groups, and the media have voiced their concerns and opposition to increased cybersecurity measures undertaken by the South African government (Right2Know, 2016: 3; Association for Progressive Communications, 2015:2). These civil society and human rights groups have voiced their concerns with regard to the dire implications the ICT and cybersecurity measures enacted, have on the constitutional

rights of South Africans, particularly the 'right to privacy' (Constitution of the Republic of South Africa, 1996; Ministerial Review Commission on Intelligence in South Africa, 2008:). For example, the Association for Progressive Communications (2015) has reported that the 2002 Interception of Communications and Provision of Communications Related Information Act (RICA) allows the South African intelligence services and law enforcement agencies to conduct surveillance on citizens, while there is inadequate and insufficient oversight on such practices (Association for Progressive Communications, 2015). As a result, civil society and human rights groups believe such practices by government agencies are a direct violation of the right to privacy in the SA Constitution (Right2Know, 2016:4).

In addition, South Africa is a constitutional democratic state. The Constitution of South Africa (Section 14) guarantees all citizens the 'right to privacy' and the right to freedom of expression. The right to freedom of expression includes the right to obtain and share information as well as the right of freedom of press and media. While that is the case, the Ministerial Review Commission on Intelligence in South Africa (2008) noted that, the National Communications Centre (NCC) was engaged in an unlawful and unconstitutional signals monitoring. The report further stated that the NCC was unregulated and could be used as an unlawful tool for mass surveillance on citizens. Moreover, with the rapid changes and developments in ICT such as the advancements in surveillance technology and increased cybersecurity regulations, governments can use such technologies to spy illegally on their citizens under the guise of "Cyber-terrorism" counter-measures (Right2Know, 2016:4).

Furthermore, in 2015 Al-Jazeera News reported on the leaked 'Spy Cable' documents. The discomfoting activities of the South African intelligence activities. The Al-Jazeera report revealed a clandestine agreement between the State Security Agency (SSA) of South Africa and Zimbabwe's Central Intelligence Agency to share intelligence and information about "rogue NGOs" and "identify and profile subversive media" (Al-Jazeera, 2015). Such revelations have been unsettling to civil society movements and human rights groups with regard to the intentions of governments and the implications they have for constitutional rights, such as the 'right to privacy' (Association for Progressive Communications, 2015:2; Right2Know,2016:4).

Therefore, it then becomes apparent that there are divergent views on the approach of governments and civil society to the governance and regulation of cyberspace and cybersecurity. While the state is concerned about the threats to its security and ensuring that it is secured against cybersecurity related threats, as Phahlamohlaka *et al.* (2011:3) stated, the civil society, human rights groups, citizens and the media are alarmed by the consequences that cybersecurity measures can have on the constitutional rights of the citizens as enshrined in the South African Constitution and the unchallenged powers such measures give to the state (Mail & Guardian,

2013). Given the responsibilities of the state to protect its citizens as discussed in section 1.1 and the allegations of infringement on the Constitutional rights of SA citizens as discussed in section 1.2, it is worthwhile to explore options to align these two aspects.

1.2 PROBLEM STATEMENT

While the growth of ICT and the penetration of cyberspace prove to be beneficial to South Africa, the threats accompanying cyberspace can have catastrophic consequences for South Africa and its citizens. It is therefore understandable that the state would want to protect itself and its citizens from harm. As realists point out, it is the function of the state to ensure its security and survival (Sorensen and Jackson, 2007:48). The South African government has pursued a number of interventions and measures to secure its cyberspace. However, such cybersecurity measures, policies and strategies have been met with strong criticism from civil society movements, lawyers, media and human rights activists as they appear to give more power to the state, its security agencies and violate constitutional rights of the citizens as Right2Know (2016:6) points out. There is a need to understand how cybersecurity laws, policies and measures in South Africa could impact on the constitutional rights of South Africans. The primary research question of this study is: *How can cybersecurity measures in South Africa be aligned to protect rather than to infringe on the constitutional rights of SA citizens?*

1.3 RESEARCH QUESTIONS

In order to answer the primary research question, the subsequent specific research questions are central to this study:

- What entails 'cybersecurity' in the context of a constitutional democracy such as South Africa?
- What are the cybersecurity regulations instituted and proposed by the South African government?
- Which cybersecurity regulations are incompatible and not within the constitutional rights of South African citizens?
- How should the existing and proposed cybersecurity regulations be aligned with the constitutional rights of South Africans?

1.4 RESEARCH OBJECTIVES

By taking into account the primary research question and the specific research questions, the following research objectives are addressed:

- To highlight and explore 'cybersecurity' in the context of a constitutional democracy of South Africa.
- To investigate and examine the cybersecurity regulations instituted and proposed in South Africa.
- To highlight and analyse the cybersecurity regulations in South Africa and their compatibility with the constitutional rights of South African citizens.
- To examine and analyse the appropriate cybersecurity regulations that can be aligned with the constitutional rights of South Africans.

1.5 CENTRAL THEORETICAL STATEMENT

While cybersecurity threats are real and have the potential to disrupt the South African government's operations, businesses and society at large, the South African government has the responsibility to avert such cybersecurity threats and secure its cyberspace. Moreover, the South African government cannot entrust its security issues and those of its citizens on other states to resolve. Therefore, the realism theoretical approach espouses two arguments that will be utilised to understand cybersecurity measures in South Africa. Firstly, the theory explains why South Africa is responding to cybersecurity threats by a number of cybersecurity measures. Morgenthau (1965: 12; 1985:31) expands on this point by stating that, like humans, states are preoccupied by their security, well-being and survival. He further states that countries have the highest regard for security and will pursue security even if it means going to war.

Secondly, the realism theoretical approach provides ample analytical tools. It helps to understand why South Africa is employing numerous cybersecurity policies. For example, the theory suggests that relations between states are branded by competition, mistrust, and a number of threats that can come from state actors and non-state actors. Therefore, states have to put in measures and policies in place that are well-calculated and that will ensure it protects its interests i.e.: security (Sorensen & Jackson, 2007:48).

While, according to realists the state has to secure itself, the state is constantly challenged in fulfilling this role of ensuring its security and survival (Morgenthau, 1985:31). Cybersecurity threats in South Africa do challenge the government's role of ensuring its security and that of its citizens. For example, the National Science and Technology Forum (NSTF) (2015) revealed that South Africa ranked third with the highest prevalence of cybercrimes in the world after Russia and China (NSTF, 2015:7). Panda Security (2018) further reported that South Africa ranks high as one of the countries that were most targeted by cybercriminals in the year 2017.

1.6 RESEARCH METHODOLOGY

Essentially, the purpose of research can be applied or basic. Basic research is conducted with the aim of amassing the general depot of knowledge and is apprehensive about creating new ideas and theories about what things are and why certain events occur (McNabb, 2004:13). In addition, research methodology describes the methods and techniques used for collecting data (Bryman, 2001:237) while Wolman and Kruger (2005:23) further point out that, research methodology also describes the tools and methods employed for the systematic and accurate conclusion of the research design.

1.6.1 Methodological Approach

This was an analysis into how increasing cyber security measures employed by the SA government could threaten constitutional rights. According to Bryman (2001:18), a research methodology is a technique for collecting data and Mouton (2001) points out that a methodology involves outlining a procedure that a researcher uses to condense, organise and analyse data in the process of undertaking a scientific research in social sciences. Therefore, the research methodology chosen for this research was a qualitative method. Leedy and Ormrod (2010:135) point out that qualitative methods “emphasize personal experiences, interpretation, and self-knowledge over quantification, are concerned with understanding the meaning of social phenomena and focus on links and attributes across relatively few cases.”

The intent of using qualitative methodology was to carefully study what has been researched about cyber security in South Africa, the measures in place regulating or governing cyber security and how such measures impact the constitutional rights of South Africans as guaranteed in the South African Constitution. Lastly, this methodology was further used to gather data from sources which include official government strategies and policy documents, cyber security bills and acts, text books, monographs, journal articles, policy briefs, internet articles and newspaper reports.

1.6.2 Data Collection Instruments

This research was a literature study utilising content analysis as a strategy for data analysis. Therefore, the literature was sourced from a variety of sources such as the following:

- The State Security Agency (RSA) official website: <http://www.ssa.gov.za/>
- Department of Justice, Correctional Services and Constitutional Development's (RSA) published documents and official website: <http://www.justice.gov.za/resources.html>
- Institute for Security Studies' publications (RSA): <https://issafrica.org/>
- South African Human Rights Commission published documents: <https://www.sahrc.org.za/index.php/publications>
- United Nations' Official Document system: <https://documents.un.org/prod/ods.nsf/home.xsp>
- Privacy International's official website and documents: <https://www.privacyinternational.org/reports>
- African Union's official website and documents: <https://au.int/web/en/treaties>
- Official South African Government online site: <http://www.gov.za/documents/notices>
- University of Johannesburg Centre for Cyber Security: <http://adam.uj.ac.za/csi/>
- International Journal of Cyber-Security and Digital Forensics: <http://sdiwc.net/digital-library/>
- ITU Telecom: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx
<http://www.itu.int/net4/itu-d/idi/2017/index.html>
- Right2Know Campaign publications and documents: <http://www.r2k.org.za/publications/>
- Catalogue of books: Ferdinand Postma Library (Potchefstroom Campus)
- Internet searches

Databases consulted for information included:

- JSTOR
- Ebsco Host
- LexisNexis
- Emerald
- Catalogue of Books: Ferdinand Postma Library
- Government Gazettes
- South African Legislation

1.6.3 Strategy For Data Analysis

This study employed content analysis as a strategy for analysing the gathered data. Leedy and Ormrod (2010:155) define this method as 'a detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes or bias.' Moreover, Webb *et al* (1981:201) add that, content analysis strategy allows a researcher to conduct an analytic study on literature. In addition, Berg (2001) points out that, this strategy is cost effective because the materials necessary for content analysis are available and easily accessible.

This strategy is useful when studying the cybersecurity measures and policies of South Africa and their implications for constitutional rights. This is because it allows the researcher to study the policies, laws, and proposed cybersecurity measures and how they impact/affect constitutional rights by examining the intended meanings, contexts and meaning of such cybersecurity measures (Webb *et al.*, 1981).

1.7 ETHICAL CONSIDERATIONS

According to Orb *et al.* (2001:13), the primary focus of qualitative research is people and their natural environment therefore, making ethical complications subtle. However, since this research was theoretical, there were no ethical consequences. Nevertheless, due to the importance of ethics in research, this study was conducted in such a way that it echoed the Institutional Research Ethics Regulatory Committee (IRERC) guidelines of the North West University (NWU). That was achieved by avoiding plagiarism. All the literature used in this research is acknowledged accordingly and is listed in the last chapter of the research in the bibliography. Moreover, before commencing with this research, ethics approval was to be obtained from the Faculty of Arts of the NWU. While no interviews were conducted, legal opinion was sought prior to the utilisation of the SSA's secret document that was sourced from the 'spy cables' of Al Jazeera (NWU, 2010:25).

1.8 LIMITATIONS OF THE STUDY

This research examined and analysed existing policies, regulations and laws on and related to cybersecurity and how they impacted on the constitutional rights of citizens in South Africa. Since the research focused on a literature study, other research tools, such as interviews were not utilised in this mini-dissertation. As a result, that limited the room to expand the study (NWU, 2010:25).

1.9 SIGNIFICANCE OF THE STUDY

This study is important in that it contributes to the understanding of cybersecurity regulation and governance in South Africa and how the increase in cybersecurity measures impacts on the

constitutional rights in the South African context. It provided several areas which could be explored in future studies as well as recommendations to align current cybersecurity regulation with the Constitutional rights of SA citizens. Moreover, it increased knowledge on the theoretical approaches followed by the South African government to cybersecurity regulation and governance.

1.10 LAYOUT OF CHAPTERS

This research contained four chapters, presented as follows:

Chapter one: The chapter provided background information of the study and also introduces key concepts regarding cybersecurity, cyberspace, the meaning and regulation thereof in the context South Africa.

Chapter two: The chapter presents literature and theoretical approaches related to cybersecurity, cybersecurity threats in South Africa. In addition, the chapter discusses the role of S.A government, constitutional rights in relation to the governance and regulation to cybersecurity. This is done through the prism of realism.

Chapter three: The chapter discusses the cybersecurity regulations and measures instituted and proposed in South Africa and how they impact on constitutional rights.

Chapter four: The chapter presents and analyses how the instituted and proposed cybersecurity measures by the South African government in South Africa can be aligned with the South African Constitution and constitutional rights of citizens. Lastly, the chapter provides findings, conclusions and recommendations.

CHAPTER 2: CYBERSECURITY IN THE CONTEXT OF SOUTH AFRICA'S CONSTITUTIONAL DEMOCRACY

2.1 INTRODUCTION

The proliferation of the internet, social networks and the penetration of cyberspace has grown immensely across the globe and this growth has also confronted governments, both democratic and non-democratic, with cybersecurity threats. As a result, a growing number of governments have sought to curb these cybersecurity threats by instituting measures as a response to this. However, these measures are not the same for governments as their referent object of security is not the same neither their understanding of cybersecurity, the system of governance or approach to security. Constitutional democracies such as South Africa or Canada, approaches cybersecurity differently than a non-democratic state like China. As a result, in this chapter, the meaning of cybersecurity in the constitutional democracy of South Africa is discussed. This is achieved by way of contrasting the understanding of cybersecurity in South Africa with that of other countries such as Canada and China to also uncover how cybersecurity is approached and understood between different countries with different systems of governance. Lastly, this is done to provide an understanding of how the meaning and understanding of cybersecurity in different countries influence the cybersecurity measures and governance.

2.2 WHAT IS CYBERSECURITY?

The development, growth and interconnectedness of the ICT such as email, the internet, mobile phones and satellite television have spread across the world at an explosive rate over the past decade. Among these, the internet proves to be the prime example. In the early 1990s, the internet contained only a few websites but grew exponentially, containing millions of websites at the beginning of the millennium. The number of people with access to ICT has been on a sharp increase due to the shrinking cost of manufacturing and selling of these technologies across the world (Choucri, 2010:42). This has also led to the gradual closing of the 'digital divide' between the developed and developing nations. Moreover, the decrease in costs of ICT has led to a decentralised and widespread usage of these technologies (Norris, 2001:21).

The growth of the internet and ICT have thus become crucial in the daily lives of many people around the world. Governments, nations and private companies have also become dependent on cyberspace and its related technologies (Krickeberg, 2016:2). While this interconnectedness of computer networks and the growth of the internet have become an integral part of everyday life, the possibility of attacks by means of computers such as viruses, cybercrimes, and worms are a

reality that confronts nations, governments, companies, and individuals today (Poulsen, 1999; Porteus, 2001). These threats in cyberspace have proven to be a serious security concern that, if not dealt with in time or prevented, can cause disruptions and damages to computer networks and also shut down the operations of both the public and private sectors. Cavelty & Mauer (2010:180) have also pointed out that, cyber threats and the possibility of attacks using malware vectors are a reality.

Due to these cyber threats and the chief risks that the internet poses to the security of computer networks, many public officials, security practitioners, academics and civil societies have thus catapulted the concept of cyber security to an important position in the field of security studies (Cavelty & Mauer, 2010:183). Cyber security has therefore assumed a high-ranking position among the 'new threats' of the post-Cold War era. As with many other concepts in the field of security studies, cyber security is also a contested concept. Cyber security is a concept that is broadly defined by different actors and has thus elicited different definitions, meanings and interpretations (Craigen, Diakun-Thibult & Purse, 2014:13-14).

According to Cavelty and Mauer (2010:180-183), the concept of cyber security first emerged in the United States of America (USA) in the 1980s, proceeding to gain popularity in the middle of the 1990s and thus spreading to different parts of the world and nations. Therefore, the understanding of cyber security and its theoretical foundation have been largely influenced by the writing on the subject by actors and academics in the USA. What constitutes cyber security has thus been shaped by the USA, but there is an emergence of variation in the different parts of the world as revolutions and advancements are made in the ICT (Brunner & Suter, 2008:87). With the ever-evolving advancements being made in technologies and science, the definition of cyber security is also broadened resulting in the lack of a comprehensive, concise and acceptable definition (Craigen, Diakun-Thibult & Purse, 2014:15).

The concept of cyber security is defined differently by actors in different sectors of security. According to Buzan (1983:37), that which constitutes security is affected and influenced by five major sectors of security. These sectors are as follows:

- military
- political
- economic
- environmental, and
- societal.

The above sectors therefore become important in the framing and understanding of security. This is because these sectors have divergent priorities and focus on what the 'referent object' of security is. The referent object of security is that particular object that needs to be protected and threats against it alleviated (Williams, 2008:5-9). Therefore, the referent object of security is not necessarily the same for different sectors. As a result, the definition of a particular concept such as cyber security will be defined differently according to each sector. The referent object, definition and meaning in each sector also influence the approach to cyber security taken by each sector. Williams (2008), further points out that, there cannot be threats or a discussion of security if there is not a referent object of security. In the context of cyber security, each sector and even actors will thus provide a definition that comprises of a referent object that needs to be secured such as email, sensitive/secret information, databases, computer networks etc.

Collins (2012:365) also makes an important observation that, the discussion on cyber security and how it is defined is not cast in stone and permanent. That is because the referent object of security in cyberspace is not static as technological developments and advances are always evolving. Collins (2012) notes that the changes in the technical aspects of the ICT change the referent object (Collins, 2012: 365). Therefore, what cyber security means and is defined as today will likely not be the same tomorrow. This then explains the lack of an agreed upon definition of what cyber security is.

Moreover, when grappling with the concept of cyber security, its meaning and how cyber security is approached, one realises that it is also influenced by three distinguishable but interrelated discussions. Collins (2012:369) states that these three discussions reinforce one another in terms of how threats are portrayed and security practices employed, referent objects of security, and major actors involved. The initial discourse on threat portrayal is technical in nature as it deals mainly with cyberspace and security threats such as worms, viruses and other malware that can result in the intrusion and disruption of computer networks and systems. The second is concerned with acts such as espionage by means of cyberspace and cyber-crimes. The third and last one has to do with the protection of critical infrastructures and "cyber-war". This is the discourse that has largely been driven by the military and more specifically the USA's defence establishment (Cavelty, 2012:369). The table below illustrates these three discourses influencing the conceptualisation and understanding of cyber security:

Table 2.1: Discourses influencing the understanding of cybersecurity

	Technical	Espionage/Crime	Military/Civil Defence
Major actors	• IT and computer experts • Anti-virus industry	• Law enforcement agencies • The intelligence services	• Military practitioners • Civil defence establishments • Security professional/ experts
Dominant referent object	• Computers i.e. hardware • Computer networks	• Operational plans of businesses and strategies • Secret and classified information (government networks)	• Military computer networks, networked armed forces • Critical information infrastructures

Source: Cavelty (2012:365)

While the table above by Cavelty (2012:364) illustrate the main actors in the sphere of cyber security, its definition and understanding, it is not only the government institutions such as the intelligence services, military and private companies that play a role in the cyber security domain and discourses. Human rights advocacy groups, civil society and non-government organisations have become crucial actors in the cyber security sphere and cannot be ignored (Buckland, Schreier & Winkler, 2015:11). Such groups also have completely different objects of security when defining cyber security and how they approach the subject. In recent years many such organisations have been vocal and critical of many definitions of cyber security and policies employed by states and government institutions (Office of the Privacy Commissioner of Canada, 2014:2). There is a common understanding that it is not only governments and private companies that play a role in cyber security but also society and individuals.

The definition of what exactly cyber security is does not exist. Every state, government, organisation and other players in the cyber space have their own definition of cyber security. The definition for each actor in cyber space is different as it is mainly influenced by what each player/actor and sector views as a referent object. As a result, one can only define cyber security in actor/sector-specific terms. This in turn can also serve as a basis for understanding the security practices and policies employed by that particular actor/player.

2.2.1 Cybersecurity seen through Realism perspective

Realism is a school of thought in international relations and its sub-field of security studies. According to Wohlforth (2011:500) realism has a rich history and continues to be the foremost and central paradigm in both security studies and international relations. Realism is mostly based on a common set of core assumptions about international relations and political life. These assumptions are, *inter alia*:

- States are the most prominent and primary actors in international politics.
- The international system is anarchic i.e. there are no central authorities that states account to.
- States are preoccupied with their own security and survival. As a result, states have to protect their territories, populations, their core values and way of life of their populations.
- States are always seeking ways to accumulate more power and enhance security.

The thrust of the cyber security debate into the fields of international relations and security studies therefore reflect (in certain ways) the resurrection of a realist-driven perspective on the security of computer networks, cyberspace, distribution of power in digital age, and the approach to cyber security by states (Craig & Valeriano, 2016:86). Cyber threats are viewed today as a priority security concern for states as governments warn of possible attacks on critical information infrastructures and other sensitive and important installations critical to the smooth running of governments. For example, in the year 2002, the US Defence Secretary at the time cautioned about a cyber 'Pearl Harbour' against important infrastructures such as the banking sector and power grids which are reliant on cyberspace or computer networks (Bumiller & Shanker, 2012:23).

The existence of cyber threats and lack of security in cyberspace became a serious reality for states across the world when the Estonia cyber-attacks of 2007 and the Stuxnet attack of 2010 on Iran (Schultz, 2016:15) occurred. Due to these attacks and others, cyber security is a priority for states. As seen through the realist perspective; this is an issue that threatens the security of states. Realists believe that states should never compromise their security and any threat to a state's security should be mitigated by any means necessary (Cavelty & Mauer, 2010:3). States

are always seeking ways to enhance their security as this can ensure their survival. Therefore, cyber security threats, according to realists, threaten the survival of the state and the security of its citizens. Moreover, the inability of any state to provide and ensure security for its population also undermines the legitimacy and authority of the state. As a result, the security of cyberspace has become a priority for states according to realists. This explains the current cyber security measures that the South African government has enacted and proposed (Schultz, 2016: 17).

Realists also believe that the international system is characterised by anarchy i.e. the absence of central authority that has power over states (Morgenthau, 1948:11). In the international system, states pursue their individual national interests and cannot rely on each other with regard to their individual security concerns and guarantees of such security. For example, while the cyber security threats are a global concern, states do not rely on international organisations and cooperation for the security of cyberspace. Rather, a large number of states have their unique and individual cyber security measures that are in line with their domestic cyber security issues (Craig & Valeriano, 2016:87).

Moreover, the lack or absence of a central authority with power over states induces distrust between states writes Waltz (1979:17). This lack of trust therefore forces countries to rely on themselves to ensure the security of their computer networks and cyber security interests. The anarchic nature of the international system also therefore explains the current lack of effective international governance in terms of cyber security (Orsi, Avgustin & Nurnus, 2016:3). According to realists, the anarchic and competitive international system fosters self-help and self-reliance among states and their cyber security measures reflect this. In recent years, states across the world have dedicated a lot of resources into cyber security initiatives and capabilities (Craig and Valeriano 2016:86).

Given the competitive nature of the international system, states therefore seek to gain an edge in securing their cyberspace and also project themselves as cyber powers. According to Nye (2011: 123) cyber power is “the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain”. Since power is central to realists, it is important for states to therefore accumulate it in cyberspace as well. This can ultimately enable states to have control over information and the dissemination thereof. Realists’ perspective on cyber security puts the state as the central actor and does not say much about how cyber security measures impact individuals and citizens. Moreover, realism remains mum on how the methods and measures employed to achieve cyber security affect the functioning of constitutional democracies such as South Africa. Lastly, realism as a theory is chiefly concerned about issues of security, power, and the centrality of states in politics, seems to be a fitting framework to unpack the debate on cybersecurity and how it can affect constitutional rights in the South African context.

Moreover, the uncertainties surrounding cyberspace and threats thereof also give realism an edge as a framework for understanding the preoccupation of states with cyber security.

2.3 WHAT IS A CONSTITUTIONAL DEMOCRACY AND WHY SOUTH AFRICA IS ONE?

The concept of constitutional democracy is a reality of our contemporary international system. However, this concept is not a recent one and has its origins in the European political thought of the seventeenth and eighteenth centuries. Constitutional democracy manifested itself in different forms during the post revolution era in England (1640 and once more in 1688), after the independence of the United States of America and through the writing of its Constitution in the year of 1787 and later in France post 1789 (Bellamy, 2013:7). Simply put, a constitutional democracy is a system of governance wherein the government rules by the consent of the majority and its citizens. Moreover, in such a system the Constitution is usually the supreme law of the country and it entails the democratic and liberal values of justice, equality, freedom, accountability, openness and transparency. The most prevalent principles in constitutional democracies are the primacy given to the respect for human rights, suffrage, freedom of speech, equality etc (Tully, 1995:4).

It should be noted that although a lot of states consider themselves constitutional democracies, they are different from one another. Countries like Germany, France, South Africa, USA, Italy and Australia are all constitutional democracies. These countries' domestic legal and political institutions, customs, and practices differ significantly in ways that mirror their diverse perceptions and notions of constitutional democracy (Bellamy, 2013:4). Moreover, in the diversity of constitutional democracies, values and principles such as human rights, equality, transparency etc are not held in the same regard and may not even have the same meaning. However, in many constitutional democracies like South Africa, USA, France and Australia there is a commonality that permeates them i.e. the centrality of the Constitution in their democratic governance system (Adagbabiri, 2015:3). The Constitution of many constitutional democracies is the supreme law, as in South Africa. In many of these countries, the Constitution limits the power of the state in defence of individual rights and the good of the entire society. Constitutional democracies therefore, in many cases, reiterate the liberal idea that government does not derive power from itself but from society. Constitutional democracies therefore, govern in terms of the democratic laws that are set out in the Constitution and which apply to all (Adagbabiri, 2015:3).

In the USA, the Constitution limits the power of the government and goes further to impose a system of checks and balances across the three branches of government (Davies, 1996:2). This is also true for South Africa. Most importantly, in many constitutional democracies all government institutions, with the inclusion of parliament, judiciary and the executive, conform to the

Constitution as the supreme law of the country. The Constitution further binds all to observe the limitations that the supreme law of the land places on their power and authority (Ogundiya, 2010:2).

At the heart of a constitutional democracy is the principle of 'separation of power'. This principle was developed and popularised by a French political thinker Baron de Montesquieu who argued that if the rights of citizens and values such as justice, equality and freedom were to be guaranteed then the three branches of government should be separated and administered as such (Scott, 1999:15). Montesquieu further stated that failure to separate the powers among the three branches of government will result in tyranny, chaos, and violence. This assertion holds true in modern day constitutional democracies as most of them are relatively peaceful and citizens can exercise their rights accordingly. The adoption of constitutional democracy as a popular system of government is attractive to many countries across the world because of putting the citizens at the heart of governance. Lastly, the liberal ideas of equality, justice, openness, accountability and transparency are seen as imperative values that can ensure human development, progress and peace (Ogundiya, 2010:2).

2.3.1 Constitutional democracy of South Africa

The abolishment of the Apartheid system and the ushering in of a constitutional democracy in South Africa have been hailed as an important victory for the majority of South Africans who had been oppressed for decades under the repressive minority rule under Apartheid. The advent of the current universal suffrage and the adoption of a constitutional democracy in the country came after the negotiations between the old apartheid regime and the former struggle movements (Suttner, 2014:7-8). The new democratic dispensation was established in order to do away with the old apartheid laws and system of governance that was racist, exploitative and repressive. The new constitutional democracy also did away with the lack of rights of the majority of the populace that was subjected to injustice, inequality and violence (Suttner and Cronin 2006:3).

The South Africa's previous system of governance was based on the parliamentary sovereignty as opposed to the current constitutional democratic system. Parliamentary sovereignty of the apartheid system was inherited from the British Westminster system. Under this system, the parliament had the power to write and amend laws of the country. However, the adoption of the 1996 Constitution in South Africa meant that the parliamentary sovereignty system was immediately abolished and that the new democratic Constitution was the supreme law of the country. The current democratic South Africa is based on the principle of 'Constitutional Supremacy'. This principle means that the highest and supreme law of the country is the

Constitution. Furthermore, this means that all laws, institutions and actions being exercised by government are all subject to the Constitution. Any law or action taken by state organs have to be consistent with the Constitution and failure therefore can be declared unconstitutional by the courts of the country (Venter & Landsberg, 2006:36).

The difference between the old apartheid regime of parliamentary supremacy and the current constitutional democratic system is significant. For example, with the former, the parliament was supreme and considered all-knowing and the courts at the time applied the law as laid down by the parliament. However, with the current system that emphasizes the supremacy of the Constitution, parliament is not considered to know best but rather the Constitution guides and dictates the actions of all three branches of the government and state power is exercised in accordance with the Constitution (Venter & Landsberg, 2006:37). The current Constitution of the country guarantees equality, justice, and the Constitution also includes the *Bill of Rights* in chapter 2 and it touches on the daily lives of South Africans in many ways (Constitution of the Republic of South Africa, 1996). The fundamental rights which could be affected by state security-centric cyber-measures, include *inter alia* (Constitution of the Republic of South Africa, 1996):

- the freedom of thought or expression - section 7(1) and section 16;
- infringement on being equal before the law - section 9(1);
- unfair discrimination as described - sections 9(3) and (4);
- infringement on human dignity and its right to be protected – section 10;
- infringement on personal privacy – section 14;
- infringement on religion, belief or opinion – section 15, and
- access to information – section 32.

Summarily, the current constitutional democratic system of governance in the country was adopted to fundamentally undo past injustices of the apartheid regime and to further put the people at the centre of government and guaranteeing all liberal values of justice, equality, and political rights that were not given to all citizens under the old apartheid regime (Suttner, 2014:7).

2.3.2 Cybersecurity in constitutional democracies and non-democracies

Threats in cyberspace permeate all states across the globe regardless of whether a state is democratic or not. However, cybersecurity is perceived and approached differently by constitutional democracies and non-democracies (Buckland, Schreiner & Winkler, 2015:22). Moreover, while all states seek to secure their cyberspace in their respective territories, in constitutional democracies all endeavours to ensure security in cyberspace have to be done in accordance with the highest law of the land i.e. the Constitution (Ibid). Therefore, how

cybersecurity is viewed and approached within a constitutional democracy should reflect the values that most constitutional democracies espouse such as respect for citizens' rights, accountability, openness, equality etc.

For example, in a constitutional democracy like South Africa, the approach to cybersecurity is from a constitutional point of view. That is, the cybersecurity measures put in place should be checked against the Constitution and should not be inconsistent with respect to it. Cybersecurity measures put in place should not be in violation of the constitutional rights of citizens like the right to privacy or the right of access to information. In constitutional democracies, much consideration is given to how cybersecurity measures can impact on the Constitution of the country and on the rights of citizens (Singel, 2008). The limitation of state power in constitutional democracies have also ensured that states do not have monopolies on cybersecurity and the measures thereof. This has thus resulted in the idea that the approach to cybersecurity by governments have to be balanced between the security of the state and that of ordinary citizens. This balance within constitutional democracies are thus seen as a way to curb the realist-driven concept of security that is traditionally state-centric and neglects issues of citizens' rights (Buckland, Schreiner & Winkler, 2015:31).

In addition, being faced with cybersecurity threats (which are non traditional), constitutional democracies have also realised that states acting alone are insufficiently equipped to tackle cybersecurity issues alone. To this end, many academics, government officials, and security professionals have advocated for a multi-stakeholder cooperation between government, businesses, think-tanks, and citizens to deal with cybersecurity governance, policy, legislation, and measures (Bailes, 2006:41). The cooperation involving different actors in most constitutional democracies therefore ensures that all views and concerns by different sectors are taken into account and maybe addressed when cybersecurity measures are enacted. The inclusion of different actors thus ensures openness, accountability and can possibly limit the monopoly of the state in defining what cybersecurity means and how it is to be approached (Buckland, Schreiner & Winkler, 2015:31).

On the other hand, non-constitutional democracies have a completely different approach to cybersecurity. Countries like North Korea, China, Cameroon, Azerbaijan, and Syria fall within this category of non-democratic states. Within most non-democratic states, the internet or cyberspace is strongly controlled by the state. According to Khalathil and Boas (2001:5), the state in authoritarian regimes have a history of playing a central role in the development, regulation, and controlling of the internet, ICT and the use thereof. While democratic governments find it difficult to control the internet due to the limited powers imposed on them by the Constitution, non-democratic states do not have to account to their citizens and abide by the Constitution as the

regime is the law unto itself. This then allows the non-democratic state to shape how cyberspace or the internet develops, grows and spreads within its territory (Kalathil & Boas, 2001:6). It is worth noting that, authoritarian and non-democratic governments do not necessarily prohibit the use of the internet but rather certain intended purposes or uses of the internet. The use of the internet to criticise the government, leaders or exposing the wrongs being done by the regime is mostly prohibited within non-democratic states.

Cybersecurity in non-democratic states is used to extend the reach of the state and its power across the society. In such governments, states use the cybersecurity rhetoric as a pretext to silence dissidence, criticism by the masses, to spread state propaganda and invade the privacy of citizens and monitor the internet usage of citizens (Kalathil & Boas, 2001:6). In essence, cybersecurity in non-democratic states are not much about enhancing the security in cyberspace for all but rather enhancing the security of the state and controlling the online conduct of ordinary citizens and the information they can access, share and produce. This is done in order to ensure that the states' power is not threatened but rather strengthened. Cybersecurity in non-democratic states also means that states can exert their control over cyberspace in order to advance their own priorities and interests. Issues of privacy and human rights are mostly not considered and cannot be balanced with the security of the state. For example, in China, the internet mostly serves the interest of the state just like in the era of Mao Zedong when he asserted that the media was a tool of the state (Lee, 1990:5). Currently, while internet usage in China is high, the state continues to play a prominent and central role in the regulation, controlling and governance of the internet in China (Foster & Goodman, 2000:8).

In addition, cybersecurity measures in China are thus employed by the state to disseminate the ideology of the state, monitor the media, curtail any opposition to the state and also use the idea that certain usage of the cyberspace is threatening 'national security'. Therefore, the notion of cybersecurity in a non-democratic state such as China is statist in its nature and the state is using such to enhance its grab and control on power rather than to enhance the security and rights of citizens like in constitutional democracies in Europe and the West (Malinowski, 2001:10). This then demonstrates that cybersecurity is understood and approached differently by constitutional democracies and non-constitutional democracies.

2.4 The meaning of cybersecurity in South Africa

The growth of cyber threats, risks and attacks in South Africa is increasing and continuing to cause damage to economy and other important sectors of the South African society at an alarming rate as demonstrated in the previous sections. This challenge has been acknowledged by the South African government, the public and private sector. For instance, in 2014 the then minister of State Security Dr. Cwele, pointed out that the role of ICT is indispensable in South Africa. However, the minister further stated that these ICT enable malevolent and malicious cyber threats such as cybercrime, cyber-attacks, and cyber espionage and cyber war. As a result, such threats have necessitated the South African government to develop ample cybersecurity measures to thwart the threats emanating from cyberspace (Cwele, 2014:2).

For example, South Africa has experienced a number of serious cybersecurity breaches which have prompted the government of the country to remain vigilant of cyber threats and institute a number of measures to thwart these threats and develop mechanisms to manage them. In one incident signalling a serious information security breach took place on February 2015 when the Al-Jazeera news agency reported that it was in possession of classified intelligence reports that were leaked to the news agency. It was widely believed that the leaked reports might have been from a source working for the State Security Agency, which was worrisome for the South African government and citizens. These reports leaked to Al-Jazeera contained information from the South African intelligence operatives who reported the problems confronting the intelligence community of the country. The reports detailed the vulnerabilities in the South African government's departments and how they could be exploited by foreign intelligence operatives. The leaked documents further reported that the operatives of SSA had traced about one hundred and forty foreign intelligence agents who were under suspicion for trying to steal South Africa's military secrets, particularly the blueprints of the Rooivalk. The Rooivalk is the South African military helicopter which is among the best internationally recognised combat helicopters (Sapa, 2015).

In addition, the party responsible for leaking the classified information was never made public thus making it difficult to know whether the breach was the person in the employment of SSA or if the information was leaked through hacking of SSA computer networks. In spite of how the classified intelligence got leaked to Al-Jazeera, it underscores a serious cybersecurity breach, specifically an information breach at the country's intelligence agency that is considered to be critical in the preservation of security in the country.

In another incident, in 2014 the South African Police Service suffered a humiliating cybersecurity attack. A suspected hactivist group known as Anonymous hacked the website of the South African

Police Service. The group was able to download about 15 000 lines of personal information and data of confidential informants and whistleblowers aiding the South African Police officials. The information was then made public and available on other websites. The hacktivists announced that the hack was in retaliation to South Africa's perceived inaction over the police officers who were involved in killing the protesting miners of Marikana in the year of 2012 (Roane, 2013). This hack also highlighted the weakness and vulnerability in the security of computer networks of the South African Police Service.

The South African security agencies have also exhibited their capabilities with regard to combating cyber-attacks and cybercrimes. For example, a plot to steal over R800-million from the Gautrain Management Agency was uncovered in 2014. The attack was carried out by an ex-employee of Gautrain who had extensive knowledge of the financial systems used by the Gautrain Management Agency. The attacker employed sophisticated software to exploit the financial system in order to access passwords and banking details. The discovery of the attack was due to the routine audit of the Gautrain Management Agency's financial systems. Had it not been for the audit, massive financial loss could have been experienced by the Agency (Hosken, 2014).

Another cyber-attack in 2012 was experienced by state infrastructure of South Africa when a cybercrime syndicate managed to steal an estimated R42-million from Postbank, which is a financial services provider and forms part of the South African Post Office (Chauke, 2012). The investigation into this incident was conducted by the then National Intelligence Agency (NIA) (now called State Security Agency). However, the NIA required the expertise of private auditing and risk management firms. The use of private firms to investigate this incident therefore brings into question the cybersecurity skills of the State Security Agency in order to deal with cybercrimes (Chauke, 2012). The Postbank is responsible for the distribution of social security grants in South Africa and holds more than R4-billion in deposits.

Therefore, cybersecurity threats and risks are viewed as serious security threats that can destabilise the entire country and cause serious disruptions to the everyday lives of its citizens. Moreover, given the seriousness of cyberspace threats and attacks, the government of South Africa has responded by enacting a series of policies, legislation, strategies, and frameworks to address the threat posed by cybersecurity threats and risks. For instance, in 2015 the South African government responded by putting in place the National Cybersecurity Policy Framework (NCPF) which is led by the State Security Agency. Prior to the NCPF, in 2013 the Protection of Personal Information (POPI) Act was also put in place which established the Information Regulator with the aim of ensuring data privacy (SSA, 2015:1). These are among the many measures in place or proposed to counter cybersecurity challenges confronting the country. In addition, given the complex and sophisticated manner of ICT and cybersecurity, the approach to

cybersecurity in South Africa involves a number of different stakeholders. The key players in cybersecurity in South Africa are demonstrated in the following table:

Table 2.2: Government departments involved in cybersecurity in South Africa

<i>Cluster</i>	<i>Department</i>	<i>Policy or Legislation</i>	<i>Agencies and centres</i>
Justice, Crime Prevention and Security Cluster Cybersecurity Response Committee	State Security Agency	National Cybersecurity Policy Framework (NCPF) Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) Protection of State Information Bill	State Security Agency (SSA) SSA Cybersecurity Centre Electronic Communications Security Computer Security Incident Response Team (ECSCSIRT, n.d.)
	Justice and Constitutional Development	Cybercrimes and Cybersecurity Bill	National Prosecuting Authority (NPA) South African Police Service (SAPS)
	Defence	Cyber Warfare Strategy	Cyberwarfare Command Centre HQ COMSEC Ltd

	Telecommunications and Postal Services	Electronic Communications and Transactions (ECT) Act Cryptography Regulations (RSA, 2006) e-government Strategy and Roadmap (DTPS, 2017d)	National Cybersecurity Advisory Council (NCAC) National Cybersecurity Hub Cyber Inspectorate
Economic Sectors, Employment and Infrastructure Development Cluster	Trade and Industry	Companies Act	-
	Public Service and Administration	Promotion of Access to Information Act (PAI) Governance of Corporate IT Framework (DPSA, 2012) e-government strategy	State Information Technology Agency (SITA)
Governance and Administration	Public Service and Administration	-	-
	Justice and Constitutional Development	-	-

Source :(Sutherland, 2017:5)

While the government plays the leading role in cyber security, it is recognised that civil society, business- and private sectors have a significant role to play (Mahlobo, 2017). For instance, at the BRICS meeting of high representatives on security issues held in China in July 2017, the then SSA minister David Mahlobo reiterated that, government should work closely with business, civil society and the private sector to create safer and security cyberspace in South Africa (Mahlobo, 2017:2). Therefore, cybersecurity in South Africa is understood as a challenge that needs a holistic approach from multiple stakeholders.

South Africa perceives cyberspace and its related technologies as drivers of economic development, better health care, education, and security. However, there is also the understanding that these opportunities brought by cyberspace and ICT are also accompanied by challenges that are complex and need to be confronted by policymaking, law enforcement, research, cooperation and development of expertise in cybersecurity and ICT (Mahlobo, 2017:2).

Cyber security in South Africa then means protecting the cyberspace against risks that can threaten the cherished values and way of life of South Africans and the effective and uninterrupted functioning of the state. The South African government has also expressed its concern at the possibility that cyberspace and ICT could be used in the civil and military spaces to the detriment of stability, security, peace, and security of the state (Mahlobo, 2017: 2). The cyberspace and ICT can be used to interfere in the domestic affairs of states, their domestic processes like elections, and used to violate the private lives of citizens.

In addition, cyber security in the South African context entails measures to curtail crimes committed through the use of cyberspace. The previous sections have demonstrated the huge amount of money that has been stolen in South Africa and the economic damages the country has incurred due to cybercrimes. Such crimes impact negatively on the economic development of the country (Griffiths, 2017:13). Lastly, while pursuing the goal of securing the cyberspace of South Africa, the government has come to understand that a secure cyber space in South Africa should not come at the expense of the constitutional rights of its citizenry. For instance, David Mahlobo (who is the former minister of SSA) in July 2017 stated that “finding a balance between security and respecting human rights in the field of information security and communication technologies continue to be a contentious matter internationally” (Mahlobo, 2017: 4). This also forms the huge part of the question that this study seeks to explore i.e. are cyber security measures in South Africa aligned with the constitutional rights of the country.

2.5 CONCLUSION

Cybersecurity continues to dominate discussion in many countries around the world and many governments seek to secure their cyberspace by instituting a number of measures. However, these measures to achieve security in cyberspace are approached differently depending on the type of government and their referent object of security when addressing the issues of cybersecurity threats. How governments approach cybersecurity can also provide an understanding of how they understand security and whether the measures they put in place as a response to cybersecurity threats will have positive or negative implications for constitutional rights of citizens as is the case in South Africa. In South Africa the understanding is that cybersecurity should be approached in a balanced manner so as not to infringe on the rights of

citizens while also thwarting the cybersecurity threats. However, this does not mean that South Africa's cybersecurity measures do not infringe on constitutional rights of citizens as this has not been researched thoroughly before. While this chapter has provided an understanding of South Africa's views on cybersecurity and its meaning, the cybersecurity measures instituted in the country still need to be examined carefully against the constitutional rights of the citizens as enshrined in the Constitution of the country.

CHAPTER 3: CYBERSECURITY REGULATIONS INSTITUTED AND PROPOSED BY THE SOUTH AFRICAN GOVERNMENT AND THEIR COMPATIBILITY WITH THE CONSTITUTIONAL RIGHTS OF CITIZENS

3.1 INTRODUCTION

As was highlighted in chapter 2, governments and their citizens across the globe are confronted with the cybersecurity threats that accompany ever-changing technologies. Moreover, the government's Medium Term Strategic Framework (MTSF, 2017:3) also states that, ICTs are an indispensable part of South Africans' lives but the threats and challenges that come with such technologies should be addressed adequately through cybersecurity policies and mechanisms (MTPF, 2017:4). As a result, most governments – especially constitutional democracies have the responsibility to ensure a secure and free cyberspace for both the state and its citizens. Delivering such a secure and free cyberspace in a constitutional democracy is done within the confines of the Constitution. This is done to ensure that the rights of citizens, as set out in the Constitution, are not disregarded and abused all in the name of cybersecurity. Therefore, South Africa, as a constitutional democracy that guarantees rights to citizens, has over the years passed, enacted and proposed laws that seek to provide a cyberspace that is secure, safe and that is not achieved at the expense of the constitutional rights of citizens. These laws are as follows:

- The Electronic Communications and Transactions Act.
- The Protection of Personal Information Act.
- Regulation of Interception of Communications and Provision of Communications Act.
- The proposed Cybercrimes and Cybersecurity Bill (Which was amended by Parliament in 2017).

These four laws are measures instituted by the government, some in part, to address cybercrimes and cybersecurity challenges. In addition, these four pieces of legislation or cybersecurity regulations will be assessed individually to determine whether or not they are compatible with the constitutional rights of South African citizens such as the right to privacy and information as enshrined in the Constitution of the country. This chapter therefore, addresses the third objective i.e.: *To highlight and analyse the cybersecurity regulations in South Africa and their compatibility with the constitutional rights of South African citizens.* At the end of examining each piece of legislation, the study will highlight the compatibility such legislation with the Constitution and constitutional rights of citizens.

3.2 THE CONSTITUTIONAL RIGHTS OF SA CITIZENS IN TERMS OF PRIVACY AND PROTECTION FROM THE STATE

The Constitution of South Africa gives the citizens of the country the right (*inter alia*) to privacy. Chapter 2 of the Constitution contains the Bill of Rights and the right to privacy is among these rights. Furthermore, Section 14 of the South African Constitution states further that, every citizen has the right to privacy and that entails they have the right not to have:

- their property searched;
- their possessions seized;
- their home or person searched; or
- the privacy of their communications infringed (Constitution of South Africa, 1996).

While the Constitution of the country protects the citizens' right to privacy, Van der Bank (2012:78) goes further to state that, the right to privacy also means that an individual can conduct their personal affairs free from scrutiny and unwarranted intrusion by the authorities. Moreover, the author also states that this right also means that a person has control over their personal information. Therefore, the Constitution of South Africa (1996) protects the citizens' right to privacy and this also extends to safeguarding the personal information of individuals. This is because, the collection, processing and distribution of an individual's personal information, without their consent, has a bearing on their privacy. Moreover, Van der Bank (2012:79), points out that infringing on an individual's right to privacy can have a negative impact on their dignity and personality especially when the private and personal information of that person is distributed or made public and embarrasses the person.

Burns (2001:3) also reiterates the point made by Van der Bank (2012:79) that, the right to privacy also preserves the dignity of an individual. The author also states that, the right to privacy enhances the psychological, spiritual, as well as physical well-being of an individual while Right2Know (2016:5) state that, the right to privacy reinforces and supports other rights such as freedom of expression, association and information. Privacy (in legal terms) has also been described as a condition of life by an individual that is characterised by segregation or exclusion from publicity (Neethling, Potgieter & Visser, 2005:4). The right to privacy as enshrined in the Constitution of South Africa also serves to protect the citizens from the abuse of power by the state and its institutions. The state and its institutions (such as the police and intelligence services) have the ability and means to infringe on the privacy of the citizens (Right2Know, 2016:6). Therefore, the Constitution of South Africa puts an obligation on the state and its institutions to respect and protect the right to privacy. However, Moor (1997:3) makes an important point that, the right to privacy is not absolute and can be limited.

According to Section 36 (1) of the South African Constitution, the right to privacy of an individual can be limited. This limitation, however, must be justified and reasonable (Constitution of South Africa, 1996). This means that the decision to limit the right to privacy must be really in the benefit of the societal and democratic values of the country (Steiner, 2013:19). For example, when a crime is committed by an individual and there is proof against such an individual, their right to privacy can be limited and thus be subject to being searched as well as their properties. Moreover, as discussed in chapter 2 of this research, technological advances have also enabled criminals to commit crimes and infringe on the privacy of others using computers and the internet (Law Society of South Africa, 2013:1). As a result, the government of South Africa passed pieces of legislation and proposed other bills to fight crimes committed in cyberspace by using technological devices and cybersecurity. Some of this legislation allows the state institutions to limit the right to privacy of citizens who are suspected of such crimes. However, it is not known whether such legislation is aligned with the Constitution of the Country, particularly the right to privacy. The next section looks at these pieces of legislation individually and their alignment with the Constitution and the constitutional rights of citizens.

3.3 PROTECTION OF PERSONAL INFORMATION ACT

The Protection of Personal Information Act (the “POPI Act”) came into law in 2014. The ever-evolving advancements and developments in ICT have heightened cyber security risks such as breaches and theft of personal information in computer networks (Sutherland, 2017). As a result, the POPI Act was enacted to protect the accessing and dissemination of personal information (Norton Rose Fulbright, 2014). It is worth noting that, the Constitution of South Africa expressly guarantees the citizens the right to privacy. As a result, the POPI Act was put in place to facilitate this very right to privacy as enshrined in the Constitution of the Country (Constitution of the Republic of South Africa, 1996). Furthermore, this act underscores the importance of privacy in the internet and information age where developments in ICT and cyberspace have demonstrated the precariousness of privacy and how technology can be used to access the most private and intimate information about individuals without their consent (Law Society of South Africa, 2013:1).

The dangers of the abuse, manipulation of personal information and invasion of personal privacy have also been recognised in a number of states across the globe. As a result, several governments have thus put in place a number of laws to address the threats to privacy that have been recognised. For instance, the European Union states, whose privacy laws are based on the foundations of human rights have developed legislation to protect and govern the collection and processing of personal data. The Organisation for Economic Cooperation and Development (OECD) has also developed laws that regulate and govern personal information with a view to protect the right to privacy. It is worth noting that, many privacy laws and the protection of personal

data regulations around the world are based upon those of the EU and OECD (Law Society of South Africa, 2013:3).

The POPI Act came into being after a lengthy investigation and research conducted by the South African Law Reform Commission (SALRC) into the global development of laws governing and regulating privacy. Therefore, the POPI Act is largely predicated on the privacy principles of the EU and OECD. As a result, the POPI Act mirrors the information security and privacy initiatives in place around the world (Law Society of South Africa, 2013:3).

3.3.1 The purpose of the POPI Act

The primary objective of the POPI Act is to facilitate and give effect to the right to privacy as stipulated in the Constitution of South Africa. The Act therefore oversees and regulates how personal data and information is collected, kept/stored, utilised, circulated, and erased (Norton Rose Fulbright, 2014:1). The meaning of personal information is broad and comprises the information that can identify and relate to living persons. This can be, *inter alia*, race, employment history, and gender. The Act also includes the information relating to existing businesses i.e. contact details of a company and confidential correspondence (Swales, 2016:4). The business and persons that, that personal information speaks about to is referred to as the data subject. The POPI Act therefore safeguards the data subjects' personal information by putting in place the minimum requirements for the legal and lawful collection, processing, usage, storage and disseminating of such information (Norton Rose Fulbright, 2014:2).

The act further states that the data subjects should be notified of the processing of the personal information and must also give consent to such except in certain circumstances. The prevalence of this is where personal information is used to conclude a contract with the data subject. The act requires individuals, the private and public sectors to comply with it. The POPI Act therefore does not set a minimum compliance threshold (Luck, 2014). It applies to foreign and South African companies that process personal information in the country. An exception is only made where such personal information is forwarded through automated means i.e. electronic devices operating under instruction automatically and where the data subject's information is being filed. However, the act does not apply in circumstances where the information is used purely for artistic, personal, household and literary purposes (De Bruyn, 2014:1317).

Sensitive information such as information relating to or dealing with children, and special information relation to a person's sex, gender, religion, biometric, health, and criminal offences is (according to the POPI Act) subject to arduous processing responsibilities. For example, the transfer of this kind of sensitive information to foreign countries require that the party transferring

such information get authorisation and approval from the approved and legitimate information regulator in South Africa, in case the recipient of such information in a foreign country cannot guarantee the satisfactory protection of the data subject (Van der Merwe, 2016:12).

The POPI Act also makes it explicitly clear that the data subject should have access to information. The act guarantees that a data subject has the right to:

- a) know if an entity or organisation has their personal information without having to pay a fee;
- b) require or access their personal information for a fee;
- c) request that their personal information be corrected or removed in case their personal information is incorrect, too much, misleading or was accessed and collected by unlawful means; and
- d) have their personal information removed or deleted in the event that an organisation or entity is no longer legally allowed to have such information.

In addition, this act stipulates that individuals should not be contacted by any organisation using automated SMS, calls or emails to promote or sell its products and services without the consent of the individual or data subject. The act further requires that all communication by organisations to data subjects should contain accurate contact details and identity (POPI Act, 2013:10). The transfer of personal information across the border to foreign entities may only take place under certain circumstances such as where the data subject has provided their informed consent and where the foreign recipient of the personal information is subject to the obligations that are similar to those stated in the POPI Act which require the foreign recipient to provide satisfactory protection of the personal information transferred. The data subject must also be informed that their personal information is being collected with the intention of transferring it to a foreign entity (Cronje & Taylor, 2014:29).

The POPI Act also makes it compulsory for the entities or organisations retaining the data subjects' personal information to notify the information regulator and data subjects when their information databases have been breached, accessed and utilised by unauthorised parties. Given the recent spike of cyber security threats and breaches that have taken place in South Africa, this act becomes important as it seeks to promote a practice of transparency between the data subjects and organisations retaining their personal information. Moreover, this can also motivate organisations to put extra cyber security measures in place to secure the personal information of data subjects. It is also noteworthy that, the act also states that, in a situation where data subjects' personal information has been unlawfully accessed, the regulator has the right to instruct organisations/ entities to publicise data breaches that have taken place if such publicising may

protect the data subjects. Lastly, all companies or organisations and individuals must comply with the POPI Act. Failure to comply with the act can result in criminal and civil action to be taken against those not complying (De Stadler & Esselaar, 2015:36).

3.3.2 The constitutionality of POPI Act and Protecting Privacy

The POPI Act appears to be one piece of legislation that puts the citizens at its centre. The act seeks to protect individuals against illegal collection, processing, and distribution of their personal information without their consent. Moreover, the act protects individuals against unfair discrimination based on their race, gender, disability etc. One can therefore conclude that this act approaches cybersecurity from a 'Human Security' point of view. However, it took the South African government four years to establish the Information Regulator whose sole purpose is to ensure the implementation of the POPI Act and the adherence to the requirements of the act. The information regulator was only appointed on the 1st of December 2016. It is worth noting that, the Office of the Information Regulator is also not yet fully functional and under resourced. That poses as problem as the office has failed to prosecute companies that committed massive data breaches in the year 2017 and 2018. Such data breaches by companies place the majority of South Africans at risk as their bank details and ID numbers are likely sold on the dark web (Open Democracy Advice Centre, 2018; Daily Maverick, 2018).

One of the key assurances that the POPI Act spelled out was that the personal information of individuals cannot be transferred to foreign states but the act does not cover the transfer of information relating to people in the employment of NGOs or Non-Profit Organisations. This is quite a disconcerting fact because, a cache of secret documents from various intelligence services released by Al Jazeera shows that, in the years 2011/2012, the SSA and Central Intelligence Organisation (Zimbabwe) entered into a Joint Action Plan. The two intelligence services (in the Joint Action Plan) agree to monitor and exchange information on "rogue" NGOs and other institutions. However, the Joint Action Plan does not detail what "other institutions" are (Al Jazeera, 2015). Below is an excerpt from the Joint Action Plan between SSA and CIO:

SECRET

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
Best practice visit by CIO to the Financial Intelligence Centre (FIC)	30 April 2012		

OBJECTIVE 2: TO MONITOR ACTIVITIES AIMED AT SUBVERTING CONSTITUTIONAL ORDER

ACTION STEP	TARGET DATE	RESPONSIBILITY	COMMENT/S
1. Monitor and exchange information on rogue NGOs and other Institutions¹. The identification, profiling and assessment of NGOs engaged in subversive activities taking into account the following:	31 March 2012 31 August 2012	CIO and SSA: Internal/Domestic	CISSA definition of rogue NGOs to apply Further engage and share information.

¹ These include other non-state actors like Think Tanks, Non Profit Trusts etc.

Page 5 of 14

SECRET

Figure 3.1: Memorandum of Understanding between SSA and CIO

Source: Al Jazeera

Therefore, while the POPI Act prohibits the transfer of personal information to foreign states, intelligence services operate with extreme secrecy and the information regulator is not part of the Joint Standing Committee on Intelligence in South African Parliament to be privy to the operations of SSA. Therefore, the POPI Act can easily be trampled upon and circumvented by intelligence services thereby acting unconstitutionally. If this practice by SSA is still on-going then, it is in contravention of the POPI Act, the Constitution, and infringes the right to privacy as even individuals such as political activists can be called “rogue” and their information exchanged with other foreign intelligence services.

3.4 REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATIONS ACT (RICA)

The Constitution of South Africa expressly protects the privacy of communications for all citizens of the country. Nevertheless, the law of general application can limit the fundamental rights of citizens if such a limitation is based on the justifiable and reasonable grounds in a democratic society (Constitution of the Republic of South Africa, 1996). According to Van Der Merwe *at al* (2016:77), states that RICA is the law of general application. The RICA Act permits the surveillance, interception, and monitoring of communications in South Africa. This act is therefore deemed necessary in a country such as South Africa given the growth and usage of ICT and penetration of the cyberspace.

Cassim (2012:78) also points out that the aim of RICA is to ensure safety and security in the country. Its objective is to assist law enforcement agencies and intelligence services to be able to identify users of cell phone numbers and quickly trace criminals for legal purposes. While the primary objectives of the RICA Act is to assist law enforcement agencies in their endeavours to fight and prevent crime, the Act also governs and regulates the monitoring and interception in the private space of citizens (Bawa, n.d).

Before the passing of the RICA Act, the country relied on the Interception and Monitoring Prohibition Act (IMPA) for monitoring and interception of communications. While this act prohibited the interception of confidential information and communications, it could not be applied with regard to private spaces. The RICA Act is different from its predecessor IMPA as it has a broader and wider reach. For example, the current act is allowed in the private space. Moreover, it proscribes the premeditated or deliberate interception or allowance of the interception of communication while it occurs or transmitted. However, the act makes definite exceptions.

For instance, section 2 of the act points out that a person cannot deliberately attempt to or intercept, or allow or obtain another person to attempt to or intercept within South Africa, any

communication while occurring or is being transmitted. It is important to note that, both 'indirect' and 'direct' communication is included in the term communication according to the RICA act (RICA Act, 2002:13). Direct communication refers to the real conversation between two individuals and taking place in their presence. Section 1 of the act defines 'indirect communication' as follows: "the transfer of information, including a message or any part of a message, whether-(a) in the form of speech, music or other sounds; data, text, visual images, whether animated or not; signals or radio frequency spectrum; or in any form or in any combination of forms, that is transmitted in whole or in part by means of postal services or a telecommunication system" (Schultz, 2017:17).

According to the act, 'indirect communication' includes facsimile, internet, intranet, phone calls, personal and private e-mail messages, and voicemail and SMS messages. 'Indirect communication' thus comprises information downloaded from an internet site, e-mail messages sent and received as this process usually entails the transferral of information in the form of data, visual images, text using telecommunications systems (Schultz, 2017:36). It is important to understand that, while this act forms the basis of the regulation of communications' interception as well as internal traffic, the act also criminalises the unauthorised interception of communications that is contrary to the act's framework. The framework also points out that the directions to intercept communications must be issued by a designated judge when such directions are requested by law enforcement officers/agencies and the intelligence community. The act also states clearly that; interception directives will only be granted on 'national security' or crime-related grounds. The act also states that the directives to intercept communications will be undertaken the Office of Interception Centres (OIC) (Schultz, 2017:37).

The establishment of communications systems and networks that cannot be intercepted or have surveillance capability is also illegal under RICA. Therefore, communications service providers and Internet Service Providers (ISPs) are obliged to assist the state to intercept communications. Moreover, telecommunications operators, communications service providers, and ISPs are duty-bound by RICA to store all communications-related data – at their own expense - for no more than five years, to make the monitoring and interception of communications possible. Lastly, the act also reiterated that all cellphone users have to register their SIM cards and also provide their communications service providers with their identity numbers and residential addresses. According to Schultz (2017:38), RICA is a law that seeks to criminalise certain conduct in the cyberspace. However, RICA is limited in its implementation due to the fact that cybercrime and cyber threats are constantly changing. This then highlights the need to review RICA and ensure that it keeps up with the ever-evolving cybersecurity threats.

3.4.1 The Constitutionality of RICA and its impact on privacy

This next section looks at the impact RICA has on the right to privacy, the constitutionality of the act, and if the implementation of RICA in the country is legal.

3.4.1.1 Office for Interception Centres

In South Africa, the interception of communications is undertaken by and at the Office for Interception Centres (OIC). The OIC is established under RICA (Act No.70 of 2002) and is located in Pretoria. The OIC is under the command of SSA and reports to the Minister of SSA. According to Swart (2016:3), the office houses and is operated by staff from the various law enforcement agencies and intelligence services. These include members from the State Security Agency, SANDF Defence Intelligence and the SAPS crime intelligence division. The members working at the OIC have certain knowledge in the sphere of cyber surveillance (Swart, 2016:4). The members working at the OIC use the equipment that facilitates and enable the monitoring of telecommunications of people suspected of terrorist and criminal activity. The communications being monitored include cellphone calls, MMS and SMS messages, facsimile, internet traffic and activity, e-mails, social network usage, and messenger services like Skype and WhatsApp. In essence, the office can intercept and monitor all data and voice communications on both fixed-line and mobile networks.

It is also important to note that the OIC can and has the capability to monitor metadata i.e. call-related information. Metadata thus details the duration and time of calls, the location of the people calling each other and their contact numbers. However, RICA clearly states that the OIC can only intercept or monitor telecommunications after being authorised by a direction obtained from a designated judge (Right2Know, 2016:5). It is worth noting that, the interception of a person's communication and telecommunications networks without the directive of the RICA judge will be a total infringement and violation of the right to privacy and of the law. This will then result in the arrest and prosecution of those in violation of the RICA law. However, law enforcement agencies and intelligence services have demonstrated that they can get interception orders from judges under false pretences. For example, in 2013 it was confirmed that the SAPS crime intelligence officers had lied to a judge to wiretap the phones of two Sunday Times journalists (Sunday Times, 2013). This shows that, the security services can easily get interception orders and infringe on individuals' right to privacy under false pretences.

The above law also applies to the interception and monitoring of metadata. However, the only difference is that the directive to access metadata can be obtained from a court or magistrate by a subpoena. One should also understand that the OIC works closely with communications

services providers and ISPs. Under the RICA regime, these service providers are obliged to store metadata for up to five years and not less than three years. As a result, such metadata can be made available to law enforcement agencies and intelligence services by service providers after attaining permission from a court. Therefore, officials from the intelligence community and law enforcement must apply to a judge of court, magistrate or regional court magistrate to obtain metadata records from service providers (Swart, 2016:4).

The OIC and officials from intelligence services and law enforcement must prove on solid basis/grounds that obtaining metadata and intercepting/monitoring of individuals' communications is definitely justified in order to prevent crime or to provide justice. It is only if when the judge is satisfied and convinced that the invasion of individuals' privacy is justified that the directive can be issued (RICA, 2002:32). It is important to know that before the monitoring and interception can take place a case docket must be opened. In addition, the docket must be opened by the police through gathering enough evidence using traditional investigative methods without the assistance of cyber surveillance and interception. Failure to do so renders the gathering of evidence through interception illegal. However, while the issuing of an interception directive by the judge should be based on reasonable grounds, RICA does not make it mandatory for those seeking interception directives to return to the judge after the interception in order for the judge to assess whether the directive was indeed justified, that the suspected individual was involved in wrong doing and that their right to privacy was infringed on, on reasonable grounds.

The telecommunications services and ISPs also play a crucial role in enabling the monitoring and interception of communications by the OIC, intelligence and law enforcement agencies within South Africa. Under the RICA regime, communications providers are legally bound to give the OIC and its officials/operative access to their subscribers' communications once the directive has been issued by the judge or magistrate court. As a result, they have installed handover interfaces into their networks infrastructures. The handover interfaces replicate user's communication signal. This can be any data or voice call communication. Devices connected to the service providers' network can thus be intercepted or monitored. However, RICA prohibits the interference with the targeted user's communications and that this interception and monitoring should take place without the knowledge of the targeted person. The problem here is this: the person whose communications were intercepted, never gets to know about the interception even after the fact and even if the suspicion of them doing wrong was not based in reality. This sends the message that: one's privacy can be infringed through interception, (even if you are clearly innocent after the interception) and you are not given a chance to know about such an interception and the reason why such an interception was granted in the first place (Right2Know, 2016). One would expect a constitutional democratic state to be transparent in such instances. Lastly, RICA

only applies to domestic interception and does not cover or apply to the services such as yahoo, gmail, and WhatsApp whose servers are situated outside the borders of South Africa (Swart, 2016)

3.4.1.2 The duplication of duties by the National Communication Centre and its unconstitutionality

Apart from the constitutional establishment of the OIC under the RICA, the SSA also runs another entity with interception capabilities called the National Communications Centre (NCC) (Mail & Guardian, 2015). The NCC was established to collect and analyse foreign electronic signals such as calls, texts, emails and any communication that emanates from outside the territorial borders of South Africa and that passes through the country (Right2Know, 2016:6). Nevertheless, in 2008, the Matthew Commission found that the NCC was not established under any law in the Constitution nor is it regulated by any legislation (Matthew Commission, 2008). In addition, the Commission found that, the NCC was performing intelligence functions. This included the mass interception of communications outside the provisions and regulations set out in RICA.

Therefore, one can see that the NCC was duplicating and continues to duplicate the work performed by OIC. The only difference is that, the NCC collects information and mass data but outside the confines of the Constitution, particularly the RICA Act. The NCC, therefore, does not require authorisation from the judiciary to intercept communications like the OIC (Right2Know, 2016:4). This then means such an institution, which is currently under SSA, is illegally and unconstitutionally infringing on the privacy of citizens. What is more concerning is this: such an entity was established outside the law and continues to be operational to this day (Right2Know, 2016:4). Moreover, since RICA does not cover services that are based outside South Africa – the possibility is that – through the NCC then the emails and private conversations of citizens are intercepted and infringed upon by the NCC. This then has negative implications for the right to privacy for citizens (Right2Know:3, 2016; Swart, 2016:5).

3.4.1.3 Problems with blanket and indiscriminate retention of metadata

As mentioned above, the section 30 (1) (b) of RICA makes it mandatory for telecommunications networks and service providers to store all their customers' communications data for a period of up to five years (RICA, 2002). The retention of this data and information, unlike that obtained through an interception, is not targeted at a specific individual who is suspected of a crime. This then makes mandatory retention of data by service providers indiscriminate and based on shaky grounds. Moreover, this means that, one's most private and intimate data or information is being collected and retained for a period of five years not based on reasonable suspicion. The

mandatory retention of data by service and network providers (under RICA) is thus untargeted, blanket and indiscriminate in nature (Right2Know, 2016).

Moreover, to retain such private information and data about citizens suggests that their right to privacy is limited. However, the South African law requires that: a right can only be limited based on the principle of necessity and proportionality (Steiner, 2013:23). In addition, this untargeted and indiscriminate retention of data suggests that the state assumes all citizens are suspects of wrongdoing. This is then contrary to the constitutional principle of “innocent until proven guilty” (Dlamini, 2002:14-15).

3.4.1.4 Technological devices used to intercept communication

While RICA allows for the interception of communications by intelligence services and law enforcement agencies, it is not known what technological devices are used by these institutions to intercept communications (Right2Know, 2016:4). Moreover, it is not known how intrusive the interception technological devices are and the impact they have on the privacy and dignity of persons under suspicion and interception. It is further not known if the law allows the use of technological devices that are intrusive. RICA is not clear on this subject and it is one that is concerning as it can have dire consequences on the right to privacy of citizens. In addition, RICA does not regulate nor provides guidance as to what type of technologies can be used when intercepting communications (Swart, 2016:3).

Therefore, RICA is an important law in the sphere of cybersecurity. It sets out conditions, strategies and regulations that must be followed with regard to interception, monitoring and surveillance of communications in South Africa. In addition, the act is also important as it borders on the very sensitive line between security in cyberspace and privacy. However, this act has serious implications with regard to the right to privacy and is open to abuse by those who work in law enforcement agencies and intelligence service as explained above.

3.5 THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

The Electronic Communications and Transactions Act (ECT) came into law on the 30th August 2002 after being promulgated on the 2nd of August 2002. This was made possible by a number of South African law practitioners. Authors called for the enactment of law that will criminalise certain cyber conduct and activities. This act is thus relevant and important to this research. According to the ECT Act, its main aim is to address the “facilitation and regulation of electronic communications and transactions in the interest of the South African public” (Schultz, 2016:21). The act is also a fundamental piece of legislation that presides over the substantive governance of telecommunications industry in the country. While the act deals with a myriad of issues, a

chapter pertinent to this research, is chapter 13 of the ECT act as it addresses the issue of cybercrime. This chapter brings to the fore several criminal offences in the South African statutes that relate to information systems as well as the unauthorised accessing of data and interference or interception of data (Electronic Communications and Transactions Act, 2002:16-19).

The act also criminalises actions or conduct undesirable in cyberspace/internet. The act in section 85 defines “access” as including the actions of any individual who, subsequent to gaining entry to any data notices that they are unauthorised to gain entry to such data and still keep on accessing that data. Punishable offences are also provided for within the context of the act. The following sections clearly articulate the cyber conduct and offenses provisions in the act:

- Section 86 deals with the interception and interference of data without authorisation. The provision of section 86 (1) further states that an individual who accesses data-intentionally-without authorisation or permission is guilty of the offence. Section 86 (2) further provides that an individual that interferes with data intentionally while not being authorised or permitted to do so i.e. interference that causes modification, destruction and renders the data ineffective is also guilty of the offence.
- Section 86 (3) states that it is an offence for a person to offer to sell, sells, adapts for use, designs, get hold of for use, possess or distributes any device, with the inclusion of computer component or programme, which is fundamentally designed to trounce data protection measures, or does any of the actions to a password, pin code or analogous kind of data with the intention of unlawfully using such item to disregard this section, is also committing an offence and guilty.
- Section 86 (4) states that it is an offence when an individual uses any piece of equipment or computer program as indicated above to illegally breach measures of security put in place to protect data and even access such data.
- Section 86 (5) stipulates that it is an offence to commit actions mentioned above to interfere with the accessing of information system by legitimate users. These include the denial or partial denial of service to users authorised or permitted to access such information systems and data.
- Under section 87, the Electronic Communications and Transactions act also addresses and deals with forgery, extortion, and fraud related to computers. The section states that any person who threatens to or executes any of the actions stated in section 86 and 87, with the intention of acquiring legal proprietary benefit by assuming to desist or cease from such acts, or by assuming to reinstate any damage caused due to those acts, will be guilty of the offence and thus legally responsible upon conviction to penalties. Secondly, the section also states that it is an offence in terms of the law, for any person to gain advantage

unlawfully through acts listed in section 86 that results in the creation of fake data produced with the internet, leading to that fake data being considered or used as though it is authentic.

- The following section i.e. 86 of the ECT Act deals with the aiding, abetting and the attempt thereof. It states that any individual who helps and encourages someone to carry out acts as described in the sections 86 & 87 is also guilty of an offence.

While this section detailed the general offences under the ECT Act, the next sections present the specific cybercrimes under the Act.

3.5.1 Cybercrimes under the ECT Act

The ECT Act, being the first piece of legislation in the country seeking to address criminal behaviour in cyberspace, stipulates several actions as cybercrimes. Among other crimes, it is a crime under the act to gain unauthorised access to a computer system and computer, or even the illegal interception of data and information. The act therefore has provisions to specifically address hacking and interception. For example, when information or data is being sent or transferred over cyberspace, the data/information is broken down into smaller packages and these can be interfered with through interception and be copied prior to reaching their intended destination. The act thus makes it a criminal offence to intercept such information (Cassim, 2009:37).

The modification of information and data also constitutes a criminal offence in terms of the ECT. The act therefore provides for the anti-modification of data/information. As a result, the unpermitted interference with information with the intention of modifying, destroying or rendering the information ineffective is a crime. These include the utilising worms, viruses and websites' defacement. The acts and conduct aimed at circumventing security measures are also criminalised under the ECT act. Under the act, the designing, selling or even the production of programmes and devices that breach the security of information, data and systems constitute criminal offences (Papadopoulos, 2012:13).

Furthermore, acts in cyberspace that are aimed at or denies the legitimate users of computers or information systems access are a crime. The denial of service or partial denial of service to persons who are authorised to have access to information systems or computers is thus a criminal offence. Lastly, computer-related conduct that includes fraud, forgery and extortion are criminalised under the ECT act. The person found to be committing fraud, extortion and forgery in cyberspace is thus guilty of an offence (Cassim, 2012:8).

The ECT Act is therefore an important piece of legislation. It set precedence partly in addressing issues of crime and other undesirable conduct in cyberspace. Before the enactment of the ECT Act, there was no direction in terms of existing laws that dealt with such issues. Moreover, the act further made it possible for electronic data and electronic documents to be valid and admissible in courts of law in the country. Lastly, the act has been recognised to be in line with legislation of the developed nations around the world, but it has not been examined thoroughly whether it is in line with the Constitution of South Africa.

3.5.2 Problems with the ECT Act

The ECT Act has been praised by many as a law that seeks to protect the integrity of data, software, hardware, and prohibits the interference with computer networks as well as criminalising the unlawful denial of access and service to computers by unauthorised personnel (Cassim, 2012:7; Papadopoulos, 2012; Schultz, 2016:19). However, the Act also has negative implications on innovation and research. ICT experts and research institutions usually innovate and improve the existing software, hardware, and other technological devices by testing for weaknesses and building upon that for new technologies (United Nations Educational, Scientific and Cultural Organization, 2002:43). However, under the act, creating devices, hardware, software, and testing of security of networks is a criminal offence. Therefore, this offence forbids and constrains innovation by ICT experts and researchers. Moreover, the act criminalises “undesirable conduct” on the internet or cyberspace. The act does not clarify what constitutes undesirable conduct on the internet. This then can be interpreted broadly and anyone can be prosecuted for “undesirable conduct” on the internet (Swart, 2016:4).

3.6 CYBERSECURITY AND CYBERCRIMES BILL IN SOUTH AFRICA

The cybercrimes and cybersecurity bill in South Africa came into existence after the Department of Justice and Constitutional Development was mandated by government to review the cybersecurity laws of the country and to also ensure that the cybersecurity laws in the country provide for an integrated and a coherent cybersecurity legal framework in the country. It is also worth noting that this bill forms part of the review process of the laws that deal with matters related to cybersecurity as contained in the Statute Book of South Africa (Department of Justice & Constitutional Development, 2015:11). In February 2018, the bill was still before the portfolio committee on justice and correctional services for consideration. The bill sought to achieve a number of objectives. They are as follows:

- to create cybercrimes' offences and penalties thereof;
- to criminalise the distribution of harmful data messages and also provide provisional protection orders;
- to provide for the regulation of jurisdiction with regard to cybercrimes;
- to regulate the aspects of mutual assistance with regard to the investigation of cybercrimes and also the establishment of an around-the-clock point of contact;
- to prove certain facts by means of affidavit;
- to oblige all financial institutions and electronic communications service providers to assist in the reporting and investigation of cybercrimes;
- to establish structures that will build capacity and promote cybersecurity;
- to regulate the declaration and identification of critical information infrastructures and the measures to protect critical information infrastructures;
- to allow for the government to enter into agreements with foreign states in order to promote cybersecurity;
- to repeal and amend the provisions of certain laws.

However, after a lengthy discussion and comments from the public and other government officials, the bill was amended and its name was changed to a standalone 'Cybercrimes Bill.' This was due to the backlash and criticism the bill received from human right activists and other government officials. Among the criticism was that, the bill was too broad and could easily be used to abuse and invade the rights of citizens. As a result, the bill was called the "Cybercrimes Bill" and issues that related to cybersecurity were removed as they were the ones causing public outcry and received criticism (ITWeb, 2018).

3.7 OFFENCES UNDER THE BILL

While the bill's aim is to create a safe and secure cyberspace in South Africa, it also introduces new criminal offences. Such offences range from those related to data, computers, messages, networks, and certain conduct or behaviour on the internet. These offences are discussed below:

3.7.1 Financial and personal information and data related offences

The internet has brought with it many benefits such as the development of online shopping and the ability to make financial transactions digitally or online. However, such transactions have created opportunities for criminals to illegally obtain data, financial and personal information of unsuspecting individuals online and use this to commit crimes or enrich themselves. As a result, the bill states the following are offences with regards to personal and financial information and data:

- The obtaining of identity-related or financial information or data illegally;
- The illegal possession or transferring of a person's identity-related or information and data; and
- The use of identity-related or financial information and data for criminal ends or purposes.

It is an offence according to the bill to obtain the financial and personal information, identity-related data of anyone illegally. It recognises that there are individuals or syndicates that use illegal, intrusive and malicious means on the internet to steal the financial- and personal information and identities of others to commit crimes or even use such information to syphon money out of bank accounts. The bill, therefore, criminalises these acts as cybercrimes. Moreover, software and computer devices used to commit such offences are also forbidden from being used and manufacturing thereof constitutes a criminal offence. The illegal and fraudulent acquisition of sensitive personal information such as passwords and other financial and personal information also constitutes a cybercrime under the bill (Department of Justice & Constitutional Development, 2015:17). This sensitive information can also be acquired by cybercriminals who masquerade online as trustworthy individuals or companies thereby robbing and defrauding unsuspecting individuals. While financial information is the prominent target of cybercriminals, other personal information is also the target of these criminals. This information includes:

- Residential addresses and telephone numbers: which can be used for identity theft
- Non-financial accounts' passwords: having access to accounts allows cybercriminals to change account settings and allow them to use the accounts for their criminal activities.

Firstly, the bill criminalises the possession and acquisition (intentional and unlawful) of personal and financial information and data with the purpose of committing a crime. Secondly, it is also a criminal offence to acquire personal and financial information by any means and intentionally and unlawfully of another person or entity and providing such information to another party for purposes of committing a crime. Thirdly, the bill states that it is a criminal offense to unlawfully and intentionally use the personal and financial information of another person to commit a crime (Cybercrimes and Cybersecurity and Other Related Matters Bill, 2017:12). Lastly, it is a criminal offence for a person to be in possession of personal or financial information of another person and if there are reasonable grounds to believe that such information was used or is going to be used to commit a crime according to the bill.

3.7.2 Unlawful access offences

The development of computer networks and cyberspace, the interconnectedness of networks and computers are used by hackers and criminals for criminal ends. These include the stealing of

proprietary information, accessing of secret and classified information and confidential information. Moreover, hackers and criminals use the interconnected of computers to unlawfully and illegally gain access to databases of governments, private firms and confidential information of individuals (Snail, 2009:4). The information and data gathered through unlawful and illegal means i.e. hacking, is sometimes further used by the perpetrators to commit other crimes or even sold to other parties such as foreign states, businesses or individuals who need such information for criminal purposes. Moreover, criminal syndicates sometimes use unlawful and illegal means via computers to syphon or steal large amounts of money from government departments, companies and individuals' bank accounts. Moreover, seeing that much of the data and information of individuals, governments and businesses is stored in computer networks, the accessing of such data and information becomes easier for cybercriminals to unlawfully and illegally gain access to and thus commit further crimes with the data and information gained unlawfully and illegally (Van Niekerk, 2017:19).

As a result of the above and the rise of cybercrime in recent years, the Cybercrimes and Cybersecurity Bill seeks to criminalise the unlawful accessing of data and information. According to the bill, the unlawful and illegal accessing of information and data not only leads to financial losses and possible commission of other crimes but also undermines and bring into question the integrity of computer devices, data, information, networks, databases and other electronic communications networks (Department of Justice and Correctional Services, 2017:43). The bill states that the unlawful and illegal accessing of data and information are criminal offenses. To be specific, the unlawful accessing in whole or part of any data, a computer device, a computer network, a database, a critical database, national critical information infrastructure, or an electronic communications network is a criminal offense under the bill.

3.7.3 Unlawful interception of data

The bill criminalises the unlawful interception of data. Any person who therefore intercepts data, a database, a computer device, computer network, national critical information infrastructure, or an electronic communications network is guilty of an offence.

3.7.4 Terrorist activities using computers offences

Cyberspace and the internet has become an instrumental tool for extremist groups in recent years. Terrorist groups have resorted to the internet to spread their ideologies, propaganda and recruit members into their ranks. Terrorist organisations can also use the internet and computer networks to target, disrupt, and destroy computer networks, electronic communications networks

and databases of citizens and states (Beida & Halawi, 2015). As a result, the bill criminalises the following computer related terrorist activities:

- The use of the internet and computer networks to spread propaganda of terrorist organisations, to publish and describe the justification of terrorist activities and recruitment into such groups or organisations.
- The dissemination of terrorist information such as training manuals.
- The gathering of information for and by terrorist groups.
- The financing of terrorist organisations.
- Online training of recruits by terrorist organisations.

3.7.5 Espionage by computers and unlawful access to restricted data and information

States, companies and individuals do store secret and sensitive information in computer systems. Cybercriminals at times seek to access such information for self-enrichment or for use against those they stole the sensitive information from. Therefore, the bill seeks to address this by criminalising the unlawful accessing of sensitive and secret information. Performing any of the acts to unlawfully access sensitive and secret data or information under the act is a criminal offence.

3.8 OTHER IMPORTANT ASPECTS OF THE BILL

While the bill is intended to create a safe cyberspace and cybersecurity environment in the country, it is worth noting that the bill also expands on the ECT Act's shortcomings in terms of offences and the penalties of cybercrimes and cybersecurity breaches (Schultz, 2017:29). The following are the important aspects of the bill and are worth noting:

- The bill criminalises and prohibits the spread of data and information that advocates, incites and promotes hate, violence and discrimination.
- The bill criminalises and prohibits the incitement of damage to property and violence especially by the use of internet such as social media etc.
- The use of the internet for illicit financial transactions such as money-laundering.
- The bill also prohibits and criminalises the infringement of copyright. This then complements the Copyright Act of 1978.
- The bill criminalises the hiding or harbouring of persons who committed cybercrimes.
- The bill also gives powers to the law enforcement agencies and intelligence services to investigate cybercrimes, search, seize and access data or information of suspects and

cooperate with international bodies or foreign states in pursuit of fighting cybercrimes (Department of Justice and Correctional Services, 2017:41).

This means that, the South African security cluster involved in cybersecurity can share the information of citizens with foreign governments without the knowledge of the data subjects.

3.8.1 Establishment of 24/7 Point of contact and structures to deal with Cybercrimes

Cybercrimes can be committed from anywhere in the world. These crimes do not require the person committing them to be physically present in the country they are being committed. Moreover, cybercriminals can commit these crimes internationally and by masking their country of origin and their location, hence it becomes difficult to investigate these crimes. Cybercriminals are able to become anonymous on the internet. According to Moller (2018), cybercriminals mostly make use of fake identities, do not share their contact information and also hide their Internet Protocol (IP) addresses when committing these crimes and it thus becomes a serious challenge for law enforcement agencies attempting to investigate crimes of this nature. This also makes it difficult to link and identify cybercriminals or individuals to crimes or even cybersecurity threats and breaches.

Therefore, the bill recognises that cybercrimes are usually international in character and often difficult to investigate. Moreover, the bill states that cybercrimes should be investigated and efforts to stop them must be initiated immediately. This is because it is believed that the cybercriminals can be traced while they are still in the process of committing these crimes and before they have the time to destroy their online and digital footprint or to further destroy the evidence linking them to crimes (Department of Justice and Correctional Services, 2017:48). Realising the problem of investigating cybercrimes, the bill seeks to establish a 24/7 point of contact. The establishment of a 24/7 point of contact is to address the challenges of investigating cybercrimes, especially the ones that transcend borders. According to the bill, this point of contact will operate 24 hours a week to assist in ensuring that cybercrimes with an international dimension will be investigated. Moreover, this point of contact will liaise with countries across the globe and cooperate on issues of cybercrimes and cybersecurity that are of mutual interest (Parliament of South Africa, 2017:2).

While currently the 24/7 point of contact is not formally established and institutionalised, the bill calls for one to be established and a cabinet member will be appointed to oversee it. Moreover, the cabinet member will be charged with the responsibility of ensuring that the 24/7 point of contact is equipped, staffed, operational and maintained. It is also important to note that the bill calls for the cabinet member appointed to be in charge of the 24/7 point of contact be appointed from the Police Department and must thus have the experience and technical expertise in the

field of cybercrimes and cybersecurity (Department of Justice and Correctional Services, 2017:57). The 24/7 point of contact will further offer services such as: technical assistance and advice; legal information; identification and location of suspects of cybercrimes; and cooperating with foreign states with regards to issues of cybersecurity and cybercrimes.

Another structure to be established under bill is the Cybersecurity Response Committee (CRC). This structure will be responsible for coordinating and centralising all cybersecurity activities in South Africa (Sutherland, 2017:84). The bill also makes it clear that the CRC will be under the auspices of State Security Agency and also situated within SSA. Moreover, the CRC will be made up of senior representatives from various governmental departments of the country, the chairperson who will be the Director-General of SSA, and other experts from governmental departments. In addition, the CRC will be responsible cybersecurity policy of government i.e.: the National Cybersecurity Policy Framework of 2015. The Department of Justice and Correctional Services (2017:58), further points out that the functions and objectives of the CRC are to:

- “identify and prioritise areas of intervention;
- coordinate cyber security activities and be a central point of contact on all cybersecurity matters pertinent to national security;
- identify and prioritise areas of intervention and promote focussed attention and guidance where required regarding cyber security related threats and incidents;
- promote, guide and coordinate activities aimed at improving cyber security measures by all role players, which would include amongst others, the strengthening of intelligence collection and improve the state’s capacity to investigate, prosecute and combat cybercrime and to deal with cyber threats;
- oversee and guide the functioning of the 24/7 point of contact, the cybersecurity centre, Government Security Incident Response Teams, the National Cybercrime Centre, the Cyber Command, Cyber Security Hub and Private Sector Security Incident Response Teams established in the Republic;
- Be in charge of international cooperation initiatives” (Department of Justice and Correctional Service, 2017: 60).

Lastly, it is worth noting that, the SSA plays a prominent and integral role in the role of investigating cybercrimes and cybersecurity under the bill. The SSA, under this bill, will oversee and be in charge of all structures that are to be established in relation to cybercrimes and cybersecurity. Such structures include the aforementioned CRC, the 24/7 point of contact, Government Security Incident Response Teams, and the Cyber Command. However, clause 51 (10) of the bill also makes it clear that the SSA chairperson must provide a report on an annual

basis to the Joint Standing Committee on Intelligence. Such a report must provide an account of the progress the CRC has made and challenges with regard to cybercrimes and cybersecurity in the Republic (Department of Justice and Correctional Service, 2017:51). However, the reports and discussions of the Joint Standing Committee on Intelligence are secret and the public is likely to never know about the work of the CRC.

3.8.2 Conflict of the Bill with the Constitution

The Cybercrimes and Cybersecurity Bill seeks to enhance the security in cyberspace and also thwart cybercrimes in South Africa. However, the bill still has some sections that are not in line with the Constitution of the Republic. Among the problems noticed in the bill is Section 5 of the bill, which criminalises the unlawful and intentional interception of data or information (Department of Justice and Correctional Services. 2017:51). This section 5 of the bill does not take into account the operations of NCC which the Matthew Commission (2008), found was operating and intercepting communications (on a massive scale) despite that it was doing so outside the law. In fact, the bill does not make reference to the illegal interception carried out by the NCC under the command of the SSA (Right2Know, 2016:6). The bill further fails to highlight that, the NCC operates illegally and thus infringing on the right to privacy of the citizens and that it duplicates the work that is done by the OIC.

3.8.2.1 State centric approach to cybersecurity by the Bill

The current approach to cybersecurity under the bill is state-centric i.e. it approaches the problem of cybersecurity from a point of view that emphasises the security of the state as opposed to human security (Research ICT Africa, 2015:19). For example in the bill the CRC and the 24/7 point of contact all fall under the command of the SSA. Moreover, this approach is based on a hierarchical top-down approach with the intelligence at the top and centre of control with regard to cybersecurity. Such an approach gives an impression that the problem of cybersecurity affects only the state. Instead of having a multi-stakeholder and horizontal approach to cybersecurity that includes civil society, NGOs, and private companies working together with state institutions. The government is the only entity in charge of cybersecurity (Research ICT Africa, 2015). The problem with the state-centric approach with the SSA at the top is that: the SSA is an intelligence agency that mostly operates in secrecy. Therefore, approaching security from only an intelligence viewpoint does not guarantee openness, transparency, and certainly does not guarantee that constitutional rights of citizens will be respected, as we have already seen with the NCC under the command of the SSA.

Moreover, the bill further risks politicisation of issues of cybersecurity by placing the CRC under the leadership of a Director-General of the SSA who then reports to the Minister of State Security,

who is a political appointee (Department of Justice and Correctional Services, 2017:53). This is likely to undermine the regulatory independence and can easily lead to the abuse of powers invested in the CRC. In addition, the bill also confers too many powers onto the law enforcement agencies and intelligence services. For example, section 31 of the bill give the SAPS and SSA the powers to investigate, search, access, and seize any database, electronic device, and networks where such may be located without even obtaining a search warrant (Department of Justice and Correctional Services, 2017:52).

3.8.2.2 No express emphasis on the protection of the right to privacy

While cybersecurity is an issue that permeates all sectors of the society and government, the bill fails to expressly state how it will balance the right to privacy and cybersecurity (Department of Justice and Correctional Services, 2017:49). The bill further does not create an oversight body that will look into the work of the SSA and SAPS in investigating cybercrimes and enhancing cybersecurity. This is likely to become a serious problem as the security services can infringe on the rights of citizens and without ever having to account for the violations of the constitutional rights of citizens. The bill therefore, does not provide for the establishment of checks and balances when it comes to the investigations of cybercrimes and cybersecurity. The right to privacy is therefore not completely protected under the bill. The bill seems to put the constitutional rights of South Africa second to cybercrimes and cybersecurity (Research ICT Africa, 2015:24).

3.8.2.3 Sharing of information and entering into agreements with foreign states

The bill also allows for the country to enter into agreements with foreign governments contrary to what POPI Act states. While the POPI Act forbids the sharing of personal information with foreign entities, the bill makes it a possibility for South Africa to share information of individuals suspected of cybercrimes with foreign states (Department of Justice and Correctional Services, 2017:57). This then nullifies certain clauses of the POPI that forbid the sharing of personal information with other states. Moreover, under the bill, the person whose information is transferred to foreign states is never notified of such a transfer. This means that the state can obtain the most private information about a South African citizen and transfer it to other states (Research ICT Africa, 2015:24). This transfer of information to foreign governments under “agreements” does not guarantee how such information will be used, handled, or stored by the receiving state. In addition, there are no guarantees that the information transferred to other states by South Africa will be obtained legally and by paying attention to the right to privacy.

The intention for the enactment of the cybercrimes and cybersecurity bill is to combat cybercrimes and augment security in cyberspace within the country. However, the bill in its current form is problematic and is not aligned with the Constitution of the country. Rather, the bill approaches

cybersecurity from a state-centric view and thus pays no attention to issues pertaining to the right to privacy, protection of personal information, and the negative implication of putting SSA at the centre of this bill.

Table 3.1: Summary of the cybersecurity measures and their constitutionality

Name of legislation	Main aims	In line with the Constitution or not?
POPI Act	• To give effect to protect the right to privacy by safeguarding personal information • Regulate how personal information is collected, processed, stored, used and shared • To protect the rights of data subjects	This act is in line with the Constitution in terms of protecting the right to privacy. However, this chapter also exposed how the SSA has an MoU with the CIO which allows both intelligence services to share information on individuals, “rogue NGOs and Think Tanks.” This means this Act is being violated by SSA as it prohibits the transfer of personal information to foreign governments or entities. In addition, the POPI Act has not been enforced to protect the rights of citizens as the Information Regulator has failed to prosecute companies that were responsible for major data breaches in 2017 and 2018.
RICA	• To regulate the interception of communications • To give direction as to when communications can be intercepted and by which institution • To regulate the execution of directions and entry	• The RICA Act is not clear on the protection of the right to privacy and the oversight mechanism that will ensure that it is not open to abuse. This study has established that this act is being used by law

	warrants by law enforcement agencies	enforcement and intelligence services to violate and infringe on the individuals' right to privacy. The NCC is operating outside this Act.
ECT Act	To facilitate and regulate electronic communications and transactions in the interest of the South African public	The act is in line with the Constitution. However, certain aspects of the act are disadvantageous to IT experts, researchers, and ICT developers as it criminalises the development of electronic devices that can be used to breach computer networks' security.
Cybercrimes Bill	The bill seeks to combat cybercrimes and create a safe and secure cyberspace in South Africa.	- The bill is not in line with the Constitution. It gives too many powers to the SSA and SAPS without proper oversight. - The bill does not expressly state how it will balance combating crimes and protecting the constitutional rights of citizens such as the right to privacy. - It contradicts the POPI Act as it allows for the government to be able to transfer personal

		information of citizens to other countries. • It has been alleged that the government has been using Finfisher spyware to eavesdrop on certain citizens (DefenceWeb, 2015). • It approaches the issue of cybersecurity from a state-centric point.
--	--	--

3.9 CONCLUSION

As it was discussed in the introduction, this chapter addressed research objective 3 of this study. This chapter thus revealed that: South Africa has responded to cybersecurity challenges by enacting several laws over the years with the last measure being the proposed Cybercrimes and Cybersecurity Bill. These were envisioned to thwart cybersecurity threats and create a safe cyberspace in the country. However, as revealed in this chapter, these measures are open to abuse by the security cluster of the country. In addition, it is only the POPI Act that seeks to protect the right to privacy in definitive terms. Other laws are fraught with state-centrism and do not give enough attention to balancing the quest to create a safe and secure cyberspace with constitutional rights as enshrined in the Constitution of the country.

CHAPTER 4: RECOMMENDATIONS AND CONCLUSION - APPROPRIATE CYBERSECURITY REGULATIONS THAT CAN BE ALIGNED WITH THE CONSTITUTIONAL RIGHTS OF CITIZENS

4.1 INTRODUCTION

Chapter 4 concludes this research and aims to answer the primary research question of this study: “How can cybersecurity measures in South Africa be aligned to protect rather than to infringe on the constitutional rights of SA citizens?” In order to conclude the study, the theoretical context (see Chapter two) of cybersecurity in SA will firstly be explained and its implications discussed. This will form the basis to secondly examine and analyse the appropriate cybersecurity measures that can be aligned with the constitutional rights of South Africans. In summary, this chapter further provides an overview of the cybersecurity measures in a constitutional democracy of South Africa, how these measures impact the constitutional rights of the citizens, and how the governance of cybersecurity can be aligned with the constitutional rights of citizens while thwarting cybersecurity threats.

4.2 THE THEORETICAL CONTEXT OF CYBERSECURITY IN SOUTH AFRICA'S CONSTITUTIONAL DEMOCRACY

The growth and proliferation of ICT and the internet has brought with it numerous cybersecurity threats that confront all states across the globe. These threats affect both democratic and non-democratic states. As a result, governments have sought to respond to these cybersecurity threats by instituting a number of counter-measures to curb these threats. Nonetheless, the measures instituted by different governments are not the same. This due to the fact that their referent objects of security may differ in each state. The referent object of security as well as the system of governance influences how states approach cybersecurity. The system of governance of states and how they understand cybersecurity inform their approach to cybersecurity. The governance of cybersecurity is therefore approached differently in democratic and non-democratic states. For example, in non-democratic states, cybersecurity is seen as the threat to the state only and should be approached from a state-centric perspective. However, in the context of a constitutional democracy such as South Africa, the citizens are given rights by the Constitution. In addition, the Constitution of the country is rooted in the respect and protection of the constitutional rights of citizens. Therefore, the cybersecurity measures that the government proposes or institutes should reflect the resolve of the Constitution regarding the rights of citizens. This was described in section 2 of chapter 2.

However, while the South African government has four primary cybersecurity measures (as pointed out in chapter 3), these measures barely make reference to the importance of constitutional rights of citizens and how cybersecurity measures will likely impact on these rights. As given in section 2.3, the fundamental rights which could be affected by state security-centric cybermeasures, include *inter alia* (Constitution of the Republic of South Africa, 1996):

- the freedom of thought or expression - section 7(1) and section 16;
- infringement on being equal before the law - section 9(1);
- unfair discrimination as described - sections 9(3) and (4);
- infringement on human dignity and its right to be protected - section 10;
- infringement on personal privacy - section 14;
- infringement on religion, belief or opinion - section 15; and
- access to information – section 32.

Similarly, the government of South Africa has not provided any definitive guidelines on what measures will be put in place to ensure the protection of constitutional rights of citizens while instituting these cybersecurity measures (as was discussed in chapter 3). This problem is also compounded by the lack of a definition of cybersecurity in the context of South Africa. A proper definition of cybersecurity in the context of South Africa that takes into account the implications of cybersecurity measures for constitutional rights will assist in understanding the referent object of cybersecurity in the country. It is only through describing the referent object of cybersecurity in the context of the South African constitutional democracy that one can fully understand the meaning of cybersecurity. For now, as was discussed in chapters 2 and 3, the meaning of cybersecurity in SA has different meanings to different sectors within the security cluster such as the: military, civil society, the police, and associated politicians.

Furthermore, while the common understanding is that cybersecurity forms an important part of the security of the country, the government of South Africa needs to capture this in the cybersecurity measures of the country while not neglecting the Constitution and the protection of the rights of the citizens. This will assist in the alignment of cybersecurity measures with the constitutional rights of the citizens. As a country with a constitution that protects the rights of citizens, the cybersecurity measures should also give effect to the protection of the rights of citizens. Chapter 2 clearly pointed out that cybersecurity in South Africa should therefore be approached in such a way that it takes into account issues associated with democracy such as the right to privacy; freedom of expression; and the right to information.

4.2.1 Realism and cybersecurity measures and constitutional rights

Realism remains the most influential theory in both international relations and its sub-field of security studies. Realists believe that states are the primary actors in international politics and their foremost concern is their security and survival. As a result, states preoccupy themselves with issues of security and the achievement of their survival at all costs and by any means as described in section 2.2.1 of chapter 2. Therefore, the rising discourse around cybersecurity has captured the attention of governments and has thus been framed by statesmen and politicians as a serious threat to the security of the state and its survival. In addition, section 2.2.1 of chapter 2 also highlighted how cybersecurity and the governance of cyberspace are mostly driven by states as realists believe that states are the primary actors in issues concerning security.

The realist view of cybersecurity has largely influenced the drive by states to assume the upper hand in the race for dominance in the digital age as discussed in chapter 2 section 2.2.1. Moreover, since there is a heavy reliance on cyberspace and its related technologies by governments to run and provide services to their populations, the threats in cyberspace have become a priority for states. States fear that threats in cyberspace and insecurity in computer networks can undermine and threaten their security. These then justify the realists' perspective on cybersecurity that states must play a prominent role in ensuring a secure and safe cyberspace. However, the approach to cybersecurity by the state should be overseen by multiple stakeholders such as the parliament, the Public Protector, civil society and cybersecurity practitioners. That will ensure that cybersecurity measures are not used to violate the constitutional rights of citizens. Most importantly, there should be an inclusion of experts with cybersecurity skills to provide expertise on the field of cyber.

Realism also explains why states have to pursue cybersecurity measures to ensure the security within their respective territories. That is, if states fail to provide a safe and secure cyberspace then their legitimacy and authority will be questioned by their citizens. This is why South Africa has resorted to respond to cybersecurity issues by enacting a number of laws and measures to ensure cyberspace that is secure and safe as explained in section 2.2.1 in chapter 2 of this study. In addition, the anarchic nature of the international system, according to realists, forces states to rely on themselves with regards to cybersecurity. States know that there is no a central power or authority above them that can guarantee a safe and secure cyberspace for states.

In addition, realists believe in self-reliance. For example while cybersecurity transcends territorial borders and permeates all societies, states do not necessarily cooperate among themselves or go to international organisations to thwart cybersecurity threats. Rather, states have come to pursue their own unique and individual cybersecurity measures that are reflective of their

domestic cybersecurity understanding and priorities. This point was discussed in chapter 2 section 2.2.1.

4.2.1.1 Central theoretical statement and its application to the study

Given the assumption made by realists that states are primarily occupied with their security, section 5 of chapter 1 discussed and explained why the South African government has responded to cybersecurity threats by instituting a number of laws and legislations. These are four pieces of legislation that are discussed in chapter 3. These laws can be seen as a way by which the South African state ensures its own security. The government cannot rely on other states for ensuring its security, as realists believe. This point was made in section 5 of chapter 1. Moreover, given the anarchic nature of international relations and the distrust among states, matters that affect the security of the state such as cybersecurity, states have to pursue unilateral measures without cooperating with each other.

While the Constitution of the country guarantees the citizens rights pertaining to privacy, freedom of expression and the right to information, realism fails to take into account these rights. For example, realism explains why states are preoccupied with their survival and security but does not explain why the violation of and infringement on constitutional rights threatens the security of the citizens. Therefore, this study also proposes that, the realist-driven cybersecurity measures should be aligned with the constitutional rights of citizens. This is because, constitutional rights are as important as their security. Furthermore, the security in cyberspace should not be achieved at the expense of the constitutional rights of citizens.

4.3 CYBERSECURITY MEASURES IN SOUTH AFRICA THAT ARE NOT ALIGNED WITH CONSTITUTIONAL RIGHTS OF CITIZENS

Chapter 3 of this study discusses the cybersecurity measure that have been instituted and proposed in South Africa. There are currently three measures that are in place with the Cybersecurity and Cybercrimes Bill still in the process to be passed into law. These cybersecurity measures are:

- 1) the POPI Act
- 2) the ECT Act
- 3) RICA Act
- 4) the Cybersecurity and Cybercrimes Bill.

These are the measures that play a pivotal role in the understanding of cybersecurity measures in South Africa as discussed in chapter 3. Moreover, the measures were discussed in length and

were further assessed to see how they affect the constitutional rights of citizens as enshrined in the Constitution of South Africa.

Section 3.2 of chapter 3 discusses the constitutional rights of South African citizens in terms of privacy and how such rights protects the citizens from abuses of power and overreach by the state. The Bill of Rights in Chapter 2 of the South African Constitution plays an important role in the protection of citizens' rights and ensuring the right to privacy. Moreover, the right to privacy is further guaranteed by section 14 of the Constitution. The right to privacy is important as it also gives citizens the freedom to conduct their personal affairs without the interference of the state and public scrutiny. This point was made in chapter 3 section 3.2 In addition, the right to privacy also makes it easier for citizens to determine how their personal information is collected or shared. The right to privacy is the foundation of citizens' freedom and protection from the state to infringe on their personal and intimate affairs without their consent. This is also discussed in chapter 3 section 3.2.

Furthermore, the point was made in the same section of chapter 3 that, once the right of privacy is infringed, the dignity of the individual is also violated (see section 10 of the Constitution). As a result, the right to privacy of an individual also assists in the preservation of a person's dignity. Moreover, chapter 3 section 3.2 established that, the right to privacy also plays an integral part in enhancing an individual's spiritual, psychological, and physical well-being. In the same vein, it was discussed that, the right to privacy supports and reinforces other rights such as freedom of association, expression and information hence, it is important for a constitutional democracy like South Africa to guarantee such a precious right.

However, the right to privacy is not absolute and can be limited as Section 36 (1) of the South African Constitution states. The limitation of privacy, however, can only take place when there are reasonable grounds and justification to do so. This limitation must also be in the benefit of the society, constitutional order of the country, its democratic values and principles. This point is made in chapter 3 section 3.2 of this study. Chapter 3 section 3.2 also highlighted that, with the developments and advancements in ICT, the right to privacy becomes difficult to protect. Moreover, technological advancements have the ability to undermine the cybersecurity and the right to privacy. The following analyses how each one of the four cybersecurity measures is not aligned with the constitutional rights of citizens. This is done to sufficiently address the third research objective of this study. Moreover, the study will further provide recommendations on how these measures can be aligned with the constitutional rights of the citizens and the Constitution.

4.3.1 The POPI Act and constitutional rights

The main objective of this act was to ensure that the personal information of citizens is protected and safeguarded. The government acknowledged that the protection of the citizens' personal information is key to the fundamental right of citizens' right to privacy. As a result, the POPI Act is intended to make it very difficult to collect, process, utilise, and share personal information without people's express consent. This law then is important in the quest to protect the right to privacy of the citizens and regulates how their personal information can be collected and used. This is discussed in section 3.2 of chapter 3.

However, while the intended objective of the act is to protect the information relating to citizens and how it is collected, processed, stored, and used; the study has shown inconsistencies in the POPI Act and how it is applied. For example, the POPI Act states that personal information of individuals cannot be transferred to foreign governments or entities. However, the only problem is that, the act does not cover the transfer of personal information of individuals who are working for NGOs and NPOs. As a result, the intelligence services of South Africa can transfer such information to other foreign intelligence agencies. This was shown in section 3.2.2 of chapter 3. The secret MoU between SSA and CIO of Zimbabwe allows for the transfer and sharing of information about individuals working for "rogue" NGOs, NPOs, and Think-Tanks. The act therefore fails to address adequately issues concerning the secret transfer of personal information of individuals or even organisations that are called "rogue" by intelligence services. In addition, the intelligence services do not necessarily announce their agreements with foreign governments and disclose what type of information they share.

4.3.1.1 Aligning POPI with constitutional rights

The POPI Act does not address the issue of the intelligence services being able to secretly transfer personal information of persons or even organisations to foreign states as demonstrated by the MoU between SSA and CIO. Therefore, the POPI Act should be amended to forbid the transfer of personal or even organisational information by the intelligence services to foreign states. The transfer of such information is not done with the consent of the data subject as POPI requires and this constitutes an infringement on the right to privacy of the citizens. It is not known what the foreign state is likely to do with the information it receives under the secret sharing of information from the SSA. This practice then should be prohibited under the POPI Act and there must be strict enforcement of the Act especially pertaining to transfer of personal information to foreign states. This is how the POPI Act can be aligned with the constitutional rights of citizens.

4.3.2 The ECT and constitutional rights

The ECT Act's primary aim is to facilitate and regulate the electronic communications in the interest of the society of South Africa. It further deals with issues pertaining to the criminalisation of certain conduct in the cyberspace. Moreover, the act describes cybercrimes, creates cybercriminal offences, and prohibits the unauthorised accessing of data, the interference with data, and interception of data. This point is discussed in section 3.4 of chapter 3.

Moreover, section 3.4 of chapter 3 in this study details the cyber conduct and offenses under the act. It was pointed out in this same section that sections 86 and 89 of the act list and detail the criminal offenses and undesirable conduct in cyberspace. In addition, the study discusses the specific cybercrimes under the act. These cybercrimes include the following:

- The interception of data by unauthorised persons.
- The modification of information and data.
- The acts in cyberspace aimed at denying legitimate users of computers access to information and committing forgery, extortion and fraud.

While the aim of the ECT is clear, it is worth highlighting that, the act is likely to criminalise innovative acts of IT experts, practitioners and researchers. The act does not clearly define what constitutes 'undesired conduct' in cyberspace and the internet. Furthermore, people working in IT usually rely upon the testing of weaknesses and strengths in systems such as computers, viruses, malware, and software to innovate better ICT products that benefit society. Therefore, such acts could be deemed "undesired conduct" under the act and those involved could be prosecuted for criminal offences.

4.3.2.1 Aligning ECT with constitutional rights

The ECT Act is likely to criminalise innocent acts of innovation by citizens and accuse especially those involved in Research & Development or the ICT sector, of being involved in acts that constitute "undesirable conduct." Therefore, rather than using ambiguous language such as "undesirable conduct," the act should encourage innovation and research that is meant to better the security in cyberspace and not discourage innovation. It is within the rights of citizens to be involved in research and innovation that does not harm or undermine the security of computer networks and related activities. Therefore, the act should be revised to ensure that it does not discourage innovation, research and development in ICT sector.

4.3.3 The impact of RICA on SA's citizens constitutional rights

While the Constitution of South Africa protects the privacy of communications of the citizens, RICA was enacted to permit the interception, surveillance and monitoring of communication in the country. This act's primary objective is to assist law enforcement agencies in the fighting and prevention of crime. It further regulates the interception and monitoring of communications that take place in the private spaces of citizens. This point was discussed in section 3.3 of chapter 3. The RICA Act also has a broader and wider reach as it also applies to private spaces. Both direct and indirect communication can be intercepted and monitored under this act. Therefore, all forms of communications such as e-mails, text messages, intranet, internet, phone calls, texts, visual images, and data can be intercepted and monitored by intelligence and law enforcement agencies as discussed in chapter 3 section 3.3.

However, the interception and monitoring of peoples' communications can only take place upon the authorisation given to the intelligence services and law enforcement agencies by a designated RICA judge. Such an authorisation can only be granted by the judge on the basis of 'national security' or 'crime related grounds' and such a directive will be undertaken by the OIC as discussed in chapter 3 section 3.3. What is evidently lacking with the RICA mechanisms is that, the RICA Judge does not get to table the interception requests to any relevant Parliamentary Committee that will provide oversight on the requests for interception and the legal bases for the granting of interception authorisations. Therefore, such interception requests can be forwarded to the said Parliamentary Committee at least once or twice a year.

Importantly, the act also criminalises the usage of communications systems and networks that cannot be intercepted. As a result, ISPs and communications service providers are therefore compelled to assist the state in the interception of communications. The act further obliges the ISPs and communications service providers to store all communications-related data for a period of five years to ensure the monitoring and interception of communications. Lastly, the act compels cellphone users to register their SIM cards by providing ISPs and communications service providers with their identity numbers and residential addresses. This was discussed in chapter 3 section 3.2.

The RICA law as a cybersecurity measure presents a number of problems many of which impact negatively on constitutional rights of citizens. For instance, while the interception and monitoring of a person's communication should be authorised by the designated judge and reasonable grounds should be provided for such an interception to take place, the study in section 3.3.1.1 of chapter 3 has shown that intelligence services and law enforcement agencies can obtain such an interception directive from the judge under false pretences. Moreover, since the intelligence

services operate in secrecy, it will be difficult to know if they can be held accountable if they get interception authorisation under false grounds. RICA does not specify which skills and expertise the designated judge should have to occupy such a sensitive and key position that allows for the invasion and infringing on citizens' privacy. Moreover, this act does not make it mandatory for the parties seeking interception directives to return to the judge and provide feedback on the outcomes of the interception. This will allow the designated judge to reflect on the grounds that were provided to obtain the interception directive and to establish if the directive was based on reasonable and justifiable grounds. This was discussed in section 3.3.1.1 in chapter 3. Furthermore, the RICA Act denies the persons intercepted or monitored the chance to know about the interception of the communications, even after the interception did not connect the targeted persons to any wrongdoing. In fact, RICA denies the citizens the right for recourse and understanding of why their right to privacy was invaded as discussed in chapter 3 section 3.3.1.1. RICA places more responsibility and cost on ISPs and communications providers as it makes it their responsibility to ensure that their communications systems and networks must be able to be intercepted and monitored. Also, there is no evidence that the storage of users' meta-data and communications for the period of five years assists in the fight against crime.

Likewise, there are other key issues that impact on constitutional rights that are enabled by RICA. For example, RICA has established the OIC for the sole purpose of interception, monitoring and surveillance of communications in the country, the SSA also runs the NCC that is not regulated by law. The NCC has capabilities similar to the OIC, but is unregulated and operates outside the Constitution of the country. Therefore, this shows that the SSA is illegally operating an interception centre that is potentially spying and infringing on the privacy of citizens. The NCC duplicates the work done by OIC and goes unchecked as there are no laws regulating the NCC or an oversight structure to look at its operations. This point was discussed in section 3.3.1.2 in chapter 3.

Another important factor discussed is contained in section 3.3.1.3 chapter 3 regarding the indiscriminate and blanket retention of data. The mandatory retention of communications data of citizens placed on ISPs and communications service providers by RICA is problematic. This is because it requires the retention of communications data of all citizens without probable cause for a period of 5 years and there is no evidence that the retention of such data serves any purpose. This then makes no sense as it creates an impression that all citizens are treated like suspects based on the assumption that this information or data will assist the fighting of crime in the future. This retention of data is also not targeted at suspected individuals, but all citizens. It furthermore violates the right to privacy of citizens without reasonable grounds.

Section 3.3.1.4 in chapter 3 discusses the issue of the technological devices used to intercept, monitor and carry out surveillance on the citizens. It is not known what kind of technological

devices are being used for interception purposes by intelligence services and law enforcement agencies of South Africa. The RICA Act also does not specify which devices are illegal or legal to use when intercepting communication. Last but not least, the intrusiveness of such devices is not known and how they impact on the privacy of citizens.

4.3.3.1 Aligning RICA with the constitutional rights

Given the problems discussed above with regard to RICA and constitutional rights of citizens, it is of utmost importance to align RICA with the constitutional rights of South Africans. The first issue that needs to be addressed in order to align RICA with constitutional rights of citizens is the blanket and indiscriminate retention of meta-data that it places on ISPs and communications network providers. The retention of the most personal and intimate information for the period of up to five years is done without any reasonable grounds. Moreover, this retention of data has not been proven to help in the fighting and prevention of crime in South Africa. In fact, the cost of this retention burdens the ISPs and network providers. Furthermore, the retention of data infringes on and violates the constitutional rights of citizens as it is gathered for longer periods of time and there are no guarantees that such data can link one to crimes that were supposedly committed in the past. Stopping the retention of data for longer periods will ensure that constitutional right to privacy is respected and not violated.

Secondly, the NCC duplicates the work done by the OIC. Furthermore, this research (see Chapter 3) pointed out that, the NCC is not established under any law in the country. This makes the NCC an illegal and unlawful entity. Moreover, it is not known what type of data and information is being intercepted by the NCC on behalf of the SSA. One could therefore conclude that the NCC is being used illegally to spy on citizens without cause and outside the constitutional mandate of SSA. In addition, since the OIC only intercepts, monitors and conducts surveillance on persons who are under suspicion and based on the directive from the designated judge, the NCC does not follow such a procedure. This gives the NCC and SSA to leeway to violate and invade the constitutional right to privacy of citizens unabated and without oversight. The NCC should therefore be disbanded in order to ensure alignment of constitutional rights with RICA.

On another note, RICA does not allow the communications networks providers, ISPs and the courts to disclose to the citizens or individuals about the interception of their communications even after such an interception was not successful or did not connect them to a crime or wrongdoing. In essence, this RICA law denies the citizens their constitutional right to find a legal recourse or redress in case their right to privacy was wrongfully violated. As a result, RICA should be aligned and reviewed in order to allow citizens to find out what the reasons were for their

communications to be intercepted. Moreover, this can allow citizens to have confidence in the cybersecurity measures of the country and to hold those responsible for cybersecurity to account.

4.3.4 Cybercrimes and Cybersecurity Bill and constitutional rights

The Cybercrimes and Cybersecurity Bill in South Africa was introduced with the aim of ensuring the integrated and coherent cybersecurity legal framework for the country in 2015 and was the brainchild of the Department of Justice and Constitutional Development as stated in chapter 3 section 3.5 of this study. Moreover, the same section of chapter 3 also details the objectives of the bill. Section 3.6.1 of chapter 3 discussed the financial and personal information as well as data related offences. The aim of these offences was stated in the bill as to protect citizens, government and businesses from financial, data and personal information theft by criminal groups and individuals in cyberspace. The bill is also not aligned with the constitutional rights of citizens. There is a number of problems with the Cybercrimes and Cybersecurity Bill. These problems are discussed below.

The first problem that was pointed out of the bill is its state-centric approach to security. The bill and its language emphasise the security of the state and not that of the citizens of South Africa or the constitutional rights of citizens in relations to cybersecurity. Additionally, the structures to deal with issues of cybersecurity fall within the command of SSA. This is a serious concern as the SSA operates clandestinely and is barely subjected to transparency, accountability and openness. The National Cybersecurity Advisory Council (NCAC) is also rather dysfunctional in that it is mostly composed of lawyers arather than with people who have the technical expertise in the filed of cybersecurity. This is because, cybersecurity is a specialised field that is technical in nature. Therefore, the NCAC should be composed of more technical persons as compared to more lawyers.

Secondly, there is a risk of politicisation of cybersecurity as the chairperson of the CRC and 24/7 point of contact will report to the Minister of SSA, who is a political appointee. In addition, the bill gives many powers to the security cluster (with limited or no knowledge of the implications this bill has on constitutional rights), also civilian control is limited. Therefore, this bill needs to be reviewed in order to align it with constitutional rights of citizens.

The other problem worth noting, is the issue of not mentioning exactly what will be done with regard to the protection of the right to privacy in the bill. The bill does not state in definitive terms how the protection of the right to privacy in the quest to protect the cyberspace of South Africa will be effected. Rights of citizens are mostly violated in an environment where the intelligence services are in charge of a sensitive issue such as cybersecurity. There is no a single structure

that is set-up under the bill to ensure that constitutional rights of citizens will be adhered to and protected by the structures that will be implementing the bill.

4.3.4.1 Aligning the Cybercrimes and Cybersecurity Bill with constitutional rights

In order to ensure the alignment of the Cybercrimes and Cybersecurity Bill with the constitutional rights, there is a need to review the entire bill. Most importantly, the bill should be reviewed to include an independent and neutral body such as the South African Human Rights Commission (SAHRC) to provide oversight on matters of cybersecurity that impact on constitutional rights of citizens. The bill is currently under the full command of SSA. As it was highlighted in the previous sections, the SSA is operating in secret and away from public scrutiny. Therefore, it should have civilian oversight such as the SAHRC to observe and ensure the adherence to, respect of, and protection of constitutional rights in its work to ensure cybersecurity environment in the country.

Secondly, the state-centric approach to cybersecurity by the bill is disconcerting. Cyber threats are a country-wide problem that does not only affect the state but also the constitutional rights of citizens. Therefore, the role of the state security apparatus should also involve civil society, human rights groups, businesses and research institutions. This will help align the cybersecurity measures such as the bill with constitutional rights of citizens and other concerns of the society at large. Moreover, government will also stand a good chance of using such a diversity of actors in cybersecurity to implement best practices that may assist in creating a cybersecurity environment that is mindful and protective of constitutional rights.

It is important to highlight that, this bill has been drastically revised and amended by the Department of Justice and Constitutional Development and the Portfolio Committee for Justice and Correctional Services accepted the bill on 23 October 2018. The bill now is called the 'Cybercrimes Bill' and the cybersecurity part of the bill has been removed in its entirety (Cybercrimes Bill, 2018). This is a positive step because, as noted previously, the cybercrimes and cybersecurity bill was met with criticism with regard to the protection of constitutional rights of citizens and the broad and overreaching nature of it. As a result, the Department of Justice and Constitutional Development removed the cybersecurity part of the bill and adopted the cybercrimes part of the bill (Cybercrimes Bill, 2018).

4.4 GENERAL RECOMMENDATIONS

The primary research question of this study is stated in chapter 1 as follows: *"How can cybersecurity measures in South Africa be aligned to protect rather than to infringe on the constitutional rights of SA citizens?"* The section above highlighted the cybersecurity measures that are not aligned with constitutional rights of citizens and provided ways on how each

cybersecurity measure can be aligned with constitutional rights of citizens. Moreover, this study proposes the following general recommendations to complement the alignment of the cybersecurity measures in South Africa with the constitutional rights of citizens:

- The government should clearly define what cybersecurity entails in the context of South Africa and how it intends to implement it.
- South African government should clarify the ambiguous, vague, and broad language used when describing cybersecurity measures so as to avoid broad interpretation by different sectors involved in the regulation and governance of cybersecurity in the country.
- Should ensure that cybersecurity measures in South Africa are balanced with the constitutional rights of citizens.
- The approach to cybersecurity in South Africa should be more human-centric security as opposed to the current state-centric approach that entrenches more power to state security apparatus. Cybersecurity threats and cybercrimes do not affect only the state, but citizens also. Therefore, the approach of the state should reflect this point.
- Cybersecurity measures should be reviewed and revised to ensure alignment with the constitutional rights of citizens.
- RICA should be reviewed in order to avoid the unnecessary retention of data. This is because there is no concrete evidence of how the retention of communications data for up to five years helps in fighting crime and contributes to a safe and secure cyberspace.
- The designated judge should be a person with the technical knowledge and expertise of how interception, monitoring, and surveillance of communications work as RICA intends.
- RICA should also provide the citizens with recourse in the instance that their communications were intercepted without valid and credible reasons.
- The establishment of the NCC is not constitutional, that makes it illegal and unlawful. The government should therefore disband the NCC and its work. While this is the job of the Parliament, this matter should be brought before the Constitutional Court, Parliament, the Public Protector or the Office of the Inspector General of Intelligence by members of the public and civil society. The interception, monitoring, and surveillance of communications should be left to the OIC.

- Empowered, open, accountable, and transparent oversight structures should be instituted that will overlook the interception of communications by the security services.
- Cybersecurity matters should not be left to fall entirely within the purview of the SSA.
- The South African Human Rights Commission should be part of the CRC and the 24/7 point of contact to ensure that constitutional rights are fully observed and respected in the implementation and maintenance of cybersecurity measures in South Africa.

4.5 CONCLUSION

Cybersecurity measures are the government's way of seeking to address cyber threats and create a safe and secure cyberspace in South Africa. However, not much attention has been given to how cybersecurity measures can threaten the most fundamental values and rights of South African citizens. The state seems to have developed several pieces of legislation which protects the state from threats instead of understanding that these measures should be in line with the rights of its citizens too. Several examples were provided where these cybersecurity measures as spelled out in legislation could contravene the rights as given in the South African Constitution. It was mainly recommended to review these pieces of legislation to also protect the consumers and citizens of South Africa. Furthermore, this chapter highlighted how easy it was for the intelligence services to use cybersecurity measures to illegally infringe upon constitutional rights. It is an important undertaking for the SA government to ensure that appropriate steps are taken to align the cybersecurity measures with the constitutional rights of its citizens. Ultimately, the approach to cybersecurity should be balanced with constitutional rights of citizens in South Africa and the threats identified to both the state and its citizens.

5. BIBLIOGRAPHY

Al Jazeera. 2015. Spy cables: Greenpeace among intelligence targets. <https://www.aljazeera.com/news/2015/02/spy-cables-greenpeace-intelligence-targets-150224115107221.html> Date of access: 07 Oct. 2018.

Akande, A.O. & Van Belle, J. 2016. ICT Adoption in South Africa: opportunities, challenges and implications for national development. <https://www.researchgate.net/publication/285593353> Date of access: 04 Mar.2017.

Association for Progressive Communications. 2016. The Right to Privacy in South Africa. Submission in advance of the consideration of the periodic report of South Africa, Human Rights Committee, 116th Session .7 – 31 March 2016. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fICO%2fZAF%2f20241&Lang=en Date of access: 04. May.2017.

Bawa, N. n.d. The regulation of the interception of communications and provision of communication relation information act. www.thornton.co.za Date of access: 17 jul. 2018.

Bailes, A. 2006. Private sector, public security. (In Bryden, A., & Caparini, M., eds. Private actors and security governance. Berlin: Lit Verlag.

Beida, D. and Halawi, L. 2015. Cyberspace: an avenue for terrorism. *Issues in Information Systems*. 16 (3): 33-42.

Bellamy, R. 2013. Constitutional democracy. (In Gibbons, M.T., ed. The encyclopedia of political thought). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2272188 Date of access: 03 Aug. 2018.

Berg, B.L. 2001. Qualitative Research Methods for the Social Sciences. 4th ed. USA: Allyn & Bacon.

Brunner, E. & Suter, M. 2008. The international CIIP handbook 2008: An Inventory of Protection Policies in 25 Countries and 6 International Organizations. Zurich: Center for Security Studies.

Bryman, A. 2001. A social research methods. New York: Oxford University press.

Burchill, S. & Linklater, A. 1996. *Theories of International Relations*. London: MacMillan Press Ltd.

Buzan, B. 1991. *People, states, and fear: an agenda for international security studies in the post-cold war era*, 2nd ed. Brighton: Harvester Wheatsheaf.
<http://press.ecpr.eu/documents/sampleChapters/9780955248818.pdf> Date of access: 17 Aug. 2018.

Cassim, F. 2012. Addressing the spectre of cyber terrorism: a comparative perspective. *Potchefstroom Electronic Law Journal*, 15 (2).
<https://journals.assaf.org.za/index.php/per/article/view/2494/2238> Date of access: 20 Oct. 2018.

Cavelty, M.D. 2012. *Cyber-Security*. (In Collins, A., ed. *contemporary security studies* 4th ed. UK: Oxford University Press.

Cavelty, M.D & Mauer, V. 2010. *The routledge handbook of security studies*. New York: Routledge.

Cawthra, G., ed. 2009. *African security governance: emerging issues*. Johannesburg: Wits University Press.

Chauke, A. 2012. Exclusive: inside the R42 heist. <https://www.timeslive.co.za/news/south-africa/2012-02-10-exclusive-inside-the-r42m-heist/> Date of access: 21 Apr. 2018.

Choucri, N. 2000. Introduction: cyberpolitics in international relations', *International Political Science Review*, 21(3): 243–63.

<https://flavioufabr.files.wordpress.com/2017/02/cyberpolitics-and-international-relations.pdf> Date of access: 08 Jul. 2018.

Collins, A. 2007. *Contemporary Security Studies*. New York: Oxford University Press.

Collins, A. 2012. *Contemporary Security Studies* 3rd ed. New York: Oxford University Press.

Cronje, F. and Taylor, D. 2014. *Questions and answers about the Protection of Personal Information Act*. Cape Town: Juta.

Cwele, S. 2014. Cybersecurity meeting, Johannesburg 27 March 2014. Johannesburg: Government Printers.

Daily Maverick. 2018. Cybercrimes Bill defanged, but our privacy rights are still not secured. *Daily Maverick*, 21 Dec. <https://www.dailymaverick.co.za/article/2018-12-21-cybercrimes-bill-defanged-but-our-privacy-rights-are-still-not-secured/> Date of access: 12 Feb. 2019.

Davies, N.1996. Europe: a history. UK: Oxford University Press.

De Bruyn, M. 2014. The Protection of Personal Information Act – Impact on South Africa. *International Business and Economics Research Journal*,13(16).

Defence Web. 2015. US intelligence analyst thinks SA government likely spying on citizens. *Defence Web*, 22 Jul. <https://www.defenceweb.co.za/security/national-security-security/us-intelligence-analyst-thinks-sa-government-likely-spying-on-citizens/> Date of access: 12 Feb. 2019.

Department of Justice and Correctional Services. 2017. *Cybercrimes and Cybersecurity Bill*. Pretoria.

De Stadler, E. & Esselaar, P. 2015. A guide to the Protection of Personal Information Act. Cape Town. Juta.

Dlamini, C.R.M. Equality or justice? Section 9 of the Constitution revisited — Part I. *Journal of Juridical Sciences*, 27(1):14-40.

Foster, W. & Goodman, S. E. The diffusion of the internet in China. Center for International Security and Cooperation. Stanford University: USA. https://www.researchgate.net/publication/24090454_The_Internet_in_India_and_China Date of access: 13 Sep. 2018.

Goldstein, J. S. & Pevehouse, J. C. 2009. International Relations. 8th ed. New York: Addison Wesley Longman.

Griffiths, J.L. 2017. Cybersecurity as an emerging challenge to South African national security. Pretoria: UP. (Mini dissertation-Masters). <https://repository.up.ac.za/handle/2263/62639> Date of access: 07 Jun. 2017.

Hart, C., Jin, D.Y., & Feeberg, A. 2014. The insecurity of innovation: a critical analysis of cybersecurity in the United States. *International Journal of Communication*, 8:2860–2878.

Hosken, G. 2014. Gautrain heist foiled. <http://www.timeslive.co.za/thetimes/2014/11/13/gautrain-heist-foiled> Date of access: 03 May. 2018.

Huysmans, K. 1995. Migrants as a security problem: dangers of “Securitizing” societal issues. (In Robert. M & Dietrich, T., eds. *Migration and European intergration: the dynamics of inclusion and exclusion*. London: Pinter.

Internet World Stats. 2013. Internet Usage Statistics for Africa. <http://www.internetworldstats.com/stats1.htm> Date of access: 04 Mar.2017.

Internet World Stats. 2017. Internet Usage Statistics for Africa. <http://www.internetworldstats.com/stats1.htm> Date of access: 24 .Apr.2017.

Jackson, R. & Sorensen, G. 2007. Introduction to international relations: theories and approaches. New York: Oxford Press.

Kaiser, R. 2015. The birth of cyberwar. *Political Geography*, 46:11-20.

Kiboi, B.N. 2015. Cyber security as an emerging threat to Kenya’s national security. Pretoria: UP. (Mini Dissertation-Masters).

Kalathil, S. & Boas, T.C. 2001. The internet and state control in authoritarian regimes: China, Cuba, and the counterrevolution. Washington D.C.: Carnegie Endowment for International Peace.

Krickeberg, M. 2015. The internet as a slippery object of state security: the problem of physical border insensitivity, anonymity and global interconnectedness. *Interstate-Journal of International Affairs*, 2015/2016(2).

<http://www.inquiriesjournal.com/articles/1344/2/the-internet-as-a-slippery-object-of-state-security-the-problem-of-physical-border-insensitivity-anonymity-and-global-interconnectedness>

Date of access: 17 Apr. 2018.

Lee, C. 1990. *Voices of China: The Interplay of Politics and Journalism*. New York: Guilford Pres.

Leedy, P. D. & Ormrod, J.E. 2010. Practical research: planning and design. 9th ed. Boston: Kevin M. Davis.

Luck, R. 2014. POPI- is South Africa keeping up with international trends? <http://www.derebus.org.za/popi-south-africa-keeping-international-trends/> Date of access: 10 Jun. 2018.

Mail & Guardian. 2013. Spy wars: South Africa is not innocent. *Mail & Guardian*, 21 Jun. <http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent> Date of access: 5 May. 2017.

Mail and Guardian. 2015. Say nothing – the spooks are listening. *Mail & Guardian*. <https://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening> Date of access: 11 Oct. 2018.

Malinowski, T. 2001. China's Willing Censors. *The Washington Post*, 20 Apr. https://www.washingtonpost.com/archive/opinions/2001/04/20/chinas-willing-censors/b15896bd-b85c-47ab-9b1a-7cea857ae955/?noredirect=on&utm_term=.d8b2cb8d0298 Date of Access: 13 Sep. 2018.

Mcnabb, D.E. 2004. Research methods for Political Science: Quantitative and Qualitative Methods. New York: M.E. Sharpe.

Moeng, B. 2011. 9 Reasons to Invest In African ICT. IT News Africa, 14 September.

Mokhele, I. & De Beer, K.J. 2007. The Use of Information and communication technology (ICT) in e-service delivery and effective governance in South Africa. *Interim*, 6 (2): 60-67.

Moller, F. 2018. Challenges during the investigation of cybercrime. Risk Diversion. Pretoria. https://www.google.co.za/search?hl=en&source=hp&ei=HjmrW47II8i6swH8ipmACg&q=the+difficulty+of+investigating+cybercrimes+&og=the+difficulty+of+investigating+cybercrimes+&gs_l=psy-ab.3...1270.14178.0.15219.43.37.0.5.5.0.364.5822.2-22j2.24.0....0...1c.1.64.psy-ab..14.25.4760...0j0i131k1j0i22i30k1j33i160k1j33i22i29i30k1j33i22i10i29i30k1j33i10i21k1.0.76w5kX3-E0k Date of access: 26 Sep. 2018.

Moor, J.M. 1997. Towards a theory of privacy in the information age. Computers and Society. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.224.4731&rep=rep1&type=pdf> Date of access: 09 Oct. 2018.

Morgenthau, H.J. 1965. Scientific Man versus Power Politics. Chicago: Phoenix Books.

Morgenthau, H.J. 1985. Politics among Nations: The Struggle for Power and Peace 6th ed. New York: Knopf.

Mouton, W. 2000. Social research methods. South Africa: Oxford University Press.

Mutula, S.M. 2010. Challenges and opportunities of e-government in South Africa. The Electronic Library 28 (1): 38-53.

Neethling, J. Potgieter, J. M. & Visser, P. J., 2005. Neethling's Law of Personality. Durban: Butterworths.

Norris, P. 2001. Digital divide: civic engagement, information poverty, and the internet worldwide. Cambridge: Cambridge University Press.

Norton Rose Fulbright. 2014. Protection of Personal Information Act: Ten things to know. <http://www.nortonrosefulbright.com/files/za-popi-ten-things-to-know-119577.pdf> Date of access: 17 Jun. 2018.

Norton. 2013. Report. http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf Date of access: 21 Apr.2017.

Nye, J.S. 2011. The future of power. New York: Public Affairs.

NWU (North-West University). 2010. Manual for postgraduate studies. <http://library.nwu.ac.za/files/files/documents/quoting-sources.pdf> Date of access: 27 May.2017.

Office of the Privacy Commissioner of Canada. 2014. Privacy and Cyber Security: Emphasizing privacy protection in cyber security activities. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/ Date of access: 05 May. 2018.

Ogundiya, S.I. 2010. Democracy and good governance: Nigeria's dilemma. *African Journal of Political Science and International Relations*, 4(6): 201 – 208. https://www.academicjournals.org/article/article1381834964_Ogundiya.pdf Date of access: 04 Aug. 2018.

Open Democracy Advice Centre. 2018. What you need to know about the information regulator. <https://www.opendemocracy.org.za/index.php/blog/177-what-you-need-to-know-about-the-information-regulator> Date of access: 10 Oct. 2018.

Orb, A., Eisenhauer, L., & Wynaden, D. 2001. Ethics in qualitative research. *Journal of Nursing Scholarship*, First quarter:93-96.

Paalman, M. 2013. The Copenhagen school in the fifth domain: successful securitising the cyberspace? Uppsala: Uppsala Universitet. (Thesis-Masters).

Panda Security. 2018. Panda Cybersecurity Report 2017: Africa in top 10 targeted regions. <https://www.itweb.co.za/content/zKWEBby4ZNqmRiO> Date of access: 11 Feb. 2019.

Parliament of South Africa. 2017. Cybercrimes and Security in Committee's Spotlight. Cape Town.

Phahlamohlaka, L.I, Van Vuuren, J.C. & Coetzee A.J. 2011. Cybersecurity awareness toolkit for national security: an approach to South Africa's cybersecurity policy Implementation. Paper presented at the Southern African Cyber Security Awareness Workshop (SACSAW) 2011.

Porteus, L. 2001. 'Feds still need to define role in tackling cyberterror, panellists say', GovExec.com, 15 May 2001. <http://www.govexec.com/dailyfed/0501/051501td.htm> Date of access: 07 Feb. 2018.

Poulsen, K. 1999. Info war or electronic sabre rattling? *ZDNet*, 8 Sep. <http://zdnet.com.com/2100-11-515631.html?legacy=zdn> Date of access: 03 Aug. 2018.

Research ICT Africa. 2012. Understanding what is happening in ICT in South Africa: Evidence for ICT Policy Action. *Policy Paper 7*, 2012.

Research ICT Africa. 2015. Submission on the Cybercrime and Cybersecurity Bill. https://www.researchictafrica.net/publications/Other_publications/2015_RIA_Submission_to_Cybersecurity_and_Cybercrime_Draft_Bill.pdf Date of access: 20 Jul.2018.

Roane, B. 2013. SAPS website hacked. <https://www.iol.co.za/news/saps-website-hacked-1520042#.VHrpBdKUdwo> Date of access: 05 May. 2018.

Right2Know. 2016. The Surveillance State: communications surveillance and privacy in South Africa. Cape Town: Media Policy and Democracy Project.

Rigoglioso, M. 2014. Civil liberties and law in the era of surveillance. *Stanford Lawyer*. 91.

SAMENA. 2014. This is what South Africa's internet actually looks like. http://www.samenacouncil.org/samena_daily_news.php?news=43974 Date of access: 11 Mar. 2017.

Sapa. 2015. Spy cables: Threats of cybersecurity against SA banks. <http://www.enca.com/south-africa/spy-cables-threats-cyberattack-sa-banks> Date of access: 04 May. 2018.

Schultz, C.B. 2017. Cybercrime: an analysis of the current legislation in South Africa. Pretoria: UP. (Mini dissertation-Masters). https://repository.up.ac.za/bitstream/handle/2263/60091/Schultz_Cybercrime_2017.pdf?sequence=1&isAllowed=y Date of access: 16 Jul. 2018.

Scott, G.1999. Controlling the state: constitutionalism from ancient Anthems to today. London: Harvard University Press.

Singel, R. 2008. Report: government's cybersecurity plan is riddled with new spying programs. *Wired*, 15 May. Threat level. <https://www.wired.com/2008/05/senate-report-g/> Date of access: 01 Aug. 2018.

South Africa. 1996. Constitution of the Republic of South Africa, 1996.

South Africa. 2002. Electronic Communications and Transactions Act 25 of 2002.

South Africa. 2002 Regulation of Interception of Communications and Provision of Communications Act 70 of 2002.

South Africa. 2013. Protection of Personal Information Act 03 of 2013.

South Africa. 2015. National Cybersecurity Framework for South Africa. Government Gazette, 39475, 4 Dec. http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf Date of access: 17 Apr. 2017.

South Africa. 2017. Medium Term Strategic Framework 2014-2019. https://www.gov.za/sites/default/files/gcis_document/201409/mtsf2014-2019.pdf Date of access: 12 Feb. 2019.

South Africa. Ministerial Review Commission on Intelligence. 2008. Mathews Commission Report.

South Africa. 2012. National Development Plan 2030: Our future – make it work. 2012: 189 <http://www.nationalplanningcommission.org.za/Pages/NDP.aspx> Date of access: 03 Mar. 2017.

South Africa. Statistics South Africa. 2015. Information and Communication Technology satellite account for South Africa. Pretoria: StatsSA.

South Africa. State Security Agency. 2014. Minister Siyabonga Cwele: Minister of State Security, Republic of South Africa. Cyber Security Meeting, Johannesburg 27 March 2014.

South Africa. State Security Agency. 2016. State Security Agency Department Budget Vote 2016/17. Parliament of Republic of South Africa, Cape Town. <http://www.gov.za/speeches/minister-david-mahlobo-state-security-agency-dept-budget-vote-201617-26-apr-2016-0000> Date of access: 03 Mar. 2017.

State Security Agency. 2015. The National Cybersecurity Policy Framework (NCPF). Government Gazette (39475). https://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf Date of access: 23 Oct. 2017.

Steiner, W. 2013. Justifying limitations on privacy: the influence of the Proportionality test in South African and German Law. Cape Town: University of Cape Town. (Mini dissertation- LL.M.).

Sunday Times. 2013. Spy cops illegally tapped journalists' phones, police find. <https://www.pressreader.com/southafrica/sundaytimes/20130818/284747744174365> Date of access: 13 Oct. 2018.

Sutherland, E. 2017. Governance of cybersecurity – the case of South Africa. *The*

African Journal of Information and Communication. 20:83-112.

<https://doi.org/10.23962/10539/23574> Date of access: 24 Jun. 2018.

Suttner, R. 2014. Popular power, constitutional democracy and crisis: South Africa 1994-2014. *Strategic Review for Southern Africa*.36(2).
[https://www.up.ac.za/media/shared/85/Strategic%20Review/Vol36\(2\)/05-suttner-pp-7-30.zp39576.pdf](https://www.up.ac.za/media/shared/85/Strategic%20Review/Vol36(2)/05-suttner-pp-7-30.zp39576.pdf) Date of access: 20 Jun. 2018.

Swart, H. 2016. Communications surveillance by the South African Intelligence Services.
https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf Date of access: 17 Jul. 2017.

Swales, L. 2016. 'Protection of Persona l Information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (SPAM)' 28. *SA MERC*, 61.

Tully, J.1995. *Strange multiplicity: constitutionalism in the age of diversity*. Cambridge: Cambridge University Press.

UN Office on Drugs and Crime. 2013. Comprehensive study on cybercrime.
http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf Date of access: 03 Mar. 2017.

United Nations Educational, Scientific and Cultural Organization. 2002. Information and Communication Technology in Education: a curriculum for schools and programme of teacher development. <http://unesdoc.unesco.org/images/0012/001295/129538e.pdf> Date of access: 12 Sep. 2018.

Van der Bank, C.M. 2012. The right to privacy – South African and comparative perspectives. *European Journal of Business and Social Sciences*, 1(6):77-86.

Van der Merwe, D.P. et al. 2016. *Information Communications Technology Law*.2nd ed. LexisNexis.

Van Niekerk, B. 2017. An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, 20:113-132.

Venter, A & Landsberg, C. 2006. Government and politics in the new South Africa. Pretoria: Van Schaik Publishers.

Waltz, K. N. 1979. Theory of international politics. London: Addison- Wesley.

Webb, E.J., Campbell, D.T, Schwartz, R.D., Sechrest, L., & Gove, J.B. 1981. Normative measures in the social sciences. Boston: Houghton Mifflin.

Welman, C., & Kruger, F. 2005. Research methodology. 3rd ed. Cape Town: Oxford University Press.

Williams, P.D. 2008. Security studies: an introduction. New York: Routledge.

Wohlforth, William C. 2011. Gilpinian Realism and International Relations. *International Relations* 25(4): 499–511.

6. ADDENDUMS: LETTERS FROM LANGUAGE EDITORS



To whom it may concern

I hereby declare that I contributed to the language editing of the mini thesis of Mr D.M. Molwantwa in my capacity as interpreter at the NWU.

Regards

A handwritten signature in black ink, appearing to read 'A. Oelofse', written over a horizontal line.

Annarie Oelofse