CYBERCRIME AS A THREAT TO THE SOUTHERN AFRICAN DEVELOPMENT COMMUNITY (SADC) MAINTENANCE OF PEACE AND SECURITY: THE CASE OF ZIMBABWE (2016-2018)

BY

ABIGAIL NCUBE

R075481T

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN INTERNATIONAL RELATIONS

DEPARTMENT OF POLITICS AND ADMINISTRATIVE STUDIES

FACULTY OF SOCIAL STUDIES

UNIVERSITY OF ZIMBABWE

APRIL 2018

DEDICATION

This dissertation is dedicated to my son Zolile Prosper Mabuya. Young as he is, he has been by my side throughout my studies. His belief in me motivated me, it gave me reason to fight on and that, is much appreciated.

Furthermore, heartfelt gratitude goes to all my sisters, Adelaide Ncube, Cassandra Ngwenya and Viola Jowa. Thank you very much for stepping up to being mum to Zolile when the going got tough, I truly appreciate. Thank you very much

ACKNOWLEDGEMENT

I would like to acknowledge my supervisor Doctor Solomon Muqayi for his patience, intelligence and wisdom which was indispensable in this research project. Thank you very much.

To my mother Mrs Sibongile Ncube, many thanks for the support you gave during my studies mum, you encouraged me to soldier on and for that I give thanks.

Not forgetting my friend Sibusiso Tshuma, I could never thank you enough for your support during my studies, I am truly grateful. Lastly, I give thanks to everyone who contributed to my studies; your contributions are much appreciated.

ACRONYMS

CIO	Central Intelligence Organization
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
ICTs	Information Communication Technology
EU	European Union
SADC	Southern African Development Community
CERT	Computer Emergency Response Team
ECU	Electronic Crime Unit
ZRP	Zimbabwe Republic Police
ITU	International Telecommunications Union
HIPSSA	Harmonized Cyber Security Legal Framework
CRASA	Communications Regulatory Authority of Southern Africa
HIT	Harare Institute of Technology
GISP	Government Internet Service Provider
MISA	Media Institute of Southern Africa
RBZ	Reserve Bank of Zimbabwe

ABSTRACT

This study focuses on the roles both SADC and Zimbabwe play in curbing cybercrime and ensuring cyber security within the SADC region and in Zimbabwe specifically. Emphasis is placed on the importance of Cyber security in the maintenance of peace and security within SADC as it can be used to dethrone regimes thus causing instability within the region. Emphasis is given to Zimbabwe which is the case study for this research as it is seen to be trailing behind in issues of cyber security. The study also gives a background to cyber-crime, its evolution and the types of cyber-crime that are prevalent in SADC and Zimbabwe too. In ascertaining the role played by cyber-crime, this study made use of the qualitative research methods with particular emphasis on in depth interviews and documentary research. Using the above mentioned methods this study established that cyber-crime is an area that is not being accorded much attention by the Zimbabwean Government although there are efforts now to try and catch up with the rest of the world in ensuring cyber security. This is evidenced by the draft Bills that Parliament will soon be pass into law. The relevant Ministries are teaming up and coming up with a work-plan to be used in curbing cyber-crime in the country. It is important to note the expenses associated with cyber security, the equipment needed for the security arm to be fully functional is quiet pricey thus forwarding a challenge for the Zimbabwean Government which is already operating on a very slim budget. It was therefore recommended that the Zimbabwean Government prioritize cyber security as cyber-crime poses threats not only to individuals but to the Government as well. This study suggests that the budget for the Ministry of ICT and Cyber security be increased to cater for these activities.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION AND BACKGROUND TO THE STUDY

1.1 Background of the Study

Security and protection of individual against the fast growing dangers of the cybercrime remain one of the major challenges facing cyber security experts, scholars and politicians (SAPS, 2011: 18). As such, cybercrime is on the rise and it has more devastating effects in the international system like that of war, terrorism and climate change (SAPS, 2011: 23). The rise of cybercrime is a result of increased bandwidth and the proliferation of Information Communication Technology (ICT) that has widened the use of the internet.

In Africa, the International Telecommunications Union (ITU, 2013) estimates that the number of subscribers reached 63% in 2013 and more than 16 percent of the African population are now on the internet. Furthermore, it is estimated that, the global value of web based retail sales in 2013, amounted to $963 billion, while business to consumer e-commerce sales for the period of totalled 1.3 trillion (Ibid, 2013). Hence the rise in the use of the internet has necessitated the ease of doing business on the continent and has resulted in huge profit margins. However, new challenges arise alongside growth, and the ever increasing technological exposure poses its own new vulnerabilities and risks (GFCE, 2016). These risks have entangled Africa in a security dilemma that has threatened its existential status. Unlike terrorism which seeks to weaken the enemy by attacking its physical infrastructure, cyber criminals weaken the perceived enemy by attacking the soft infrastructure which can have adverse effects on state security.

Cyber-crime is a growing global phenomenon, which, according to Symantec Corporation Report (2013), is increasing at a more rapid rate in Africa than in any other area of the world. Indeed, cyber security experts estimate that 80 per cent of personal computers on the African continent are infected with viruses and other malicious software (Gady, 2010). For example, according to Norton Cyber-Crime Report (2014), every second, 18 adults are victims of cybercrime resulting in more than 1.5 million victims globally per day. In addition, South Africa (80 per cent) ranks third with highest percentage of cybercrime in the world, after Russia (92 percent) and China (84 percent) (NTIS, 2014). The Symantec report further reveals that in 2012, the number of targeted cyber-attacks in Africa increased by 42% whilst 31% of these attacks are categorised as cyber espionage have hit state's vital infrastructures such as power companies, telecommunication companies and government infrastructures.

At a regional level, Cybercrimes pose various threats to Zimbabwe, SADC and the globe at large. The economic impact of inadequate cyber security is immense. The Norton Cybercrime Report (2012) indicated that direct financial losses totaled an average of $197 per victim worldwide, while globally a grand $110 billion in direct financial loss. The study by the International Data Group Connect (2012), estimates that annually, cybercrimes cost Southern African economy $573 million. Zambia, Botswana and Zimbabwe alone registered a loss of $200 million due to cybercrimes. This therefore shows that cybercrime is indeed a security challenge in Southern Africa thus need for the principal body in SADC to initiate counter measures.

Over the last few years, the Postal and Telecommunications Regulating Authority of Zimbabwe (POTRAZ) (2016) has noticed an increase in the number of people seeking assistance from the administrative authority to recover money lost in purchasing deals involving syndicates masquerading as buyers of large corporations, especially mining companies. Naturally, the syndicates target unsuspecting ordinary citizens whom they suspect to have a lot of money. According to POTRAZ (2016), roughly 80 000 people fall for scam every day and share their personal information which is then stolen and used for cybercrimes. In addition, the social media portals such as Facebook, WhatsApp and twitter have been used to effect cybercrimes and the onus has fallen upon the government to effectively deal with the crime of this nature. The Baba Jukwa scandal also portrayed how influential cybercrime has and this according to former Minister Jonathan Moyo, "constituted a threat to the peace and security of the country."

The influential yet controversial Baba Jukwa and Wiki Leaks orchestrated by activists in and around Zimbabwe since 2010 has put the whole issue of cybercrime as a threat to the peace and security of Zimbabwe and that of the Southern African Development Community on a different scale. (Chindaro, 2017). What influenced these political mobilizations? How did the government respond? How did the regional body react? These amongst other questions have all been tabulated and yet no clear cut and satisfactory responses have been given. In essence, cybercrime encompasses a wide range of activities, but these can generally be broken into two categories (Techopedia, 2018).

According to US Department of Justice (2012), it entails crimes that target computer networks or devices and crimes that use computer networks to advance other criminal activities. The working definition of this paper thus understands cybercrime as criminal activity that entails the use of a computer system, computer technology, or the internet.

In response to cybercrime, national and international institutions have adopted various measures, practices, methods and procedures. For example, in December 2016, Ukraine experienced a blackout as a result of cyber-attacks on electric power distribution companies (Wikipedia, 2017). Most recently, and still ongoing are allegations of Russian interference in the USA elections through cyber activities and the FBI have opened investigations on the matter. (FBI, 2016). This paper also understands that the WikiLeaks case which also affected Zimbabwe is a typical highlight of another form of cyber-espionage. All these incidents to mention just a few have brought into light, situations of cybercrime which needs instant attention. Consequently, Southern African countries through SADC have urgently scaled up efforts to combat cybercrimes through a multi-stakeholder approach involving government, industry and civil society organizations.

The appointment of a fully-fledged Minister of Cyber Security, Threat Detection and Mitigation in Zimbabwe during the Mugabe era was met with a lot of skepticism though it had a noble agenda. It was mainly driven by the perceived duplication of responsibilities among ministries, and the lack of public understanding of the real threat cybercrime poses (Techzim, 2017). One needs to imagine an attack on the Eco-Cash mobile banking system which disables all associated services such as mobile money transfers even just for a day or disrupts/cuts off Econet, Telecel or Tel-One mobile communication. One needs to imagine the disruption that can occur and the damage to the conutry’s economy could be quite substantial.

The outcry that accompanied the disruption of WhatsApp services for a few hours in 2017 around the world is an example of the potential effect of cybercrime on everyday life. This perception threatens to downplay one of the fastest growing threats to technological development, not affecting Zimbabwe only, but the world at large(Techzim, 2017). All these led the government passing the Cyber Security Act and Cybercrime and Cyber security Bill (2017) which addresses the associated issues. This paper thus attempts to understand the effects of cybercrime as a threat to the maintenance of peace and security in Zimbabwe and SADC.

What remains true and constant to the domain of international relations is that the traditional understanding of state threats has changed. Previously issues to do with nuclear, weapons of mass destruction, espionage and wars were considered to be the core sources of international threat. However, the advancement and persistent reliance on technology has brought about new forms of threats that can equally threaten the existential capability of other states in the international system. That is cyber threats can cause an equally devastating effect just like any of the traditional threats mentioned above.

Although the study of cyber threats is basically a field that is dominating in the field of hard sciences, there is need to develop an intellectual body in the field of international relations. The cyber world has created new battle fields which are not fought by guns and bayonets but by a simple ‘QWERT’keyboard. As such this research argues that QWERTY wars (cyber wars) need the same attention like how states are giving terrorism a huge attention.

1.2 Statement of the Problem

Threats in the international system can also be crucial in understanding state behavior and how various states relate to each other. As such the rise of cybercrimes has influenced foreign policies of many nations Africa and in SADC as a whole. More so, in Zimbabwe the field of cyber security is mainly dominated by computer scientist, electronic engineers and robotics experts. The challenge is that there is need to conceptualize such a threat in the domain of state security and its implications in the field of international relations.

Additionally, there are a plethora of events that have posed as threats to the maintenance of peace and security of Zimbabwe. Cybercrime arguably is a factor that threatens peace and security in Zimbabwe and SADC at large. Cybercrime includes a broad range of illegal activities committed by means of a computer system or network and has become much more sophisticated and threatens to derail the socio-economic and political benefits being achieved through technological advancements. Therefore cybercrime is a threat to human rights, state security and regional peace and stability in SADC. The widespread use of social media platforms has benefited Zimbabwe from somehow moving from a political passive community to a relatively high political awareness. There has been no critical study focusing on cybercrime in SADC and Zimbabwe as a state thus the focus of this study.

However, the abuse of social media platforms has resulted in a perceived political instability which has threatened various economic sectors in Zimbabwe. Several announcements by senior government officials relating to the use and perceived abuse of social media also raised fears about what the Ministry of Cyber Security, Threat Detection and Mitigation together with the Ministry of Information and Communication Technology could do. The primary fear or question is what it would mean for civil liberties; especially those related to freedom of speech but most crucially, also adversely masking the real threat posed by cybercrime. This research therefore tries to understand from all possible objective angles how cybercrime is a threat to peace and security of Zimbabwe and of SADC at large.

1.3 Objectives of the Study

The study seeks to:

- Examine the effects of cybercrime in Zimbabwe
- Evaluate the impact of counter cybercrime measures on human rights development in Zimbabwe
- Evaluate the relevance of SADC in maintaining peace and security through counter cybercrime measures
- Recommend on how to mitigate the threat of cybercrime in maintaining peace and security

1.4 Research Questions

The study seeks to answer the following questions:-

- What is cybercrime?
- What effects does cybercrime have on peace on security of Zimbabwe?
- To what effect does the counter cybercrime measure have on human rights development in Zimbabwe?

- To what effect is the role played by SADC in mitigating cybercrime in the region?

1.6 Justification of the Study

The research seeks to add literature on the area of interest: the threats caused by cybercrime and its impact on peace and security in Zimbabwe. Others studies have effectively focused on threats to peace and security in Zimbabwe from political turmoil, economic defects, but however this study argues that these factors are also caused by cybercrime, thus need to look at the latter as a single unit of analysis. Indeed countering cybercrime clearly constitutes a legitimate aim in maintaining peace and security, however, it is necessary to analyse the proportionality, necessity, legality and efficiency of some measures and their impact on the society at large.

Zimbabwe's responses to cybercrime arguably go beyond the expected and prescribed limits. (Chindaro, 2017). For example, the creation and express functions of the Ministry of Cyber Security, Threat Detection and Mitigation really infringe on the rights and freedoms enshrined under the Fundamental Rights and Freedoms in the Constitution. It is also hoped that this study will initiate new thinking on the existing national and global policy designs and implementation strategies for the inclusion of counter cybercrime measures in national security policies. The study is assumed to benefit all sectors of the society, general public, government as well as research. It is the aim of this research to help human rights activists and governments at large on the area of human rights development and counter cybercrime measures.

1.7 Literature Review and Theoretical Framework

1.7.1 Theoretical Framework

A theoretical framework is an essential element in any research for it gives the tools that can be used for an effective analysis. A clear understanding of the causes and goals of cybercrimes helps one to formulate and frame a counter measure with the innate desire to guarantee peace and security as this is one of the main feature of Zimbabwe's foreign policy. Since the study focuses on the causes of cybercrime and its threat to the maintenance of peace and security, the realist theory and strategic theory will be utilized.

- **The Realist theory**

Hans Morgenthau (1947), outlines that realism in international relations "focuses on the nation state as the principle actor in international relations and its central proposition is that since the purpose of statecraft is national survival in a hostile environment the acquisition of power is the proper, rational and inevitable goal for states within the international system." In light of the need to maintain its peace and security (foreign policy tool), the government of Zimbabwe have been seen implementing measures that guarantee that cybercrimes do not extensively continue to threaten its security.

In addition, Newman (2005) claims that the realist approach is based on the idea that these international institutions are formed and meant to serve the interests of the powerful states. This is true of the formation of SADC in 2002 by both big and small states within the region which have interests although the interests do differ in terms of capabilities and distribution and are not sovereign equals. Institutions like SADC can be argued to have been created to further the interests of South Africa thus need of Zimbabwe and other states to initiate domestic methods that adversely protect their interests. As argued by Waltz (1972), security is best understood individually thus for Zimbabwe to fully understand the threat caused by cybercrimes, there is need to unilaterally counter this threat and also join forces with SADC when it best suit their interest. That is realism according to classical realists and can be utilized in this research paper. This is why Mearsheimer (2016) argued that the realist theory is based on the assumption that "states think strategically about how to survive in the international system".

- **The Strategic Theory**

The strategic theory is also essential when one tries to understand the response to cybercrimes by Zimbabwe and SADC at large. The main proponent of this theory is Harry Yarger in his Treatise, The Strategic Theory. It came about as a handbook to help nation states create objective policies in their domestic and foreign affairs. Strategy can be defined as a way of doing something using resources at one's disposal. From a state perspective, strategy has an underlying logic which is clearly captured by Yarger (2006: 2). Yarger (2006) defines it as the art and science of developing and using the political, economic, social psychological and military powers of the state in accordance with policy guidance to create effects that protect or advance national interests relative to other states, actors, or circumstances. Concurring with this, Jablonsky (1992: 10) captures the real meaning of strategy stating that:

> "In the context of the state affairs, strategy entails the engagement of various instruments of power that is either political or diplomatic, economic, military, virtual and informational) to realize the political aims of the state in collaboration or in antagonism with other actors pursuing their own—possibly conflicting—objectives".

It therefore follows that strategy entails calculative use of state resources in statecraft but more importantly it stresses the importance of the use of force in pursuit of national goals in the international system such that other forms of state power are there to buttress and complement the use of force.

The major tenets of the strategic theory includes that strategy affords direction for the government, seeking to get the most out of positive outcomes and minimize undesirable consequences, as the state moves through a complex and rapidly changing environment into the future, strategy is politically determined, strategy is understood from the environment amongst other tenets. However, the theory is criticized for putting the government on the face of all political processes.

1.7.2 Literature Review

Literature review entails scholarly texts on the subject of interest. In this case, this section reviews the relevant literature on the variables under study: cybercrime, peace and security, the role of SADC and the relationship between cybercrime and maintenance of peace and security.

- **Cybercrime**

Ever since the dawn of the new millennium, there has developed various threats to the maintenance of international peace and security. One of those threats has come out in cybercrime which has adversely developed into one of the challenges to state security. According to US Department of Justice (2012), cybercrime entails crimes that target computer networks or devices and crimes that use computer networks to advance other criminal activities. Therefore, cybercrime is as criminal activity that entails the use of a computer system, computer technology, or the internet.

Chindaro (2017) argues that “cyber-crime comes in different forms and it can be categorized into attacks against individuals, companies, organizations or other countries.” One notable way of cybercrime is phishing. According to Chindaro (2017), phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Most phishing methods employ some technical deception technique to make an email attachment or link appear authentic.

- **Peace and Security**

The concept of security has always been vague in terms of its definition. Security is an ‘essentially contested concept' (Gallie, 1956:184), a concept on which no consensus exists. According to (Buzan, 1991:15), security defies pursuit of an agreed general definition. Traditionally the concept of security has been understood from the realist perspective. The view emphasized the state as an object to protect at whatever cost. Another definition proffered by Martin cited in (Buzan 1991:17) is that "Security is relative freedom from harmful threats" and that security in any objective sense measures the absence of threat to acquired values in a subjective sense, the absence of fear that such values will be criticized"

In the most basic sense and relevant to this paper is the notion of human security. Human security presents an intellectual and policy challenge to the state-centered notion of security by focusing on the individual as the main referent object of security. (Ghali,1992). The term ‘human security' was first defined in the 1994 United Nations Development program’s (UNDP) Human Development Report. This document gives a broad definition of human security, describing it as the condition of safety from seven classes of threats, divided into: economic security, food security, health security, environmental security, personal security, community security and political security, and composed of the two elements of ‘freedom from fear and freedom from want' all these facets are now challenged by cybercrimes.

From the definition of human security, it can be seen that it is a new concept that recognizes an inherent connectedness among development, human rights, and national security. According to Beetham (2007), the concept brings together the human element of security rights and development. As such, it is an interdisciplinary concept which is people cantered, multi-sectorial, comprehensive, content specific and prevention oriented. It is within this framework that the paper argues that cybercrimes posits a threat to human peace and security.

- **Cybercrime as a threat to peace and security in Zimbabwe**

There have been various reports in Zimbabwe where cybercrime has caused diverse effects thus threatening peace and security. A range of scams targeting individuals have been identified and Zimbabwe has its fair share. According to Techzim (2017), a number of people can testify to being lured online into depositing money to buy goods such as cars, clothing, groceries or services such as shipping, just before the companies and individuals disappear from the cyber-world after collecting the money. There have also been reports of individuals lured into depositing money to secure non-existent job opportunities among other scams.

In addition, there have been reports of malware attacks on educational institutions and companies' websites. These institutions are positioned as centers of information in Zimbabwe thus vital to state security. These include the Herald, the government, National University of Science and Technology (NUST) and the Harare Institute of Technology reportedly affected. (Stephens, 2016). This reflects the reality of the threat on Zimbabwe's doorstep and the need to counter cybercrime. Companies and banking systems have also been subject to hacking. According to the US Department of Homeland Security (2004) hacking involves the illegal penetration and use of computer systems to acquire unauthorized information. This has led to the defrauded by individuals of large amounts of money. The classical case is of a Chitungwiza man who hacked OK Zimbabwe's Money Wave System before stealing $70 000 reported widely, is a typical example of such cybercrime activities. All these cybercrimes entails that the challenge is real and there is need for counter cybercrime measures.

1.8 Methodology

This section presents the methodology of this study. Eminue (2004:78) posits that methodology is a system of broad principles or rules from which exact methods or procedures are derived to solve different problems within the extent of a particular discipline. In order to satisfy the objectives and research questions of this study, qualitative research is going to be followed. Thus, this section covers the following issues; the researcher outlines the research design, the research method, the research approach and the methods of data collection, the selection of the sample, the type of data analysis, the ethical considerations and the research limitations of the project.

1.8.1 Research Designs

Every research needs a design before data collection and analysis can commence. According to Robert (2008) "the purpose of a research design is to guarantee that the evidence obtained enables one to answer the initial question as unambiguously as possible."

- Case study

A case study is an essential tool for investigating trends and specific situations according to Webster (2006:12). A case study is an in-depth study of a particular situation, a method used to narrow down a broad field of research into an easily researchable topic argues Rolls (2005). The research utilizes Zimbabwe and the threat it faces from cybercrimes. The response of the government is also essential as it outlines the security agenda of the nation at all costs

1.8.2 Sampling Techniques

According to Palys (2008:13), "purposive sampling signifies that one sees sampling as a series of strategic choices about with whom, where and how one does research." The research uses purposive sampling because it ties to the objectives mainly the one on the role played by SADC and the Zimbabwean government in maintaining peace and security whilst countering cybercrimes. Since purposive sampling entails the selection of informants on their knowledge and experience, the research utilizes knowledge and experience from security experts, economists and political analysts to understand in detail the threat caused by cybercrimes on peace and security.

1.8.3 Data Collection Methods

- Key Informant Interviews

Interviews are the mostly used qualitative research tool. According to Siegfried (2005), an interview can be thought of as a guided conversation between a researcher and the informant. Semi-structured interviews entails that the interviewer will develop a guide to the topics of cybercrimes, peace and security outlining the relationship between the two: the impact and effects of cybercrimes on the maintenance of peace and security of Zimbabwe. More so, Key informant interviews are ideal for they allow for prompting the informant to clarify and expand on certain points of interest.

- Documentary Review

Rolls (2005) defines documentary analysis as involving obtaining data from existing documents without having to question people through interviews and questionnaires. Documents are essential for they are tangible materials in which facts and ideas have been recorded in understanding the impact of cybercrimes on the peace and security of Zimbabwe and the region as a whole. The research will make use of written and produced material in newspapers, articles, government policy records, international organizations and documents. It is true that documents can indeed reveal in detail about the research topic.

1.8.4 Data Analysis and Presentation

- **Content Analysis**

According to Cole, (1988) content analysis is a method of analysing written, verbal or visual communication messages. It is also known as a method of analysing documents. Content analysis allows the researcher to test theoretical issues to enhance understanding of the data. Content analysis enables one to distil words into fewer content related categories. Cavanagh (1997) argues that when classified into the same categories, words, phrases and the like share the same meaning. According to Krippendorff (1980), content analysis is a research method that makes replicable and valid inferences from data to their context, with the purpose of providing knowledge, new insights, a representation of facts and a practical guide to action.

- **Thematic Analysis**

According to Guest et al (2012:13), thematic analysis is one of the most common forms of analysis in qualitative_research. It prioritizes pointing out, examining, and recording patterns (or "themes") within data. Creswell (2002) defines themes as patterns across data sets that are important to the description of a phenomenon and are associated to a specific research question.

The themes become the categories for analysis. Braun and Clarke (2006) claim that thematic analysis is performed through the process of coding in six phases to create established, meaningful patterns. These phases are: familiarization with data, generating initial codes, searching for themes among codes, reviewing themes, defining and naming themes, and producing the final report. The central purpose of using thematic analysis is to identify patterns of meaning across a data that offer an answer to the research question being addressed. Through thematic analysis, patterns will be identified through a painstaking procedure of data familiarization, data coding, and theme development and revision. There are many reasons and advantages of using thematic analysis. Thematic analysis is theoretically-flexible and this means that it can be used within different frameworks to answer different types of research questions and scrutinizing the objectives of the study.

1.9 Limitations

Limitations are inherent design parameters that can limit the scope of the research findings. Therefore, this research had to cut the geographical concerns as the population of study is Zimbabwe, located in Southern Africa. Basic research methods, not all the research techniques, are used due to budgetary constraints. Even though limitations have the potential of reducing a study's validity, after a careful and deliberate consideration, the research findings will be useful and valid.

1.10 Delimitations

According to Simon (2011), delimitations "define those characteristics that limit the scope and define boundaries of one's study." In as much as cybercrimes have an impact on many societal norms and spheres, this study focuses on their effect on peace and security. Zimbabwe is a case study since it has been affected by diverse cybercrimes and recent developments in countering the phenomena makes it worth to study.

1.11 Dissertation Outline

Chapter 1 will outline the background of the study, statement of the problem, justifications as well as the methodology. Chapter 2 will give a conceptual framework of cyber security while Chapter 3 will provide an overview of SADC cyber security. Chapter 4 will highlight the presentation of findings and the analysis. Chapter 5 will conclude the thesis by giving overall conclusion and recommendations.

CHAPTER TWO: CONCEPTUAL FRAMEWORK

2.1 Introduction

Since the turn of the new millennium, various schools of thought have tried to define, conceptualize and understand cyber security. Various strategies and even theories have been put into practice to counter this threat to international peace and security. However, there is no distinct or even a precise definition of cybercrime for threatened societies define it to suit their cyber security strategy. There is no silver bullet for cyber security is a constantly evolving, constantly active process just like the threats it aims to prevent. In an attempt to widely understand cyber security, this chapter discusses on cyber security and what it entails the background and development of cyber security as a concept and Southern African Development Community (SADC) cyber security overview. All these are understood in a framework of trying to effectively counter cybercrime as a threat to peace and security.

2.2 Conceptualising cyber security

The conceptualisation of cyber security differs from society to society. The cyber security debate originated in the United States of America in the mid-1990s, from where it subsequently spread to other developed countries and manifested itself on security policy agenda. Today, the whole globe has been affected either directly or indirectly by cybercrime thus need for cyber security enhancement. According to Griffiths (2010), the topic is a product of two recent developments which are the so-called information revolution and the integration of these technologies into a multimedia system of communication with global reach. In this regard, cyber security is concerned "with making cyber space safe from threats, namely cyber-threats." (Griffiths, ibid) As commonly used, the term cyber security thus refers to three things according to Neeroy (2016). These are:-

- A number of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other aspects of cyberspace, from all threats, including threats to the national security;
- The degree of protection resulting from the application of these activities and measures;

- The associated field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality.

In this regard, cyber security thus refers to measures, practices and methods implemented to make the cyber space safe and productive for the society.

In his cyber security strategy, Lord Hammond (2016: 12) argues that cyber security refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm or misuse. This includes damage caused intentionally or accidentally by the operator of the system, as a result of failing to follow security procedures. This is why cyber security has become an integral part of a societal well-being thus need to be observed at all costs.

In addition, cyber security as understood by AFRICACERT (2017:15) is “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber space and organization’s user assets.” In this regard, cyber security involves the protection of electoral information from all forms of harm and misuse. At a national level, cyber security strives to ensure the attainment and maintenance of the security properties of the country and state’s assets against relevant security risks in the cyber environment (Kiboi, 2015). Information technology experts unanimously agree that the general cyber security objectives comprise the availability, integrity, which may include authenticity and non-repudiation and the confidentiality of information. In short, cyber security tries to guard against cybercrimes and threats.

2.2.1 Types of cyber threats

There are various cyber threats that have an effect on the maintenance of peace and security. These threats are what cyber security mechanisms try to counter. Common cyber threats fall under three general categories: -

- **Attacks on confidentiality**

AFRICACERT (2017) argues that stealing, or rather copying a target's personal information is how many cyber-attacks begin. These cybercrimes also include garden-variety criminal attacks like credit card fraud, identity theft, or stealing bit coin wallets. In the discourse of national security, nation-state agents for example the Criminal Investigation Agency in the US and the Central Intelligence Organization (CIO) in Zimbabwe make confidentiality attacks a major portion of their work, seeking to acquire confidential information for political, military, or economic gain.

- **Attacks on integrity**

Cybercrime is also affected through sabotage of information. That is the common term used when referring to integrity in cyber threats. Porup (2017) writes that integrity attacks seek to damage, corrupt, or destroy information or systems, and the people who rely on them. Perpetrators can range from script kiddies to nation-state attackers. The alleged Russian intervention in the 2016 American General Election falls under this category of cybercrime. Arguably, this has had diverse effects on the American political environment.

- **Attacks on availability**

Preventing a target from accessing their information is most frequently seen today in the form of ransom ware and denial-of-service attacks. Ransom ware encrypts a target's data and demands a ransom to decrypt it. Norton Report of 2013 in South Africa reported that South Africa and the Southern African region were experiencing this type of attack. South Africa is even ranked 3rd in the list of countries experiencing cybercrime.

2.3 The Development and Background of Cyber Security

Arguably, information and communication technologies have evolved ever since the turn of the new millennium and are now integrated into virtually every aspect of human life and survival. SADC and Zimbabwe can be argued to becoming rapidly a digitalised community so as the world. However, the transformation brought about by this digitalisation creates new dependencies. According to the National Cyber Security Strategy (NCSS) 2016-2021, economies, the administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. Indeed, a loss of trust in that integrity jeopardise the benefits of this technological revolution.

Cyber security as a concept developed during the early 2000s for it was now an era where computer systems were developing into a determining factor in world geopolitics. Initially, the word only highlighted the challenges faced by network computers and how the hardware was corrupted. However, Griffiths (2017) argues that it later moved from this technical understanding to a more realistic and precise meaning as experts argued that the threats emerging through new technologies could be harnessed in such a way that they could have serious societal impact and cause direct harm to the state and its citizens. From a human security perspective that evolved after the end of the Cold War (Buzan, 1998), cyber security developed to counter threats to human beings for it had direct impact on the latter.

Importantly, President Obama in 2010 identified cyber security as one of the most serious economic and national security challenges for the United States, but one that the U.S. as a government or as a country is not adequately prepared to counter. (CN, 2011). The U.S. for example is therefore actively supporting and engaging industry, academia and other nations to help build the necessary cyber capabilities and workforce. (US Cyber Security Strategy, 2013). In Japan, a series of remarkable cyber-attacks on government and private targets (including Sony, Mitsubishi, Yahoo Japan, and National Pension Administration) have firmly placed cyber security on the political agenda in Japan (Netherlands Enterprise Agency, 2015).

The training of plentiful, capable staff and exercises for incident response has been stated as a key priority for the Japanese government, which is coordinating efforts through its National Centre of Incident readiness and Strategy for Cyber security (NISC) (Netherlands Enterprise Agency, 2015). In addition, Cyber security and innovative financial technology solutions are high priority in Singapore. (Singapore National Cyber Security Strategy, 2012). A few years ago, the Singapore government launched a five-year National Master plan 2018 on Cyber Security Singapore with the objective to stimulate development of capabilities in the aforementioned areas and to create a cyber-security hub for the region (Singapore National Security Strategy, ibid) (ASEAN, 2016).

The world's largest inter-governmental organisation has also tried to come up with various cyber security mechanisms. During the 2011 United General Assembly meeting in New York, it was discussed that there should be capabilities that effectively counter emerging new threats in cyber space and ensure that the digital infrastructure is secure and trusted to enable further international trade and economic growth. This therefore shows that cybercrime has been an existing threat to nation states thus a need to create feasible cyber security measures.

2.3.1 Background and Development of Cyber Security in Southern Africa

Unfortunately, SADC member states are yet to give a detailed and comprehensive report on how cybercrime and leading to cyber security has developed in the region. However, this research will base on detailed reports from various organisations and companies within the region. Wolfpack, a South African Company in 2012-2013 gave an analysis on cyber security within South Africa and the region at large. Cyber threat has developed through denial of service to organisations, governmental telecommunications and finance. This has direct impact on the government since the reach of protocol in information delivery caused mayhem in governmental operations. Wolfpack (2013:26) reported that the most affected targets are global credit cards and financial networks along e-commerce sites.

Research conducted by SAPS Electronic Crime Unit (ECU) shows that cyber-attacks are often transitional and planned by organised crime syndicates based abroad. Cybercrimes like these are difficult to stop since perpetrators are operating within foreign lands with near impunity. According to Norton a security company in (2013), 61% of adults in Southern African countries are affected directly or indirectly by cybercrimes. These published reports thus indicate that cybercrime is a growing threat to Southern Africa. Collectively these researches indicated that there is need for an effective cyber security strategy that can protect and maintain peace and security, either human or traditional security.

2.4 SADC Cyber Security Overview

There has been no major activity by SADC in the discourse of cyber security. Scholars argue that lack of this has caused the region to experience diverse cybercrimes and threats. There has been a call for SADC to comprehensively adopt a cyber-security mechanism so as to effectively deal with cybercrime which is a threat to the peace and security of the region. The widely used

"Harmonisation of ICT Policies in Sub-Saharan Africa: Computer Crime and Cybercrime: Southern Africa Development Community Model Law" is arguably the best framework initiated by the organisation in cyber security. However, the framework was financially aided by the European Union, and this shows the intensity of cybercrime and cyber security as failing to be addressed by the responsible SADC body. There also instruments initiated by SADC in cyber security mechanisms including National Exchange Units but these arguably are not enough.

Part Two of the SADC Model Law, titled *Offences* gives a wide range of cybercrime offences and how they are countered. Illegal access to information is described as:-

> "A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both".

This definition of illegal access and the penalty for that is an attempt to protect the integrity, availability and confidentiality of information: cybercrimes that affect national security. Understood with illegal access, illegal remaining means that person who intentionally, without lawful excuse or justification o remains logged in a computer system in which they do not have due access. As a cyber-security mechanism to these illegal activities, SADC has come to terms that:

> "A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent".

This therefore shows that SADC gives the state the mandate to punish cybercrimes as they deem fit. Could this be an issue of sovereignty being respected or it is just lack of intent by the regional body to effectively counter cybercrime? No definite response has been gathered thus far.

Southern African Development Community (SADC) mission is to promote sustainable and equitable economic growth and socio-economic development through efficient productive systems, deeper co-operation and integration, good governance, and durable peace and security. (SADC, 1992). In regards to this, the proposed regional priorities for 2011-2012 includes, amongst others, the setting up of National and Regional Internet Exchange points; harmonisation of Cyber Security Regulatory Frameworks in SADC. This was a proposal to include collaboration in fighting against cybercrime and collective action was one of the ways of going about it.

Most Southern African countries drafted national cyber security strategies motivated by this initiative. For example, South Africa’s first draft of the South African National Cyber Security Policy was published for comment in February 2010. This draft included cyber security awareness as part of the role of the proposed National CSIRT. The content of the SA cyber security draft entailed the Legislative Framework, Policy Objectives, Creating Institutional Capacity to Respond to Cybercrime and Threats, Reducing Cyber security Threats and Vulnerabilities, Coordinate Local and International Partnerships and Continuous Innovation, Skills Development and Compliance. (Dhlamini et al, 2011: 19). South Africa is further recognised with its own Electronic Communications Security Computer Security Incident Response Team (SA- ECS-CSIRT). The ECS-CSIRT is the South African National government and its constituency is the whole South African governmental organisation cyber community. (Dhlamini, ibid). In addition, the Robert Mugabe led administration in Zimbabwe once even went further and created a Ministry entitled with Cyber Security. All these are mechanisms inspired by SADC, arguably on cyber security.

2.5 Conclusion

Indeed cybercrime is a threat to peace and security of nations. Within this understanding, there is need to counter cyber threats through adoption of cyber security procedures and processes. However, cyber security is not as clear cut and depends on each country as well as the ever changing nature of cybercrimes. There is need thus to objectively understand cyber security, trace its development and of relevance to this study, how SADC, a regional body mandated with promoting development within the region, has understood and developed cyber security mechanisms. This chapter attempted to understand such concepts.

CHAPTER THREE: AN OVERVIEW OF THE SADC CYBER SECURITY PROTOCOL

3.1 Introduction

The previous chapters have attempted to give a background of the evolution of cyber security and cybercrimes. It has to be noted that this research seeks to emphasize the important role cyber security plays in securing the peace and security of Zimbabwe and SADC as a whole. This chapter looks at SADC's commitment to curbing cybercrime in the region and also the centrality of issues to do with cybercrime since it is a global phenomenon. The proceeding chapters acknowledged the evolution of technology which has resulted in human beings living what some call an e-life, which is over reliance on the internet thus increasing the risk of cyber-attacks. This chapter is in three parts that is measured by SADC to deal with cybercrime, major challenges in implementing the SADC Cyber security protocol and lastly forms of cybercrime that SADC faces.

3.2 Measures by SADC to deal with cybercrime

To be able to unpack the measures SADC has taken to curb cybercrimes, it is prudent to understand the background from which the region then resolved to take such measures. According to the Herald Newspaper of 12 April 2012, in an article written from a SADC meeting on the harmonized cyber security framework held in Gaborone, Botswana, " Using modern telecommunication networks such as emails, chat rooms and social networks, cybercrime has threatened world's security and financial health (Verma et.al, 2012)." The then Botswana's Transport and Communications Minister said:

> "Access to information and knowledge through Information Communication Technologies (ICTs) is necessary for the achievement of the Millennium Development Goals (MDGs) since ICTs have the capacity to improve the living standards of SADC citizens…., however, the same advancements in ICTs could pose serious challenges, particularly for developing countries that have relatively low expertise in dealing with challenges such as cybercrime."

To understand this background this paper brings forth some submissions from officers from the Ministry of ICT and Cyber security in Zimbabwe who were of the view that, Cybercrime covers any illegal behaviour committed by means of, or in relation to, a computer system or network. With respect to cyber security, it was defined as "preservation of confidentiality, integrity and availability of information in cyberspace" and this is according to the International Standardisation Organisation (ISO).

In a bid to curb the effects of computer related crime, SADC formulated the **SADC**

3.3 Harmonised Cyber Security Legal Framework (ITU-HIPSSA)

The Framework consists of the following model laws for the region;

- E-Transactions/E-Commerce Model Law
- Data Protection Model Law;
- And Cybercrime Model Law

These model laws were approved by the SADC ICT Ministers on 8th November 2012 in Mauritius. They were formulated using guidelines from the ITU Global Cyber Security Agenda (GSA) of 2007 which provided a framework for international cooperation aimed at enhancing confidence and security in the information society. Model laws are also in conformance with the African Union (AU) Convention on Cyber Security. The model laws are also a result of the Declaration on Information and Communication Technology (2001) that was signed by Heads of State and Government in August 2001. The Declaration evidences the commitment of SADC states to use ICTs for regional growth focusing on economic and social benefits derived from ICTs.

The Declaration has five (5) priority areas of focus:

- Regulatory environment for ICT;
- Infrastructure for ICT development;
- Community participation and governance in ICT development;
- ICT in business development and
- Human resource capacity for ICT development.

As stated in the SADC website, these priority areas intend to secure widespread cultural acceptance of ICT innovations, thereby improving economic and social development in the region.

The above illustration shows SADC's commitment to curbing the problem of cybercrime in the region. Kuda Hove, a legal and ICT policy officer at the Media Institute of Southern Africa in his LinkedIn article of July, 2017 acknowledges that this regionally harmonized approach to regulating cybercrime has its merits primarily because cybercrime by nature cannot be restricted to one geographical location or country. According to Hove, a cybercriminal based in Botswana can easily institute an online offence or attack against victims situated in Zimbabwe. Hove further postulates that it therefore makes sense for Botswana and Zimbabwe to have harmonized Cyber laws that would make prosecution of that cybercriminal possible in either of the two countries. On the contrary, this approach has a downside, for instance if the SADC Model Law on Cybercrime carries defects there is a high chance that the national laws that are drafted under the guidance of the Model Law will inherit some, if not all of the defects contained in the Model Law (Hove, 2017). In theory, the SADC Model law overlooked the distinct levels of technological advancements and differing political climates in the different SADC member states. These differences result in nuanced definitions of cybercrime in each respective SADC Member State.

In revelations made by respondents from the Ministry of Defense in Zimbabwe, technologically advanced countries have invested large sums of money in cyber-security as evidenced by the trending Cambridge Analytical case where the company harvested private Facebook information from over 50 million users and used it to influence the 2016 American election. If big economies like America can be subjected to cybercrimes, then small countries like Zimbabwe are at a higher risk. One respondent applauded the Zimbabwean Government for using a biometric method for voter registration only arguing that biometric voting can be manipulated to suit cybercriminals. Therefore, Zimbabweans living in the diaspora must travel back to Zimbabwe in order to participate in the 2018 election which will be conducted manually, in the ballot box.

3.3.1 The Nature Cyber Crime

The official from the CIO who requested anonymity was of the view that, the lack of awareness not only about the nature of cybercrime but also its scope has impacted negatively on the effectiveness of the SADC's responses including through its Model Law. The respondent felt there is a serious need for the regional body to marshal an early warning mechanism through a properly coordinated network of regional intelligence/security and relevant law enforcement institutions. This was so that the legal framework can produce the desired objective of effective combat against cybercrime. Given that the ultimate objective of the criminal procedure system is to secure deterrence through successful conviction there may be a need for the creation of a regional cybercrime court to deal only with cases that involve cybercrime. Assuming that cyber criminals are almost invariably ahead of law enforcement agencies there is need for continuous training and research on the part of the latter and the rest of the criminal justice system in order that they prevail upon the former. It goes without saying that all this requires a substantial injection of resources including monetary. Except perhaps for SA, it is too much of an expectation for the rest of the SADC member states to bankroll the foregoing ahead of other more pressing needs like droughts and diseases.

On the dominance of the study of cyber security in International Relations the CIO officer stated that the former is still a grey area which is slowly emerging as an area of study under the non-traditional security category. He said the rate at which cyber security and cybercrime are shaping international business and affairs certainly requires that these two be accorded an appropriate slot in the field of International Relations. According to him, indications are that this is the direction the study is taking.

3.3.2 POTRAZ on Cybercrime and Cyber security

It came out in an interview with the Head of ICT at POTRAZ that SADC set up a Communications Regulatory Authority of Southern Africa (CRASA) whose mandate is mainly to monitor SADC cyberspace. In line with this mandate, this authority encourages member states to protect their national cyberspaces and encourages the harmonization of laws between countries. The official from POTRAZ intimated that Cyber-security must not be looked at as a pure computer security issue, it must also be seen as a national policy matter because the illicit use of cyberspace can impact negatively on the economic, public health, safety and national security activities and since all these activities are the main concern of Governments, then national leaders are accountable for Cyber-security. According to him, cyber-security aims to preserve data confidentiality, data integrity, access control, communication security and availability.

During the interview he alluded to the SADC Model Law on Cybercrime which he defined as a guideline from which member states borrow to craft their own country specific laws. In his view, the countries that have adopted this model law have successfully come up with cyber specific laws as it encourages the creation of cyber specific units within the police force, the courts and so forth for the development of guidelines for the protection of users.

3.4 MAJOR CHALLENGES IN IMPLEMENTING THE SADC CYBERSECURITY PROTOCOL

It is interesting to note that despite the frantic efforts made by the region to come up with a wholesome approach towards countering cybercrimes, there is non-commitment from other member states which is caused mostly by incapacitation. Credit must be given to SADC for the effort it has put towards countering this security threat.

3.4.1 Lack of Sufficient Equipment

For Zimbabwe, it has taken too long to have the three Cyber-Security Bills passed into law due to lack of equipment needed to investigate cyber-security and foreign currency shortages to mention but a few. SADC as a whole does not have the technical capacity to deal with cyber-crime. Notably, most countries in Southern Africa do not possess any Computer Emergency Response Teams (CERT) whilst in the Arab regions their (CERTs) are connected such that it is easy to apprehend a perpetrator as long as they are still within the Arab region. An official from POTRAZ disclosed that POTRAZ had only received an email from CRASA on 15 March 2018 in which the institution was asked to establish an expert group on public key infrastructure and (CERT).

An official from the SADC-RTP in Harare was of the opinion that, a lot has to be done in terms of acquiring tools to fight cybercrime. In his view, cyber criminals take advantage of the fact that SADC countries are not yet able to track the origins of a text message hence the constant abuse of social media for example, when Zimbabwe’s new President Emmerson Mnangagwa recently went to Addis Ababa for the African Union conference, people started sending messages insinuating that the President was being sidelined because he was a product of a coup and yet in actual fact President Mnangagwa was applauded for a job well done to the extent that even the theme of the conference was changed to “Africa is open for business” taking after president

Mnangagwa" "Zimbabwe is open for business." social media destroyed Libya and Tunisia and that is a clear indication of the amount of damage it can cause if it is left unattended to. This therefore brings out the need to establish an institution that trains individuals on cyber-security to enable fast and real time responses to cyber-attacks.

3.4.2 Lack of Expertise

Another major challenge that was listed is that of lack of awareness on what cyber- crime is. Due to the fact that Southern Africa is trailing behind technologically, people are not aware of the cybercrimes that are manifesting in their midst on a daily basis. There is therefore a need for governments to embark on large awareness campaigns in which people will be educated on the available cyber-crime legislation, effects of cyber-crimes and how they can be affected by cybercrime. Such crimes are usually overlooked as people think they only occur in more developed countries and yet they happen on a daily basis. In 2017, a famous Zimbabwean gospel singer named Fungisai Zvakavapano Mashavave became a victim of cyber bullying as insults were hurled at her on Facebook, a social media platform for doing a collaboration with a Zim Dancehall artist and failing to keep up with his dance moves. This will also help government to know and keep up with trending cybercrimes thus making it easy to counter them. A cyber security institution of higher learning will be able to track down the origins of such malicious messages and apprehend the perpetrators.

3.5 COMMON TYPES OF CYBERCRIME IN THE SADC REGION

According to the Reserve Bank of Zimbabwe (2017), cybercrimes fall into three broad categories namely, crimes against

- Individuals and corporations: This type of cybercrime can be in the form of cyber stalking, distribution of pornography, trafficking;
- Property: This type of cybercrime can be done through the stealing of a person's bank details which they use to steal money, cloning of credit cards, and use of malicious software to gain access to an organization's website and steal information or disrupt the systems of the organisations. A very good example is that of Zimbabwe, were criminals have used the mobile money transfer platforms, tricking unsuspecting members of the public to make payments for non-existent services and;

- Government: This type of cybercrime against a government is referred to as cyber-terrorism. Criminals hack into government websites, military websites with various motives, including stealing or destroying information or simply to embarrass the government. The perpetrators can be terrorists or individuals unfriendly to the government of the day.

According to Symantec, the primary motivation for cybercrime is financial gains. This crime has become the domain of sophisticated large criminal groups who target large sums of money.

3.5.1 Phishing

Common in SADC now is phishing, which according to Gupta (2014) is the unscrupulous practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. According to www.techsmart.co.za, in September 2013 a group of 54 individuals was hurled to the South African courts on charges of fraud, money laundering, racketeering and theft. According to this website, "the group had apparently been running an extensive phishing scam to gain access to people's banking details, while also utilizing SIM swaps and identity theft to rob its victims. The syndicate subsequently opened fake store accounts using the information, and also used cloned identities to access credit facilities. On one occasion they managed to siphon off almost R7 million from 21 accounts in a mere 24 hours. On a separate occasion, 30 accounts were compromised to the tune of an additional R3.1million."

3.5.2 Credit Card Fraud

This happens when a stolen credit card is used to make payments for goods bought online (Jara and Gundemoni, 2006). It is done to obtain goods without payment or to access unauthorized funds from an account. The perpetrators are hardly caught as it is extremely difficult to trace the transaction back to the offender. The most common form of credit card fraud is the card-not-present (CNP) fraud, which makes up a high percentage of card fraud cases, followed by counterfeit cards. The CNP fraud is a fraudulent transaction used for ordering goods online or over the phone where neither the card nor the cardholder is present while conducting transactions. Notably, the highest losses from CNP fraud are in respect of tourism and hospitality services including airline tickets, travel agencies, vehicle hire and hotel accommodation as well as direct marketing.

3.5.3 Identity Theft

The National Science Foundation (2002) clearly show that identity theft happens when cyber-criminals gain access to information about someone's identity (name, date of birth, current and previous addresses) enough to allow them to commit fraud. The perpetrators do not care if the victims are alive or deceased and through identify theft victims lose large volumes of money after these criminals use their names to access bank loans, mortgages and credit cards. For example, Valeryevich Seleznev, a Russian cyber-criminal pleaded guilty in September 2017 to charges of identity theft (U.S Department of Justice, 2017). Seleznev admitted to being associated with carder.su, an internet-based, international forum in which members committed identity theft, bank fraud and computer crimes.

In 2012, a scam involving Facebook developed as an attempt to use social media to steal financial information from users.

Hackers hijacked users' accounts, impersonating Facebook security. These accounts would then send fake messages to other users, warning them that their account was about to be disabled and instructing the users to click on a link to verify their account. The users would be directed to a false Facebook page which asked them to enter their login info, as well as their credit card information to secure their account.

3.5.4 Electronic Money Laundering

According to AUSTRAC (2011), money laundering is the term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. The processes by which criminally obtained goods may be laundered are extensive. It is important to understand that the many features of electronic money make it a convenient tool for criminals to use it as means of money laundering and terrorism financing, since they allow performing an easy and fast large sum transfer from one place to another in the world with the Internet access.

At the present moment electronic money takes up its own place in the Virtual Currency. Electronic fund transfers have been used in concealing and moving proceeds of crime across jurisdictions. With the emergence and proliferation of various technologies of electronic commerce, criminals are using virtual currency to launder funds and evade tax. Nine virtual currencies of interest are the use of Bitcoins, Web money, Paymer, and Perfect Money (RBZ, 2017). Bitcoin is a new innovative payment network, which uses peer-to-peer technology to operate with no central authority or bank. It is a form of digital currency created and held electronically, through computer software which generates virtual value from a process called Bitcoin mining where people are tasked to solve complicated mathematical problems.

3.6 Conclusion

This chapter has presented SADC's commitment to curbing cybercrime in the region and also the centrality of issues to do with cybercrime since it is a global phenomenon. It also presented the challenges of curbing cybercrime in the region. The chapter forms the basis within which the next chapter can be discussed. The next chapter focuses on the presentation of findings and analysis.

CHAPTER FOUR: CYBERCRIME IN THE CASE OF ZIMBABWE

4.1 Introduction

The proceeding chapter looked at the cyber-security status quo in the SADC region and the different strategies the regional body has employed to deal with the threat of cybercrime. Perspectives from various policy makers were discussed as well as concerned stakeholders. Findings from the respondents interacted with indicated that, SADC is largely incapacitated to deal with this animal called cybercrime and a lot of work still has to be done regarding this global phenomenon. This chapter's purpose therefore is to dwell more on how Zimbabwe is attacking the same phenomenon of cyber-security. This submission will look at the National Cyber-security Policy, The theoretical and contextual aspects of Cyber-Security, Cyber-Security in the banking and financial services sector, securing Cyberspace for society and lastly case studies on cyber-attacks.

Table 1: Summary of Respondents

Targeted Respondent	No of respondents expected	No of respondents who were interviewed	Date of Interviews
POTRAZ	3	2	17 March 2018
Academic	3	3	26 March 2018
Network Subscribers	4	3	2 and 3 April 2018
The Ministry	3	2	17 April 2018
SADC	3	2	22 and 24 April 2018
Total	**16**	**12**	

Source: by the author

4.2 Uncontrolled, unlicensed and un-regularized software

According to an academic from Harare Institute of Technology (HIT), Zimbabwe currently holds the pole position of the most "hackable" country in the world. The BSA Survey highlighted that Zimbabwe was joint number 1 with Libya (with a percentage of 90%) in the rankings of countries in the world with the highest rates of unlicensed software installations. As a benchmark, the global average was 39% and the average for the Middle East and Africa was 57%. It is also worth noting that, according to the same report since 2009 Zimbabwe has been consistently ranked among the top 3 countries in this regard in the whole world. According to a Technomag report of July 2017, Zimbabwe has been ranked number 18 in Africa on the Global Cyber-Security Index 2017 for cyber security commitment. Mauritius, Egypt and Rwanda were the top three countries on the continent. The second edition of the Global Cyber-security Index 2017, released by the International Telecommunications Union (ITU), measured the commitment of ITU Member States to cyber security and highlighted a number of illustrative practices from around the world (ITU, 2017).

An official from Grant Thornton stated that it is interesting to note that most organizations keep their budget for IT security very minimal compared to the budgets allocated to other departments. In light of this, one can safely say that a large number of corporate institutions in Zimbabwe adopt a rather reactive approach to cyber security than a pro-active one. She further stated that cyber security goes beyond the normal anti-virus and firewalls and she called for capacity building in respective organizations in order to grow expertise in this field. The interviewee alluded to the fact that it is proving to be difficult to strike a balance between the functionality of an IT system and its security. To support this notion, she felt that the more secure a system is, the less user friendly it becomes hence the choice by most administrators to keep it user friendly despite the risks associated with doing so.

4.3 Proliferation of cybercrime in Zimbabwe

The Parliament of Zimbabwe Policy Brief Number 8 of November 2017 indicates that in most developing countries, there is a paradox where increased internet usage and other technologies have increased the rate of malware and exposure to cyber threats. The reason being that, such countries are less mature in their security capabilities (Nicholas, 2014). In Zimbabwe the most common cyber threats include hacking, phishing, malware, viruses, and spam according to the Government of Zimbabwe (GISP, 2017). The Government Internet Service Provider reports that the cybercrime affect people who buy online. Those people who are into mining and those who buy cars online are the most affected. Prospective buyers of mining equipment are usually trapped by the cybercriminals who pretend to be suppliers of mining equipment yet they will be companies that do not even exist (Government of Zimbabwe (GISP), 2017). The syndicates create websites online and give references of their other chain members so that when people call they talk to other members of the syndicate if they want verification to authenticate their story. Their company vanishes once they get the money leaving the victims stranded, (Government of Zimbabwe (GISP), 2017). These types of cybercrimes involve the locals and their foreign based accomplices.

According to the same Parliamentary Policy Brief, there has been significant growth in internet usage in Zimbabwe with statistics showing a penetration rate of 50% in 2016 (POTRAZ, 2017). As at 30 June 2017, the total number of internet subscriptions was 6,668,155 (POTRAZ, 2017). According to POTRAZ (2016) Report, Zimbabwe had 12,878,926 mobile phone subscribers. Facebook is the most popular platform in Zimbabwe; Twitter is also slowly gaining momentum

(MISA-Zimbabwe, 2015). This has seen mobile Internet data usage up by 19%, whilst national mobile voice traffic declined by 15% (POTRAZ, 2017). This indicates growth in internet usage in Zimbabwe and Zimbabwe has been a victim of a number of cyber security breaches on various institutions especially in government departments.

The Reserve Bank of Zimbabwe (RBZ, 2015) states that cybercrime contributes to the US$1, 8 billion estimated illicit proceeds generated from criminal activity annually in Zimbabwe. The same report states that about 140 cases of cybercrimes were reported between 2011 and 2015 and these include; Phishing (20); Credit Card Fraud (13); Identity Theft (10); Unauthorized Access (24); Hacking (72); and Telecommunications Piracy (1). These statistics show Zimbabwe's vulnerability to computer and cybercrimes and thus the pressing need for a legal framework to combat these crimes before they become pervasive (MISA-Zimbabwe & Digital Society Zimbabwe, 2017).

Parliament of Zimbabwe's website was reportedly hacked in February 2016, by cyber attackers identifying themselves as Anonymous (iharare.com, 2016). Websites belonging to ZANU PF Party, the state controlled broadcaster Zimbabwe Broadcasting Corporation (ZBC) were reportedly hacked and shut down by an internet vigilante group named Anonymous Africa, in retaliation of their perceived government's blockade of access to instant messenger services WhatsApp on July 7 2016 (The Southern Daily Zimbabwe, 2016; Sultan, 2016). The attack on Zimbabwean government website disrupted the online service of the country's official portal (zim.gov.zw) (Sultan, 2016; & Shaban, 2016). According to Sultan (2016), Anonymous has also been conducting Operation Op Africa since 2015 which aims to attack government and oil sectors against corruption, child abuse, and child labor in the continent. In the education sector, the National University of Science and Technology (NUST) and the Harare Institute of Technology (HIT) websites suffered cyber-attacks on the 21st of June 2017 (Tshuma, 2017). This claim was corroborated by Pindula news which stated, "National University of Science and Technology (NUST) and the Harare Institute of Technology (HIT) were hacked with the hackers demanding a ransom of 1 000 Bitcoins to restore information to their website" (Pindula News, 2017)

4.4 Zimbabwe conforming to SADC cyber security protocol

Upon engaging an official from POTRAZ, they revealed that Zimbabwe does conform to the SADC cyber-security protocol or model law. This is evidenced by the frantic efforts being made by the government to complete the crafting of the three cyber security bills and their subsequent passing into law. The Cyber-Security Conference that ran from 10 to 1 April 2018 which ran under the theme “Cyber Security: Our Shared Responsibility” saw a variety of stakeholders coming together to tackle the problem of cyber- crime and to try and establish how best Zimbabwe as a nation can keep up with the fast changing technologies manifesting in the cyber space taking into cognoscente the budget restrains that we face as a nation. The Herald of 16 March 2018 reported of the launch of the National ICT policy by President ED Mnangagwa and Minister of ICT and cyber security, Honorable Supa Mandiwanzira and the purpose of this policy is to guide Zimbabwe’s economic development through a coordinated use of ICTs which is the ICT policy.

4.5 Ministries and Departments making significant strides

At a cyber-security conference held by the Ministry of ICT at the Celebration Centre from 10 to 11 April 2018, the Permanent Secretary in the same ministry Engineer Samuel Kundishora alluded to the fact that the national policy has to be reviewed from time to time in order to keep up with the ever changing technological advancements. He implored all concerned stakeholders to be wary of repetitive attacks and guard against them by all means possible. Kundishora advised that, it would be prudent if the country came up with a cyber-security forum and a cyber-security steering committee, a national CERT and lastly a national security operations center. There is therefore need for high level Government leadership in crafting and implementing cyber security strategy as demonstrated through the Conference held on 10 and 11 April 2018. Government must also consider collaboration in developing and implementing the strategy at national level between government, corporates, and society. Efforts by the SADC Secretariat to counter the threat of cyber-crime show the international and regional cooperation to fight against cyber-crime. Due to the nature to the crime at hand, there is need for constant reviewing and reconstructing a legal framework for combating cybercrime, and mitigating the impact of cyber threats.

4.6 Cybercrime negatively affecting human rights

According to a Newsday publication of 25 August 2016, part of the problem with the HIPPSA Model that Zimbabwe copied, was the lack of appropriate expertise in preparing it. The model laws were based on workshop outcomes and not a consultative process. The same problem haunts the draft, which, like the model laws was based on both technological and legal ignorance that renders it obsolute in the 21st century. The draft contains the clumsy wording of a "Computer Crime and Cyber Crime". In Cyber Law, cybercrime is recognized as an overarching term that encompasses computer crime. Computer crime is, in fact, a term that is disappearing from cyber law texts and jurisprudence (Newsday, 2016). Another clumsy feature is the very purpose of the draft which is to create "a Bill for an Act to criminalize offences against computers and network-related crime". Of course, that sentence makes no sense, but the drafters saw it fit to keep that in (Newsday, 2016).

The article postulates that if one fails to articulate the purpose of the Bill, there is no point in reading everything else that follows. As trivial as this may sound, this is the reason to have the Bill revised since courts interpret legislation through the lens of the purpose which gives guidance as to how it should be interpreted.

If one wants to see what was added by the Zimbabwean authorities to the draft, a look at the visible change of fonts will be enough. The Newsday article states that the draft was hurriedly produced such that the basic tools of cut and paste were applied without ensuring uniformity. Any change of font size in the text will reveal what the Zimbabwean authorities added. The definitions in the draft are both inadequate and outdated, thereby creating both a lacuna and an absurdity, which will become visible upon the enactment of the draft.

This "modern-day" draft ignores issues to do with decryption, encryption, encrypted information, decryption keys or decryption holders. The draft does not define what data is but goes ahead to create an offence of corruption for using "false data".

The draft then creates an offence of data espionage, which is not just weird, but unfortunately inoperative, secular in meaning and quite frankly, nugatory, given the fact it is a duplicate, if not triplicate, offence. This is because the elements of this ancient offence of data espionage are already offences within the draft, which means that one would essentially get charged for doing the same thing twice, if not thrice, in terms of the same draft.

According to the Newsday (2016), the absurdity of the draft doesn’t end there. There is constant reference to offences created “in excess of a lawful excuse or justification”. With respect, that simply cannot be read logically without making a mockery of the law. Those phrases are not only foreign to Zimbabwean law, but law in general and in this regard, I want to challenge the relevant ministry to detail what those concepts mean and to demonstrate how one can ever exceed a justification. The most obvious flaw in the draft and model law is that there is blatant intrusion on the privacy of citizens by authorizing interception of data communication without sufficient oversight and checks and balances to prevent abuse which is, of course, contrary to the Constitution. In terms of the draft, police would be able to approach any court and, on the basis of an affidavit and if satisfied, the magistrate will allow interception to take place. Interception would mean that the State can lawfully have access to your private communication — at all levels (Secretary of State, 1999). The magistrate can similarly grant an order for devices to be searched and seized. This intrusive power is weirdly unchecked.

Here’s the first problem with that, the Zimbabwe Republic Police (ZRP) will have no problem in producing false affidavits to a magistrate. Simply asking that one be produced is to create a situation open to abuse. The lack of integrity within the police force is a cause for concern. For example, the ZRP has, on more than one occasion, alleged that a helmet and baton stick were stolen and on that basis, secured warrants without any substance to those

The draft unfortunately narrowly defines what child pornography is and confines it to instances of explicit sexual conduct. They have never proved their claims, but they continue to use the charge on various perceived enemies of the State. The fact that some magistrates keep supporting the police in securing such warrants is a reason why more checks are needed. History has shown us that such processes are easily abused. Privacy is one of the most dearest and personal of rights in our constitutional order so it only makes sense that intrusions are sufficiently justified.

The inclusion of an offence relating to spam is welcome but in its present form is open to abuse as potentially anything can be seen as spam. Spam is not a subject that can easily be dealt with in a few lines as the draft does. Some countries have specific legislation dealing with spam and a good example of this is Singapore (Sanchez et.al, 2016). Without the necessary amendments, the spam offence is overbroad and will criminalize innocent actions that are not seen as spam in most countries and these may include possession of pornographic materials in general apart from the usual distribution or procurement. It will thus be an offence to record a sex tape or have one in one’s computer library. It would also be an offence to publish it or provide links of the same. H-Metro will be the biggest loser in this regard but perhaps that’s not such a bad thing. To its credit however, the Draft seems capable of dealing with revenge porn since it criminalizes the possession and distribution of pornography.

In striving to be unique, the draft like the Model Law comes up with worryingly bizarre terms that are not found anywhere else in the world which thus makes it almost impractical to seek international cooperation and extradition assistance. Such terms include access providers, caching providers, hosting providers, hyperlinks providers and search engine providers. To further show that the cyber legal understanding informing the draft is both inept and elementary , the draft defines illegal ‘access’ as ‘the entering of a system’. Not only is that formulation surface level but it is also outdated and rarely used to handle cyber security in the 21st century.

Most of the offences have no sentences attached for example, the crime of illegal data interception. This again shows that the Draft was a reactionary draft that was not thoroughly prepared.

4.7 Challenges of cyber crime

Having noted that cyber-crime is an international offence, it is clear that apprehending its perpetrators is not an easy job. An individual based in New York, USA is capable of instituting a cyber-offence in Zimbabwe and the impact will be as bad as if it was done by someone in Zimbabwe. Therefore, cyber-crime is difficult to monitor. This brings us to the expenses associated with cyber security, SADC as a whole is struggling to acquire the right equipment that will enhance the monitoring of the SADC cyber-space. Notably, Zambia is amongst the few SADC countries that have a CERT, an indication that SADC is far from achieving its goal of curbing cybercrime. Regarding the expenses associated with cyber security, one cannot leave out the expensive tuition for cyber security training. Zimbabwe on its own does not have a cyber-security specific institution and establishing one will cost large sums of money.

Lastly, people lack knowledge on what cyber-crime is and are therefore victimized on a daily basis by cyber-criminals. On the other hand, there is a general belief that perpetrators of computer crimes are invisible and thus law enforcement agencies are unable to apprehend them. Resultantly, such cases go unreported and are thus not dealt with.

4.7.2 Lack of sufficient expertise

It is important to acknowledge the fact that more training institutions and universities are now beginning to offer local training, certifications and degrees in cyber-security though foreign currency shortages continue to hinder the progress of such innovations. A report from the Harare Institute of Technology (April, 2018) revealed that there is a rise in cases of “trojanized bittorent software”. A Trojan is a software that pretends to be what it is not and cybercriminals use it to defraud innocent and yet unprotected internet users. The same report talks of crypto-jacking, a form of cybercrime in which the criminals manipulate other people’s machines to get more crypto money. A high level of recklessness has been observed by law enforcement agents amongst Zimbabweans regarding bad use of pin numbers where individuals do not take extra caution towards protecting them.

Corporate organizations are encouraged to take extra caution towards securing their cyber space. A Boeing manufacturing plant suffered a ransom ware attack on 28 March, 2018 and this resulted in huge financial loses. The virus locked down all machines, and demanded that the system owners pay a ransom in crypto currency to resolve the issue. Social media reports are that Microsoft has issued patches to limit the virus’ spread, but that apparently has not completely eliminated it. This goes to show the level of vulnerability that organizations expose themselves to if no measures are taken to secure their cyber space. However, Governments are also susceptible to the threat of cybercrime as evidenced by the recent ransom ware attack on the City of Atlanta in the USA that caused serious digital disruptions in five of the city's 13 local.

The banking and finance sector needs secure, resilient, and reliable systems to ensure seamless operations and maintain public confidence in their monetary systems. Information security therefore plays an integral part in all institutions in this sector. Financial institutions are therefore prone to attacks by various kinds of criminals including cybercriminals. Voeller (2008) attests that, “to curb this upsurge, institutions across the sector are working closely to improve inter- and intra-sector communication and create private–public partnerships for information sharing and encouraging innovation”.

Dube et al. (2009), state that the first visible form of electronic innovation in Zimbabwe was in the early 1990s when Standard Chartered Bank and the Central African Building Society (CABS) installed automated teller machines (ATMs). (Kass, 1994 cited by Goi, 2005). Electronic banking in Zimbabwe has grown significantly in recent years. Gono (2012), fifteen banking institutions have already introduced mobile banking products in partnership with mobile operators and the number of banking institutions venturing into mobile banking are on the increase. The, volume of mobile payment transactions and the volumes of internet transactions also increased substantially. However, according to an interview with an official from Grant Thornton-an independent assurance and tax advisory firm, it came out that the banking and financial services sector in Zimbabwe is lagging behind with regards to cyber-security as we see failure to cope with new, emerging threats. She was of the opinion that organizations in Zimbabwe are not prioritizing IT security and that the main focus is on the functionality of the systems rather than their security. In emerging and developing economies the issue of fighting electronic fraud is a major problem owing to a number of reasons. Mostly, advances in technology are fast-paced and so are the cyber-criminals, organizations are however often far behind and the availability of advanced technologies with high capacity and connectivity make it easier to escape detection. In the African region we do not have up-to-date technical security measures and contemporary cyber-security goes beyond anti-virus packages, and firewalls (Kritznger and Solms, 2016; Harry, 2002; PWC, 2017). There is lack of resources to investigate cyber-crime and beef up required instruments to combat electronic fraud and information security packages are highly priced such that they are out of the reach of the ordinary citizens.

In the wake of ever increasing ICT advances the banking and financial services sector needs to conduct vigorous cyber fraud awareness and education campaigns. The lack of awareness among the general public on how to maintain a minimum level of security with regards to personal information or electronic property, and it is vital not only to educate the people involved in the fight against cybercrime, but also draft adequate and effective legislation (Harry, 2002; Gercke, 2011; Mwaita and Owor, 2013). Kritzinger and Solms (2012) are of the view that this is a risky situation which translates to the fact that there is a clear, but certainly not deliberate lack of cyber security awareness and education to make cyber users aware of all possible cyber threats and risks.

The Global State of Information Security Survey of 2014 states that "telecommunications reach deep into the daily circumstances of individuals, businesses, and governments. It in fact touches nearly everything, everyone and, along with energy, forms a foundation upon which all other critical infrastructure operates. Therein lies the appeal to cyber adversaries." A successful cyber - attack on a telecommunications operator is capable of disrupting services for thousands of phone clients, it can cripple businesses, server Internet service for millions of consumers and shut down government operations. Cyber- attacks against critical infrastructure are on the rise. To exemplify, in 2012, the US Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, dealt with approximately 190,000 cyber incidents involving US government agencies, critical infrastructure, and the department's industry partners. This represents a 68% increase over 2011. It should be noted that there is a striking lack of security practices that exists among telecoms organizations that have implemented customer facing mobile applications. The Global State of Information Survey of 2014 revealed that only 34% of respondents said they have created secure mobile app development processes, and just 26% employ a unique set of network and firewall policies to protect data. Encryption of data is key in safeguarding information packets in the wild, but only 27% of telecoms respondents said they encrypt sensitive data in the mobile app and just 30% employ transport encryption. However

The increasing use of mobile devices also increases the use of cloud computing services. Though the cloud has been around for a while, 50% of operators say they are using some sort of cloud service from which 57% say the technology has improved the security of their cyberspace. However, today's cyber criminals are constantly deepening and evolving their knowledge in order to take advantage of new vulnerabilities and to address these threats the operators must use activities and investments with comprehensive, up to date knowledge about information assets, ecosystem threats, and vulnerabilities.

Social media is used for communication, from sending messages, voice calls and video calls with one's family and friends. It is being used to build a network of friends, business networks, thus forcing businesses to adapt marketing strategies that involve social media as a marketing tool. Companies are creating specialized corporate social media official pages such as corporate Twitter handles, YouTube channels, or Facebook fan pages.

4.8 Conclusions

In conclusion, this chapter has presented the findings and analysis of the study. It has presented and analyzed the findings using thematic and content analysis techniques. The findings and techniques presented here answers research questions and objectives of the study. The next chapter focuses on the conclusions and recommendations.

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter concludes the research by presenting the summary of the findings, conclusions as well as recommendations. The research focuses on the threat of cybercrimes on the maintenance of peace and security in the SADC, particularly in Zimbabwe. A lot of challenges were noted and these form the basis of recommendations suggested.

5.2 Summary of Findings

5.2.1 Purpose of the Study

Cybercrimes have become prevalent and source of security threat and violation of peace in the 21st century. SADC, as a region has not been spared from this challenge. Zimbabwe as a member of SADC has not been spared too. The study sought to analyse the effects of cybercrime on peace and security in SADC in general and Zimbabwe in particular. Others studies have effectively focused on threats to peace and security in Zimbabwe from political turmoil, economic defects, but however this study argues that these factors are also caused by cybercrime, thus need to look at the latter as a single unit of analysis. Indeed countering cybercrime clearly constitutes a legitimate aim in maintaining peace and security, however, it is necessary to analyse the proportionality, necessity, legality and efficiency of some measures and their impact on the society at large. Zimbabwe's responses to cybercrime arguably go beyond the expected and prescribed limits.

5.2.2 Restatement of the Objectives

The study sought to:

- Examine the effects of cybercrime in Zimbabwe
- Evaluate the impact of counter cybercrime measures on human rights development in Zimbabwe
- Evaluate the relevance of SADC in maintaining peace and security through counter cybercrime measures
- Recommend on how to mitigate the threat of cybercrime in maintaining peace and security

5.2.3 Restatement of the Research Methodology

The nature and objectives of this study compel the researcher to follow qualitative research methodology. To design the research, the researcher employed the case study technique. This research used both primary and secondary methods of collecting data which are interviews and documentary sources, respectively. Documents which were used include journal articles, books, electronic sources as well as government reports and publications. Respondents were chosen using the purposive sampling technique where people with expertise and knowledge in this field were selected. The researcher used thematic analysis for data analysis and the information was presented using emerging themes.

5.2.4 Theoretical Framework

The study made use of the realist and strategic theoretical frameworks to explain the data gathered. From a realist point of perspective, institutions are created to further the interests of member states. Institutions like SADC can be argued to have been created to further the interests of South Africa thus need of Zimbabwe and other states to initiate domestic methods that adversely protect their interests. From a state perspective, strategy as the art and science of developing and using the political, economic, social psychological and military powers of the state in accordance with policy guidance to create effects that protect or advance national interests relative to other states, actors, or circumstances.

5.2.5 Limitations

The researcher encountered a challenge in getting in touch with targeted key informants. Some of the key informants were busy and access to them for in-depth interviews could not be afforded easily and the researcher resorted to make use of questionnaires which were filled at their convenience. The study also made use of data which was gathered through documentary search to compliment interviews and questionnaire.

5.3 Summary of Findings and Analysis

5.3.1 Relevance of SADC in Maintaining Peace and Security through Counter Cybercrime Measures

The study have found out that, although there are many notable loopholes, SADC has had SADC has come up with various pieces of legislations and structures to deal with cybercrimes as means to maintain peace and security. These structures include harmonised cyber security legal framework (ITU-HIPSSA) and the Declaration on Information and Communication Technology. This Declaration has top five priority areas which are regulatory environment for ICT, infrastructure for ICT development, community participation and governance in ICT development, ICT in business development and human resource capacity for ICT development. These organs have had positive impacts on the maintenance of peace and security in the region. However, the study has shown that SADC's organs and legislations of counter cybercrime still have some loopholes.

5.3.2 Zimbabwe's Efforts

The research found out that Zimbabwe has made significant strides in curbing cybercrime. Responsible Stakeholders such as the Ministry of ICT and POTRAZ have made significant efforts in trying to reduce the number of cybercrimes.

5.3.3 The Challenges Faced By SADC and Zimbabwe in Countering Cybercrimes

The study found out that SADC and Zimbabwe have met various challenges in countering cybercrimes in the regional and the country respectively. In the case of SADC, some major challenges it faced include the following; lack of sufficient equipment, lack of expertise and lack of equipment. It was noted that, SADC as a whole does not have the technical capacity to deal with cyber-crime. Due to the fact that Southern Africa is trailing behind technologically, people are not aware of the cybercrimes that are manifesting in their midst on a daily basis. These problems have been seen even in the case of Zimbabwe. These problems, together with many more have found it difficult to for SADC to counter cybercrimes.

5.4 Recommendations

The research recommends that;

- SADC should effectively work in harmony and shoulder by shoulder by member states in mitigating cybercrimes. Collective effort will see countries reducing the number of cyber-related crimes and subsequently SADC will succeed.

- SADC should come up with ways to train and educate people in the region about cybercrime. It also had to make sure that it has special and technical personnel that are abreast with the evolvement of cybercrimes.

- SADC has to adopt updated technology to trace, detect and counter cybercrimes. Technology has continued to develop, thus the need to develop counter strategies.

5.5 Conclusion

This chapter has presented the summary of findings, conclusions and recommendation on the topic; Cybercrime as a threat to the Southern African Development Committee (SADC) Maintenance of Peace and Security: The Case of Zimbabwe (2000-2017).

BIBLIOGRAPHY

Adams, S et.al. (2015). The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK. Tilburg University.

Akande, D. (2004). *International law Immunities and the International Criminal Court.* American Journal of International Law 98, 419-432.

AUSTRAC, (2011). Australian Transaction Reports and Analysis Centre. Money Laundering in Australia. [Accessed 30, April 2018]

ASEAN, (2016). Master Plan on ASEAN Connectivity 2025. http://asean.org/storage/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf [Accessed 30 April 2018]

Chindaro. (2017). Introduction to Proposal Writing. http://grantspace.org/training/calendar/online/introduction-to-proposal-writing-2016-2-17-webinar.

Creswell, J. (2002). *Research Design.* New York: Sage Publications

Dara, J & Gundemoni, L. (2006). Credit Card Security and E-Payment.Enquiry into credit card fraud in E-Payment. https://www.diva-portal.org [Accessed 30 April 2018]

Franz-Stefan Gacy. (2010). *Foreign policy: Africa's internet threat. National Public Radio,* 29 March 2010. Available from www.npr.org/templates/story/story.php?storyId=125297426.

Gupta, N; (2014). Analysis of Issues in Phishing attacks and development of prevention mechanism. Journal of Global Research in Computer Science Vol 5, (6). https://www.jgrcs.info/index.php/jgrcs/article/download/915/592 [Accessed 30 April 2018]

Harrell, E; (2017). Victims of Identity Theft. Bureau of Justice Statistics.

International Data Group Connect, Africa (2013): *Cyber-crime, hacking and malware.* White Paper. Available from www.idgconnect.com/view_abstract/11401/africa-2013-cyber-crime-hacking-malware.

International Telecommunications Union, (2017). Global Cybersecurity Index. https://www.itu.int/dms-pub/itu-dlo/pb/str/D-STR-GCI.01-2017-PDF-E.pdf [Accessed 30 April 2018]

Mearsheimer, J. (2016). *The False Promise of International Institutions*. International Security Journal. Winter 1994/95, 19 (3), 5-49

Morgenthau, H. (1947). Review of A Free and Responsible Press, composed by The Commission on Freedom of the Press, American Journal of Sociology, 53 (3) 22.

NewsDay, (2016). Zimbabwe's Cyber Laws- Going nowhere quickly.

Nieto, E; (2012). The Question of the Fight against Money Laundering. https://cfmuneso.it [Accessed 30 April 2018]

Sánchez, M; Loon, T & Victor, V. (2016). An Anti-spam Framework for Singapore, Media Asia, 30 (4), 240-246, DOI: 10.1080/01296612.2003.11726727

Secretary of State, (1999). Interception of Communications in the United Kingdom. A Consultation Paper.

Rolls, G. (2005). *Classic Case Studies in Psychology.* Albringdon: Holder Education

Schumacher, J. And McMillan. (1993). *Qualitative content analysis: Qualitative Inquiry,* 2(4), 320 – 336.

Siegfried, L. (2005). *Qualitative Social Research.* BeltzVerlag: Weihnhein

Simon, M. K. (2011). *Dissertation and Scholarly Research: Recipes for Success.* WA, Dissertation Success: Seattle

Symantec Corporation, (2012) Norton Cybercrime Report, September 2012.

Thompson, M, E. (1997). *Theory of Sample Surveys.* London: Chapman and Hull

Yarger, H. (2005). *The Strategic Theory*. Boston: MIT Press

ANNEXURES

Annexure A

My name is Abigail Ncube; a postgraduate student pursuing a Master of Science Degree in International Relations (MIR) at the University of Zimbabwe. I am kindly requesting for information in response to my research topic entitled **"Cybercrime as a threat to the Southern African Development Committee (SADC) maintenance of peace and security. The case of Zimbabwe (2000-2017)"**. The central objective of my study is to understand the implications of cyber threat to SADC's regional peace and security. Your participation in this research is voluntary and I also assure your confidentiality, privacy and anonymity.

Section A

1. What is your understanding of
    a. Cyber Security
    b. Cyber crime
2. What measures has SADC put in place to deal with cyber-crime?
3. Does SADC have the technical capacity to deal with cyber-crime? Please explain
4. What is your understanding of the SADC cyber security Protocol?

5. How effective has been the cyber protocol in dealing with cyber-crime?
6. What have been the major challenges in implementing Cyber security protocol in SADC?
7. What are the various forms of cyber-crimes that SADC mostly face?
8. Compared to other regional blocks globally is SADC doing enough to address this challenge?
9. In international relations how dominant is the study of cyber security as a form of modern security threats?
10. Can international relations as a field of study contribute further to the conceptualization of cyber security?

Section B

11. What is the current situation in Zimbabwe in so far as cyber -crime is concerned?
12. How has cyber-crime manifested in Zimbabwe?
13. Does Zimbabwe conform to the SADC Cyber security protocol? Please explain
14. What have been the major forms of cyber-crime in Zimbabwe?
15. What measures has the ministry of home affairs put in place to address cyber-crime?
    a. Have they been effective? Please explain
16. What are the major challenges faced by the country in dealing with cyber-crimes?
17. What has been the impact of cyber-crime on human rights development in Zimbabwe?
18. Is there any possibility that cyber security measures may negatively impact human rights development in Zimbabwe? Please explain.
19. Do you have any further comments?
20. What recommendations can you give to the Zimbabwean Ministry of Home affairs?

Thank you