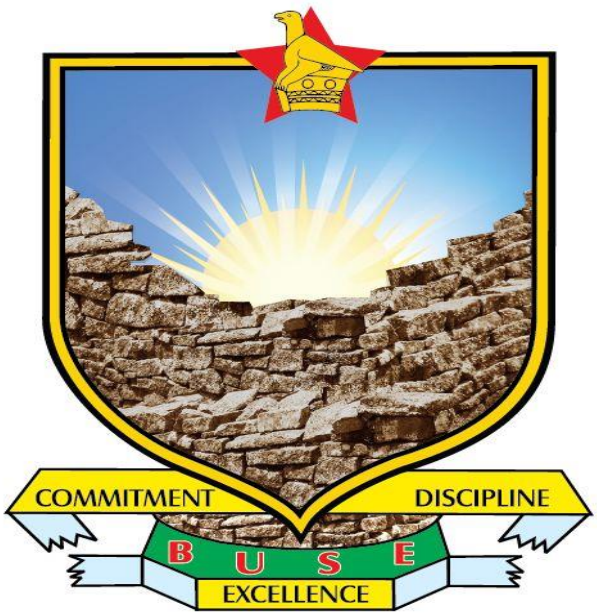
CYBER CRIME AS A THREAT TO SADC'S PEACE AND SECURITY: THE CASE OF ZIMBABWE

BY

Jacqueline Rumbidzai Tanhara (B1644828)

A Dissertation submitted in partial fulfilment of the requirements for the Master of Science Degree in International Relations.



Faculty of Social Sciences and Humanities

Supervisor: Dr. J. Kurebwa

Bindura, Zimbabwe

October 2017.

ABSTRACT

The purpose of this study was to understand the effects of cyber crime as a threat to SADC's peace and security with specific reference to Zimbabwe. Qualitative methodology and a case study research design of Zimbabwe was used as a case study. Primary data was gathered through key informant interviews, while documentary search was used to review scholarly literature on the subject. Key informants for the study were drawn from institutions and organisations that specifically deal in combating cyber crime. The key findings of this study are that SADC as a region does not have adequate and effective legislative instruments to combat cyber crime. Zimbabwe as a country is also lagging behind in terms of legislative provisions on cyber crime. The key findings reveal that cyber crime is a threat to peace and security in the sense that it can be used to bring down the critical infrastructure upon which the country depends, for example, the banking system. It can also be used to disrupt communication thus bringing down communication networks. Recommendations for this study include prevention and awareness; training and development; development of new technology and introduction of new laws and updating of current legislations.

DECLARATION FORM

I JACQUELINE R. TANHARA declare that the research project herein is my own and has not been copied or lifted from any source without the acknowledgement of the source.

Signed

……..

Date

……..

DEDICATION

I dedicate this research to my parents Mr and Mrs C.C.R Tanhara for their unwavering support and love. Without their encouragement this research would not have been completed.

ACKNOWLEDGEMENTS

My deepest gratitude goes to My Creator and God for the spiritual inspiration that fortified me to script this document to the last dot and for being my greatest pillar of strength throughout my research work. I will remain prayerful and honourable to your existence. To my academic Supervisor and mentor, Dr. Jeffrey Kurebwa, words are not enough but only to say thank you for your professional guidance, mentorship, intelligent and expert advice throughout this whole project. Your patience and constant drive made this dream a reality. To my brothers and sisters, my two daughters Tanyaradzwa Renee Chiduku and Kirsten Nyapadi, my friends Eustina Macheka, Tracy Matyatya, Eugene Ncube and most importantly Dr. Bendick Mahleko for not giving up on me during my weakest moments and for your constant support, and laughs that lightened up my hardest moments, I thank you.

I am grateful to many people who shared their memories, experiences and expertise, especially all the respondents who participated throughout this research. To my former Boss Dr. M.C. Tapera and all my current work colleagues at Chinhoyi University of Technology, I believe I was placed under your leadership for this specific reason that I now see come to life.

I must acknowledge all members of staff of the Faculty of Social Sciences, Department of Peace and Governance for their emotional and intelligent support. Although I have dedicated this research to my parents earlier, I feel overwhelmed with tears as I think of my mother's undying love as she took care of my daughters while I ate into the night to complete my project. Mom and Dad you are the greatest. I thank you.

LIST OF ABBREVIATIONS AND ACRONYMS

CIPIT- Centre for Intellectual Property and Information Technology

COMESA- Common Market for Eastern and Southern Africa

ECOWAS- Economic Community of West African States

FICA- Financial Intelligence Act

GSA- Global Security Agenda

ICT- Information, Communication Technology

ISP- Internet Service Provider

RICA- Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA)

SADC- Southern African Community Development

UK- United Kingdom

UNECA- United Nations Commission for Africa

USA- United States of America

TABLE OF CONTENTS

CHAPTER ONE

1.0 INTRODUCTION

1.1Background of the Study

As the volume of cyber-attacks or cyber terrorism continues to rise and also the levels of harm suffered from them, it is becoming critical that organisations can demonstrate that reasonable efforts are being undertaken to reduce cyber-risk. Computers and networks gained widespread use from the 1980s. Responsible hacking was then used to explore computer networks and improve their efficiency. At this stage, hacking did not pose any threat to economies or individuals, but over the years the sector was penetrated by criminals who used their knowledge and expertise to derive benefit by exploiting and victimizing others. This marked the beginning of cybercrime.

According to the recent online report by PWC, digital technology continues to transform and disrupt the world of business, exposing nations to both opportunities and threats. So it's hardly surprising that cybercrime continues to escalate – ranking as this year's second most reported economic crime. As the world goes digital, people have become the top target for cyber criminals as opposed to machines. The International Technology Unit (2014), regards cyber criminals as computer savvy individuals who look for vulnerabilities that can be easily exploited. Such attacks as viewed by Eichner (2012) can take different forms where a computer terrorist could break into a company's computer network causing havoc, sabotage a country's gas lines or wreak havoc on the international finance system. Hoscheidt (2012) is of the view that these cyber attacks against information infrastructures, computer systems, computer programmes and data may cause injury, loss of life, reputational damage as in the cases of social media abuse and destruction of property. The aim of such unlawful attacks is to intimidate or persuade a government or its people to further a political or social objective.

Mutisi (2017) views cyber attacks as breaches in data security and sabotage. Personal data, intellectual property, trade secrets and information relating to bids, mergers and prices are tempting targets for data security breach. Cyber attack methods as in the eyes of Sikuka (2012) are also said to possess many advantages over conventional terrorism.

Since the beginning of the 21st century, Africa has continued to witness a phenomenal growth in Internet penetration and the use of ICTs. According to Ka Mtuze (2015), statistical data indicates that Internet users in Africa grew from 4,514,400 million people in 2000 to 297,885,898 million people in June 2014. This phenomenal growth which is still in progress, has been linked to factors such as the liberalization of the telecommunications market in African States, the widespread availability of mobile technologies, and the increasing availability of broadband systems. Microsoft estimates that by 2020, up to four billion people will be online and that will double today's figures for what is known as the "human attack surface" or the number of people who can be targeted by cyber criminals online. This means cyber crime will continue to grow as a lucrative industry for criminals.

According to a report by Thomson Reuters Accelus, the global cost of cybercrime will reach $2 trillion by year 2019, a threefold increase from the 2015 estimate of $500 billion. The cybercrime cost figure above may be the tip of the iceberg. The Global Risks Report (2016), indicates that "from the World Economic Forum, a significant portion of cybercrime goes undetected. This is particularly true in the case of industrial espionage and the heist of proprietary secrets, because illicit access to sensitive or confidential documents and data is hard to detect." The increasingly networked world people live in now, from personal banking to government infrastructure set of connections brings about a lot of cyberspace vulnerabilities. Protecting those networks is no longer optional. Cyber crime is now at the top of the International agenda as high-profile breaches raise fears that hack attacks and other security failures could endanger economies (Mutisi, 2017).

According to Kizza (2013), the spread of ICTs and Internet penetration in African states has also raised concerns about cyber security at regional and sub-regional governance forums thereby contemplating various legislations by African Countries of which some are still in the process of coming up with such legislations guarding against cyber crime. Consequently, according to Manarcoda (2012) some African intergovernmental organizations and regional groupings developed legal frameworks for cyber security. South Africa is one typical example of a nation that is at high risk of cyber attacks where it is already perceived that it is the initial hub for cyber criminals and terrorists following its unprecedented levels of uncontrolled criminal activity.

The convergence of the physical and virtual worlds has resulted in the creation of a "new threat" called cyber terrorism. Before 9/11, as noted by Schjolberg (2008), much apprehension arose about the threat of cyber terrorism including fears about a "digital Pearl Harbour". The millennium bug commonly referred to as September 9/11 where the World Trade Centre and the Pentagon was bombed by terrorists further enhanced this fear. In the context of post 9/11, the threat of cyber terrorism is often linked to Al-Qaeda, ISIS and other terrorist organisations.

The horrific events of 9/11 provided the impetus for many Western countries to introduce anti-terrorist legislation. Such anti- terrorist legislation not only focuses on legislation to criminalise cyber terrorist activity and impose penalties proportional to the act but also to prevent cyber terrorist activity or mitigate its impact by denying cyber terrorists materials, finance, support and equipment. The September 11 attacks as noted by Ka Mtuze (2015) illustrated that terrorism crosses national and ethnic boundaries and changed the prevailing attitudes to terrorism. Indeed, after 9/11, the discussion about cyber security and cyber crime took centre stage. The United States of America introduced the Patriot Act of 2001 in response to the 9/11 attacks on its soil.

Jeong (2011) points out that South Africa has introduced a number of legislative measures to address the growing threat of cyber terrorism and terrorist financing such as the Prevention of Organised Crime Act 38 of 1999 ("POCA"), the Financial Intelligence

Centre Act 38 of 2001 ("FICA"), the Electronic Communications and Transactions Act 25 of 2002 ("ECT), the Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 ("RICA") and the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 ("PCDTRA"). Zimbabwe has recently introduced a cyber bill although it is still at its infancy to be launched. The study will also examine the guidance that is being given to these developing nations that are rapidly deploying information and communication technologies.

1.2 Statement of the Problem

SADC has not done much to promote cyber security in Zimbabwe. Information technologies is breeding extremism, promoting terrorism, crime, xenophobia, potential cyber war and all forms of violence. As the use of cyberspace and ICT networks increases, global threats from a wide variety of sources including criminals, hackers and other agents are manifesting themselves in cyberspace with disruptive criminal activities that target individuals, businesses, national infrastructure and Governments. According to Cletty (2014), it is being viewed by critical thinkers as a threat to peace and security. Technological evolution as noted by Cassim (2012) has a lot of repercussions in the field of international relations and drastic consequences. It has sidelined traditional diplomacy and has failed to stop the emergencies of cyber war and various conflicts. According to Malik (2012), developments in advanced technologies such as the next generation microelectronics, nanotechnology, biotechnology, robotics and artificial intelligence will upset existing balances of power and shape military capabilities for future conflicts. Governments must ensure the security of cyber space and critical infrastructure such as telecommunication networks, electric power grinds, air transport, roads and railways however, the existing SADC legal instruments are not providing adequate frameworks for mutual assistance and international cooperation on cyber security and cyber terrorism control for South Africa and Zimbabwe. As such these countries are at high risk of cyber attacks despite attempts of setting up various legislations that promote

cyber security. To this effect national security is threatened and at high risk of cyber attacks as there is clear and adequate legislation guarding against cyber terrorism in particular

1.3 Purpose of the Study

The purpose of the study is to understand the risks associated with the rise of technologies in Africa and the role SADC is playing in combating cyber crime in Zimbabwe.

1.4 Research Objectives

1) To examine the challenges brought about by ICTs in International Relations.
2) To understand cyber crime issues in Zimbabwe.
3) To assess the effectiveness of Zimbabwe's legislature in promoting cyber security.
4) To evaluate the role played by SADC in combating cyber crime in Zimbabwe.
5) To provide recommendations that improves SADC roles in curbing cyber crime.

1.5 Research Questions

1 What do you understand by the term cyber crime?

2 How is cyber crime a threat to peace and security?

3 How effective is Zimbabwe's legislature in promoting cyber security?

4 What measures can be put in place to combat cyber crime?

1.6 Significance of the Study

The study is of paramount importance to the following:

SADC- This study is crucial to SADC officials for purposes of policy making and legislatures as well as reviews. This will provide also recommendations for future interventions thereby promoting cyber security and dealing away with potential cyber terrorist attacks. The research will go a long way to help these to come up with different frameworks of combating terrorism. The whole study will enhance the impact of regional cooperation to promote peace and security.

Zimbabwe- The study is also crucial to Zimbabweans so that they become aware of cyber terrorism and be able to come with effective ways to combat cyber crime. Information Communication Technology gives power to non state actors. With ICTs they have found a platform to air out their views pertaining the politics, economics and social issues in the international system. They have become the main users of the internet and all information and communication accessories. The general people will be conscientised about the consequences and implication of ICTs.

ICTs Organizations- These comprise of software developers, inventors and promoters of ICTs. It is fundamental that they also understand the negative impact of ICTs and try to develop technologies that are secured or that by all means would not threaten national security.

Academics- From the study findings, scholars will be equipped with the skills and knowledge on the cyber security issues here in particular cyber crime or cyber terrorism. It will also enable them to conduct further research.

1.7 Assumptions

1) With the increasing ICTs, Zimbabwe is at high risk of cyber attacks.
2) SADC has not come up with effective measures to combat cyber crime.

1.8 Delimitations of the Study

The prime focus of this study is to understand the role of SADC in combating cyber crime. The area of focus mainly is SADC, Zimbabwe. However, special references of where cyber terrorism has taken place will also be given. The timeframe will stretch from 2015 to 2017. The study is not going to cover all issues to do with cyber crime as it is a very broad topic. It is also not going cover on what other regional groupings are doing to combat cyber crime.

1.9 Limitations of the Study

Availability of key informants- Meeting key respondents such as the senior officials in the Ministry of ICT and SADC officials was difficult. This delayed the completion of this study. The Researcher had to reschedule the interview dates.

1.10 Definition of Key terms

i. **ICT (Information Communication Technologies) -** According to Calder and Watkins (2012), Information technology (IT) security includes data, computing, information and network.

ii. **Globalisation**- Globalisation is defined by Kozul-Wright and Rowthorn (1998) as an increase in the volume of cross-border economic interactions and resource flows, producing a qualitative shift in the relations between national economies and between nation-states.

iii. **Cyberspace**- Conway (2007) regards it as the meeting place for criminal groups. Cyber space has recently emerged as the latest battleground in this digital age.

iv. **Cyber terrorism**- According to Cassim (2011) it is one of the recognised cyber crimes and has been defined as the "premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in the furtherance of such objectives.

v. **Cyber crime**: is referred by Ayofe and Irwin (2010) as any illegal behavior directed by means of electronic operations which target the security of computer systems and the data processed by them.

vi. **Cyber security**: The ITU (2014) defined the term as “the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organization, as well as users’ assets”.

1.11 Chapter Outline

The research report will be presented in five chapters.

Chapter One - Introduction

It consists of statement of the problem, significance of the study, objectives and ethical considerations. The chapter also gives the background of the study as well the justification of the study. It also provides definitions to the main terms that are going to be used throughout the whole project.

Chapter Two - Literature Review and Theoretical Framework

It provides the rationale of the research project. It is important because it gives reference to previous findings on the area of study. Also included in this chapter are principal theories upon which the study research project will be constructed. The chapter also gives case studies of where cyber crime has taken place and various legislations in place to promote cyber security. It also increases the understanding of cyber crime and cyber security issues as well as the role of SADC in combating cyber crime.

Chapter Three- Research Design and Methodology

This explains fully the methods used for data collection and different sources of data. This will mainly describe the basic research plan. The research design and methodology will focus on the qualitative research methodology as it provided the research instruments for the study.

Chapter Four - Data Presentation, Analysis and Discussion of Findings

Special attention will be given to the data collected from a sampled household population within the study area. Under discussion will also be findings from focus group discussions and interviews. The Chapter provides the discussion of findings in relation to previous research.

Chapter Five- Summary, Conclusions, Recommendations and Areas for further Research

This concludes the study and makes recommendations. It is the summarization of the main findings. The chapter discusses a summary of the findings, and includes a conclusion as well as the limitations of this study. It also offers recommendations for actions to respond to the research problem and for future and further research.

CHAPTER TWO

2.0 LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 INTRODUCTION

In this chapter the research looked at studies on the role of SADC in combating cyber terrorism. The researcher will focus on the issues underpinning the cyberspace and the relevance of Information Communication Technologies. The study will look into various debates on cyber terrorism and different legal frameworks being signed to contain cyber terrorism. The rest of the themes will then focus mainly on case studies and the background of South Africa and Zimbabwe. It will also look at what other regional and continental blocs have done to combat cyber terrorism. This chapter also discusses the theoretical framework to be used in the research.

2.2 Theoretical Framework

2.2.1 The Globalization theory

The globalisation theory can be used by the researcher to understand the importance of ICTs in International relations. According to Wallenstein (2012), the world is becoming a small village through the deepening and widening as well as the interconnectedness amongst states. It is through globalisation that there is now rapid technological advancement. In this particular scenario globalisation has brought about the advancement of Information and Communication Technologies. Radunovic (2010) notes that rapid development of information and communication technologies (ICT) has lead to significant changes in social, economical and political relations of the modern society. Access to information and control over it contribute to the prevalence of soft power in politics of digital age, and empower the non-state actors in international relations.

The dynamics of globalization unleashed by technology is transforming relations amongst nations. Technological advances as viewed by Kizza (2013) have emerged as the principal agents of social, economic and political change, drawing the world closer whilst also dividing it.

The "revolution in dual-use technologies" for instance, is generating fundamental transformations both in the way wealth and power is created and wars are fought because technology diffusion is now virtually instantaneous and unstoppable. Unlike in the past, Julich (2015) notes that technology diffusion now takes place at its most advanced level. Commercial satellites, GPS readings, space-based imagery, weather data, and Internet data – they all have potential military applications in communications, navigation, intelligence and operation support. The "equalizing" feature of ICT as viewed by Knapp, Mamis (2009); has also lent non-state entities more power to initiate societal change and to address the broadest audience possible in virtual time, undermining in some cases the monopoly of the modern state to govern and rule. Using suicide bombers and improvised explosive devices as their technologies of choice, terrorist groups – considered non-state players in the international arena have exposed the shortcomings of traditional war-fighting responses and created new vulnerabilities for states – Cyber Terrorism.

Technologically advanced nations also enjoy the power to set the norms and standards of behaviour in international politics. Kim and Geong (2011) concur to say that great powers, in particular, compete ferociously to maintain their top dog status through their edge in technology. Most high-tech developments are driven by the competitive national quest to maintain the technological superiority over others. Military strategists, in particular, see superior technology as the key to remaining ahead of enemies and competitors. According to Jirasek (2012), technological advances invariably upset existing power balances and shape military capabilities for future conflicts. The restrictions on the transfer of high technology have long been a bone of contention in Washington's relations with both New Delhi and Beijing. But global technological diffusion will continue to be uneven, and will allow some nations who have the

technological edge to gain strategic advantage over others. The changes in geopolitical systems of trade, offshore production by multinational corporations, and intellectual property protection, coupled with advances in ICT, have helped globalize research and development (R&D) activities.

Barman (2002), puts forth the idea that in a globalized world economy, countries will take advantage of their comparative technological advantage over others. Access to technology (or the lack of it) will determine a country's place on the pecking order in the regional and global hierarchy.

According to Alfred Thayer Mahan, 'in a globalized world economy, whoever has the technological edge will dominate the world. In the 21st century, the destiny of the world would be decided in the Science and Technology field. Short of wars, major power rivalries and alliances will revolve around technology, resources and trade. Technology could help moderate great power competition and hopefully, prevent wars as nuclear weapons technology did after the Second World War. Advancements in technology will not only change the way we live and fight, but also the way our world is organized. As technological advancement brought about globalization have given rise and power to non state actors (Terrorist groups) thereby risking the possibilities of what is known as cyber terrorism.

2.3 The Role of ICTs in International Relations

Information and Communication Technologies were born out of Cold war politics. Bazelon (2006); notes that the relevance of breakthrough technologies gained much prominence in the 21st century. The impact of unprecedented advancements in information technologies is heavily contested in International relations. According to Kluz and Firlej (2015), technology has enhanced communication, raising awareness, spreading democracy throughout the world.

However pessimists like Kritzinger (2008), have condemned technology stressing repercussions of tottering national and digital security. Although cyber terrorism has become a more dominant force in the global battle between information and network

warfare, much misconception still exists over what cyber terrorism entails. As stated earlier, it is important to recognise that all "cyberspace-based threats" are not necessarily terrorism. According to Stohl (2012), the concern with the threat of cyber terrorism stems from a combination of fear and ignorance. Stohl maintains that the discussion about cyber security also involves some misinformation and the exploitation of fears of the general public. The failure to distinguish between hacktivism and cyber terrorism has also contributed to the fear and hype about the threat of cyber terrorism. Some writers believe that the media has also exaggerated the possibility of cyber terrorist attacks causing much concern and panic in the public domain. However, the number of potential targets and the lack of proper and adequate safeguards have also made addressing the threat a daunting task. One should also not underestimate the risk and potential of future threats. Thus, a need arises for the re-examination of commonly held beliefs about the nature of computer systems and cyber terrorism.

To this end, measures to address cyber security, to introduce adequate cyber terrorist legislation and to make software safe and effective should be introduced. One should also bear in mind that the removal of technical information from the Internet (such as information on how to execute terror attacks), does not provide an adequate guarantee to safeguard the Internet as such material can be easily loaded onto offshore or other international severs. Gordon and Ford maintain that an urgent need arises for the development of minimum standards of security for computer networks. They also endorse the idea of negotiations to resolve long-standing disputes with terrorist groups, the careful use of surveillance techniques to gather information on terrorist communications and the sharing of information across various public and private sectors to combat terrorism.

2.4 The European Convention on Cyber Crime

The Convention on Cyber Crime (ETS no 185) ("ECCC") is the first international treaty addressing crimes committed via the Internet and other computer networks. It was signed by member states of the Council of Europe and by non-member states in

Budapest on 23 November 2001. It came into force on 1 July 2004. It deals specifically with infringements of copyright, computer-related fraud, child pornography and violations of network security. It is submitted that articles 2-6 which address offences against the confidentiality, integrity and availability of computer data and systems, may be used to address the offence of cyber terrorism. The Convention also contains a range of powers and procedures addressing the search of computer networks and the interception of computers.

Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. An international 24/7 network of contacts requires all participating countries to establish points of contact for transnational investigations that are accessible 24 hours daily, 7 days a week. South Africa is the only African country to sign the European Convention on Cyber crime (ECCC). However, it still needs to ratify and accede to the ECCC. Its ratification of the ECCC will garner much needed support in its fight against cyber terrorism. International co-operation is also necessary to fight cyber terrorism.

A Global Security Agenda (GSA) was launched by the International Telecommunication Union in Geneva during May 2007. The GSA strives to provide a global framework for dialogue and international cooperation. Its objective is to coordinate an international response to the increased challenge to cyber security and to enhance confidence and security in the information society. The GSA also calls for the development of cyber crime legislation that is globally applicable and consistent with existing national and regional legislative measures. It is submitted that South Africa should become involved in such an initiative to enhance its cyber security measures.

It is submitted that South Africa can also learn from the approaches followed in other countries such as the United States, the United Kingdom and India. To this end, South Africa can also use increased surveillance measures against terrorist websites and set up

a counter terrorist strategy to address radicalisation on the Internet. Indeed, South Africa should not become complacent. South Africa can also examine the success of Internet filtering measures introduced in countries like Saudi Arabia. Saudi Arabia introduced the Internet Service Unit during 2000 to filter web traffic from ISPs (Internet service providers) before permitting users access to the contents. The result is that if the requested URL is blacklisted, then the user is directed to a page that informs him or her that access to the requested page has been denied.

It is submitted that such measures may prevent access to illegal websites that promote cyber terrorism and pose a serious threat to the government's national security. However, such measures may well infringe the constitutional right to privacy in section 14 of the South African Constitution of 1996. It is noteworthy that the USA Patriot Act, the UK's anti- terrorism laws and the Information and Technology Amendment Act 2008 in India have all been criticised for violating the constitutional rights of citizens in their respective countries. Therefore, South Africa needs to be wary of jeopardising basic human rights and freedoms in its quest to tackle cyber terrorist threats in the future.

2.4 The AU Convention on Cyber Security and Personal Data Protection

The AU commenced the development of regulatory initiatives on cyber security towards the end of the last decade and the development of cyber security initiatives could be traced to the low penetration of ICTs in Africa prior to the widespread proliferation of wireless technologies within the last decade. One of the first AU statements on the need to promote cyber security is found in the AU Draft Report on a Study of the Harmonization of Telecommunication, and Information Communication Technology Policies and Regulation (2008).The objective of this Convention was to propose the adoption at the level of the African Union, a Convention establishing a credible framework for cyber security in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime.

Article III – 1 – 1: Laws against cyber crime- Each Member State shall adopt such legislative measures as it deems effective to set up material criminal offenses as acts which affect the confidentiality, integrity, availability and survivability of ICT systems and related infrastructure networks; as well as effective procedural measures for the arrest and prosecution of offenders. Member States shall take into account the approved language choice in international cyber crime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations where necessary.

Article III – 1 – 5: Harmonization- Each Member State shall ensure that the legislative measures adopted in respect of substantive and procedural provisions on cyber crime reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures.

The Report noted *inter alia* that emerging questions that needed to be addressed in the converged ICT environment include the "tracing and combating of cyber crime in all its forms (hacking, virus propagation, denial of service attacks, credit card fraud, etc)". The Report also emphasized the need for the establishment of a harmonized regional policy and regulatory framework on cyber security. Subsequently, on the 5th of November 2009, the AU Ministers in charge of Communication and Information Technologies adopted a set of declarations known as the *Oliver Tambo Declaration*. The Declaration directed the AU to "jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection". It also recommended that AU Member States should adopt the Convention by 2012.

In 2011, the efforts of the AU and UNECA led the development of a draft framework on cyber security known as the Draft Convention for the Establishment of a Credible Legal

Framework for Cyber security in Africa. The Draft Convention was subsequently adopted by the AU Expert Group on Cyber security in September 2012. This was also followed by its approval by the 22nd Ordinary session of the AU Executive Council in January 2013. Several petitions by civil society groups and members of the academia were forwarded to the AU Commission to prevent the adoption of the Draft Convention following concerns that some of its provisions may harm the right to privacy and freedom of expression. Other concerns included lack of wide consultations and the absence of some critical governance mechanisms.

The Centre for Intellectual Property and Information Technology Law (CIPIT) at the Strathmore University, Kenya led the opposition to the Draft Convention and also established an online petition to prevent its ratification. Following these developments the Information Society Division of the AU Commission gave further room for the consideration of those concerns till 31 May 2014. Later on 27th June 2014, the AU Heads of State and Government adopted a revised version of the draft Convention during the 23rd Ordinary Session of the AU Assembly in Malabo.

The Convention which is known as the AU Convention on Cyber Security and Personal Data Protection aims to harmonize the laws of African States on electronic commerce, data protection, cyber security promotion and cyber crime control. The Convention recognizes that cyber crime "constitutes a real threat to the security of computer networks and the development of the Information Society in Africa". To a great extent, the Convention adopts a holistic approach to cyber security governance by imposing obligations on Member States to establish national legal, policy and institutional governance mechanisms on cyber security. This approach apparently goes beyond that of the Council of Europe Convention on Cybercrime which focuses on the criminalization of cyber crimes and the establishment of procedural mechanisms for law enforcement and international cooperation.

2.5 The ECOWAS Directive on Fighting Cybercrime

In August 2011, the ECOWAS Council of Ministers adopted the Directive C/DIR.1/08/11 on Fighting Cybercrime at its Sixty Sixth Ordinary session at Abuja. The Directive imposes obligations on Member States to criminalize cyber crime and also establishes a framework to facilitate international cooperation on cyber security. In this respect, article 33(1) of the Directive provides that:

Where Member States are informed by another Member State of the alleged commission of an offence as defined under the Directive, such Member States shall cooperate in the search for and establishment of that offence, as well as in the collection of evidence pertaining to the offence.

The Directive also provides that "such cooperation shall be carried out in line with relevant international instruments and mechanisms on international cooperation in criminal matters. Applicable ECOWAS instruments on international cooperation include: the ECOWAS Convention on Mutual Assistance in Criminal Matters and the ECOWAS Convention on Extradition.

The ECOWAS Convention on Mutual Assistance in Criminal Matters establishes a broad Framework for the rendition of mutual assistance amongst ECOWAS States where there is an absence of applicable international agreement between them on the basis of a reciprocal legislation. Under the Convention, Member States are required to afford each other "the widest measure of mutual assistance in proceedings or investigations in respect of offences the punishments of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Member State". Thus, within the framework of the Convention, every ECOWAS Member State has an obligation to render mutual assistance to all other ECOWAS States where such assistance is requested with respect an offence that constitutes a crime in both the requesting and requested Member States, regardless of the absence of an applicable bilateral mutual assistance agreement between the requesting and requested Member States.

The ECOWAS Convention on Extradition also establishes a broad framework for the rendition of extradition requests between ECOWAS Member States. Thus, the Convention requires Member States to render extradition requests on the basis of dual criminality regardless of the absence of a bilateral extradition treaty between the requesting and requested Member States. Accordingly, the existence of the above ECOWAS Conventions on mutual assistance and extradition creates a broad framework on which ECOWAS Member States that have established cyber security laws can render mutual assistance and extradition requests to other ECOWAS States on the basis of dual criminality and regardless of the absence of applicable bilateral mutual assistance or extradition treaties.

2.7 The COMESA Model Cybercrime Bill

In October 2011, the COMESA established a Model Cybercrime Bill to provide a uniform framework that would serve as a guide for the development of cyber crime laws in Member States, however, the Bill does not establish any binding obligations on Member States to criminalize cyber crimes. The Bill largely adopts the language and model of legal instruments such as the Council of Europe Convention on Cybercrime and the ITU Toolkit for Cybercrime Legislation. It also establishes an elaborate guide for the development of general framework to facilitate international cooperation, extradition, and mutual assistance and provides for the establishment of national 24/7 points of contact. However, despite its framework on international cooperation, the Bill only serves as a mere guide or model for development of national cyber security laws in Member States. Thus, the Bill does not establish any international cooperation obligations on Member States and neither can it be used as a legal instrument for cooperation amongst Member States. Also unlike the ECOWAS, the COMESA does not have any existing legal frameworks to facilitate mutual assistance and extradition among Members. As such, COMESA Member States that have used the Bill to develop their national laws would still have to enter into separate bilateral arrangements with other Member States in order to obtain any form of international cooperation or mutual assistance.

2.8 The SADC Model Law on Computer Crime and Cybercrime

Africa comprises of 55 sovereign states and it is classified as the world's second largest and second most populous continent after Asia, with a terrestrial mass of 30, 2044, 049 million square km and a human population of over one billion people. The continent has five geographical sub-regions, comprising of: Southern Africa, Central Africa, East Africa, North Africa, and West Africa. The AU is the most prominent regional intergovernmental organization that unites African States and it comprises of 54 sovereign States with Morocco being the only sovereign State that is not a member of the union. Some notable intergovernmental organizations that operate within Africa's sub-regions include: the COMESA which comprises of 19 Member States, the ECOWAS15 which comprises of 15 Member States, and the SADC which comprises of 15 Member States.

In March 2012, the SADC adopted the Model Law on Computer Crime and Cybercrime to serve as a guide for the development of cyber security laws in SADC Member States. However, it does not impose any obligations on Members to establish cyber crime laws. It does not also establish any provisions to guide the development of international cooperation regimes in Member States and neither does it establish any international cooperation obligations on Member States. However, Members that have established cyber security laws may rely on the SADC Protocol on Mutual Legal Assistance in Criminal Matters and the Protocol on Extradition to obtain international cooperation from other Members. Under the SADC Protocol on Mutual Assistance, Member States are required to provide each other with "the widest possible measure of mutual legal assistance in criminal matters". The Protocol also requires that such assistance shall be rendered without regard to whether the conduct which is the subject of the mutual assistance request by a Requesting State would constitute an offence under the laws of the Requested State.64 On the other hand, the Protocol on Extradition requires that SADC States can only obtain cooperation amongst themselves on the basis of dual criminality.

From a critical point of view, the AU Cyber Security Convention does not provide an adequate framework for international cooperation and mutual assistance amongst African States. However, there is the existence of international cooperation and mutual assistance mechanisms within two African sub-regional groupings, the ECOWAS and the SADC. Consequently, Africa has a situation whereby there is no regional wide cooperation and mutual assistance on cyber security, thus resulting in the limitation and fragmentation of cooperation and mutual assistance along sub-regional and bilateral arrangements. While it is agreed that cyber threats that affect African States may also emanate from outside the continent, which also underscores the need for wide international cooperation amongst all States, however the development of a framework for such global cooperation is beyond the SADC and the scope of this study.

2.7 The Case of USA

Since September 11, concerns about cyber terrorism in the United States have multiplied. The USA Patriot Act of 2001 was enacted By President George Bush in response to the 9/11 attacks on the World Trade Centre and Pentagon. Although the USA Patriot Act addresses several issues, certain key provisions relate to cyber security and other computer concerns. To this end, the Act has eased restrictions on electronic surveillance to facilitate the capture of terrorists. The Act also contains anti-money laundering provisions in order to prevent terrorists from achieving any financial gain from their actions. The Patriot Act also includes terrorism and computer crimes on its list of offences. However, the Act has been criticised for violating the civil rights of ordinary American citizens.

Cyber terrorists are said to have the ability to cripple critical infrastructure such as communication, energy and government operations. Cell phones have also been used to track terrorists and to provide evidence against them. Terrorist websites are also under increased surveillance since 9/11 to strengthen the fight against terrorism. A call has also been made for the development of cyber intelligence as a better co-ordinated

government discipline to predict computer-related threats and deter them. A bill on cyber security is currently being debated by the US Senate. The bill is aimed at the protection of critical infrastructure such as power and phone companies, water and treatment plants and wireless providers. The enactment of the USA Patriot Act and other measures taken by the American government demonstrates the government's commitment to combat international terrorism including cyber terrorism.

2.8 The UK Experience

The Terrorism Act of 2000 was introduced to address terror attacks in the United Kingdom. The listed prohibited actions include endangering another person's life or creating a serious risk to the public health or safety, acts designed to seriously interfere with or disrupt an electronic system and acts involving serious violence to or death to another person or serious property damage. Section 1(2) (e) of the Terrorism Act 2000 describes a terrorist act as one that "is designed seriously to interfere with or seriously disrupt an electronic system". The inclusion of this section is said to consider cyber terrorism. This phrase might contemplate cyber terrorism including for example, attacks on banking services through the internet and destruction of computer-stored data. The emphasis on "serious" is said to be important as "a costly nuisance" does not amount to cyber terrorism.

In response to the September 11 attacks, the British Government passed the Anti-Terrorism, Crime and Security Act of 2001. On 14th December 2001, the British Anti-Terrorism, Crime and Security Act became law. Its object is to ensure the Government has adequate powers to counter the increased threat of terrorism in the United Kingdom following the events of September 11th. This Act has also been the subject of criticism. The Terrorism Act of 2006 was introduced in response to the 2007 London bombings. Provisions in the Act now make it illegal to 'glorify terrorism' and distribute terrorist publications. The Terrorism Act of 2006 also allows groups or organisations to be banned for those offences and covers anyone who gives or receives such training.

The Act also creates new offences of undertaking terrorism training, preparation or planning of a terrorist act and disseminating terrorist publications. The Act has been criticised by human rights campaigners and concerns have been raised about the issue of "glorification". Section 17 of the Act facilitates the prosecution of terrorist offences committed outside the United Kingdom.

Information available on the Internet is being used not only by sophisticated terrorist groups but also by disillusioned and unhappy individuals who are prepared to use terrorist tactics to pursue their agendas. To illustrate this, in 1999, a right-wing extremist David Copeland planted nail bombs in different areas of London. His actions targeted multi-racial communities and the gay community, and he killed three people and injured 179 over a period of three weeks. At his trial, Copeland disclosed that he learned his deadly techniques from the Internet by downloading copies of *The Terrorist's Handbook and How to Make Bombs: Book Two.*

Thus, the United Kingdom government is seeking protective measures against the cyber terrorist threat. To this end, the United Kingdom government has also set up the National Technical Assistance Centre which is a surveillance advice and interception facility. A call has been made to introduce a new offence that would render data inaccessible, introduce the use of more effective filtering mechanisms, educate the general public about cyber terrorism and create public-private partnerships to address security strategies in the computer industry. Terrorists are said to be increasingly using online technology to perpetrate cyber attacks and communicate their propaganda. Hence, the British Government has also recently launched a counter-terrorism strategy to keep pace with evolving technology and counteract radicalisation on the Internet.

A Cambridge technology company Plextek is also urging the UK Government to create a Cyber Attack Prevention Agency to effectively protect the national critical infrastructure against cyber terrorism. A recent proposal by the government to introduce a new strategy of interception of communication has been criticised by civil society as it

will lead to a violation of people's privacy. The above discussion demonstrates that the UK Government is taking the cyber terrorist threat seriously. The government has recognised that it has a primary duty to maintain security in all spheres of government. However, it remains the responsibility of human rights campaigners to monitor carefully the enforcement of anti-terrorist legislation and to ensure that miscarriages of justice are avoided.

2.9 The Case of South Africa

Cybercrime is said to be growing faster in Africa than any other continent. The advent of information technology has made Africans more dependent on the Internet. At the same time, the increase in untrained and apathetic users has made information infrastructures in African countries more vulnerable to attacks by criminals who can pursue their malicious agendas undetected. The absence of suitable legal frameworks and safe and effective computer software to address cyber terrorism at national and regional levels, inadequate telecommunication infrastructure, the pre-occupation of African countries with internal factors such as the Aids crisis, poverty, rising unemployment, basic service delivery, crime and corruption have all contributed to the continent becoming a "haven" for cyber criminals including cyber terrorists. This has created an environment that is vulnerable to attacks by cyber terrorists.

The question arises how real is the threat of cyber terrorism in South Africa? There is presently no reported case of cyber terrorism in South Africa. Similarly, the nature of terrorist financing in South Africa is not well documented, although the spectre of terrorist threats looms in Africa. It has been reported that a number of Al-Qaeda or al-Qaeda-related operatives have been arrested in Southern Africa or being captured in transit. Botha maintains that a likelihood of Al-Qaeda attacks against Western interests exists in South Africa, even though the South African government disregards such a threat because of its neutrality on the so-called "war on terror" and its pro-Palestinian stance. Nevertheless, there are also reports of right-wing terrorism in South Africa with members of some right- wing organisations currently facing trial for sabotage and

terrorism. Right wingers remain on trial for trying to overthrow the government in 2002 through many attacks. Such attacks included an explosion on a railway line at Soweto outside Johannesburg that killed a woman. The case is still continuing. Despite reports of plots by terror groups ranging from Al-Qaeda to "home grown" white militants to attack the World Cup Soccer 2010 event, none materialised.

There have also been recent reports of the use of South African passports by terrorist groups. However, the South African home affairs government has conducted an investigation concluding that the passports were fake. South Africa, therefore, has introduced the following legislative measures to counteract cyber terrorism and terrorist financing:

2.8.1 The Prevention of Organised Crime Act 38 of 1999

POCA contains measures to *inter alia* combat organised crime, money laundering and criminal activities. The Act also contains provisions to freeze and confiscate property, and forfeit it to the state if such property is acquired through criminal activities. POCA requires businesses to report transactions involving funds or assets associated with criminal activities. This includes the financing of future terrorist activities. Thus, POCA targets organised crime, money laundering and terrorist financing both nationally and internationally.

2.8.2 Financial Intelligence Centre Act 38 of 2001

South Africa is a country rich in mineral resources such as gold, diamonds, uranium and platinum. This makes the country vulnerable to clandestine business transactions which can be used to facilitate terrorist financing and money laundering. The advent of AML/CFT (anti money laundering and combating the financing of terrorism) regimes have thus become key tools in addressing terrorism in the post 9/11 era. FICA outlaws money laundering and other unlawful actions. The aim of this legislation is to prevent and suppress terrorism financing. To this end, the Act has introduced an anti-money laundering regime to encourage voluntary compliance and self-regulation by institutions

(such as banks) which may be exploited for money laundering. To this end, all bank customers are required to be FICA compliant to operate their accounts. Section 21 of FICA requires banks or financial institutions to verify the identity and residential addresses or business addresses of all customers before rendering any financial service. Thus, stringent financial controls have been put in place to counteract the threat posed by terrorist financing.

2.8.3 The Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002

RICA requires all customers with cell phone numbers on cellular networks in South Africa to register their details with their respective networks as from 1 August 2009. Section 39 of RICA provides that before a telecommunication service provider must register a contract, the customer is required to furnish the service provider with his or her full name and address and a copy of his or her identity document. Section 40 of RICA contains a similar requirement but it is directed at the sellers of cellular phones and SIM cards. The aim of RICA is to help make South Africa a safer country. The objective of the Act is to help law enforcement agencies identify users of cell phone numbers and track down criminals using cell phones for illegal activities. The failure to comply with this law will result in the disconnection of cellular numbers from their cellular networks. Thus, this Act can also be used to track down cyber terrorists using cell phones to plan their malicious agendas and commit illegal activities.

RICA prescribes harsher measures than the ECT. To illustrate this, section 51 of RICA prescribes fines not exceeding R2000 000 or imprisonment not exceeding 10 years. Regarding juristic persons, fines may increase to a maximum of R5000 000. Thus, the criminal sanctions in the ECT appear to be inadequate when compared to RICA. RICA legislation has proved to be useful to police in securing convictions with intercepted cell phone evidence. It has been reported that convictions in numerous cases have depended on cell phone evidence either in terms of the communication between individuals

involved in crime or determining the location of individuals who were involved in crime.

The implementation of the Act is not without criticism. It has been reported that South Africa has no system in place to reel in cell phone customers who are in possession of RICA-registered SIM cards even if their personal information have not been entered into the network databases as required by law. Unscrupulous traders have also sold RICA-registered SIM cards without asking buyers for their personal information and documentation in contravention of the law. Thus, a national audit of the RICA system is due to be debated to discuss the scope of the problem. RICA has implemented most of the measures presently being introduced in the United Kingdom. However, the routine abuse of such measures in South Africa should be investigated to determine the extent of the problem.

2.10 Conclusion

Literature reviewed the relative background of South Africa and issues to do with terrorism. It exposed the strengths and shortfalls of the SADC in combating cyber terrorism. The chapter gave a conceptual analysis of the role of ICTs and its consequences. It examined the concept of globalisation and its effects. The next chapter focuses on the research methodology. Information and communication technologies (ICT) in particular have cast a pervasive impact in the dynamics of international relations. According to Weiss (2005), the impact of ICT "may be classified as operating through one of four main mechanisms which include changing the architecture of the international system: its structure, its key organizing concepts and the relations among its actors and also changing the processes by which the international system operates, including diplomacy, war, administration, policy formation, commerce, trade, finance, communications, and the gathering of intelligence.

CHAPTER THREE

3.0 RESEARCH DESIGN AND METHODOLOGY

3.1 INTRODUCTION

The chapter presents the research methodology of the study. This includes describing the samples, setting, instruments and the process related to how the data is managed and analysed. It describes and justifies the methods and processes to be employed to collect data that is used in answering the research questions. This section thus outlines the techniques that will be employed to obtain relevant data for each objective. The chapter will commence by considering the suitability of the selected province as an indicative case study in achieving the research objectives. It will also discuss the data collection process, with particular attention given to the population in question, the sample, the structure of the research and the data collected. Additionally, the chapter will outline the data analysis tools utilised and conclude with a validation of their suitability and reliability.

3.2 Research Design

Burns and Grove (2003:195) define a research design as "a blueprint for conducting a study with maximum control over factors that may interfere with the validity of the findings". Parahoo (1997:142) describes a research design as "a plan that describes how, when and where data are to be collected and analysed". Polit (2001:167) define a research design as "the researcher's overall findings for answering the research question or testing the research hypothesis". Babbie and Mouton (2008:74) defines a research design as a plan or blueprint for conducting a research. The study focuses on cyber crime as a threat to SADC's peace and security with maximum concentration on the case of South Africa and Zimbabwe. Therefore a case study design is utilized in this study. Yin (1984) defines the case study research method as an empirical inquiry that

investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.

3.3 Research Methodology

Research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically, Kothari 2004. There is a study of the various steps involved that are generally adopted by a researcher in studying his research problem along with the logic behind them. It is necessary for the researcher to know not only the research methods/techniques but also the methodology. Researchers not only need to know how to develop certain indices or tests, how to calculate the mean, the mode, the median or the standard deviation or chi-square, how to apply particular research techniques, but they also need to know which of these methods or techniques, are relevant and which are not, and what would they mean and indicate and why.

The research takes a qualitative approach. In order for there to be a clear research framework, the use of research designs is essential as it provides a clear guide with methods decisions and sets the interpretation. Therefore the main reason for undertaking the study using the qualitative approach is the need to understand and explain how cyber crime is feared a threat to SADC's peace and security. Priest (1996) contends that when the researcher's goal is to understand people, the social and cultural context in which they live, there is need to use qualitative research methods. This is because it is a holistic and inductive approach which will provide the opportunity to develop a descriptive, rich understanding and insight into the individual's or subject's belief's concerns, motivations and aspirations, lifestyles, cultures and preferences. Qualitative research also gives room for flexibility hence allows greater spontaneity and adaptation of the interaction between researcher and participants. For example, qualitative research employs mostly 'open ended' questions that are not necessarily worded in exactly the

same way with each participant. With these questions, participants are free to respond in their own words and their responses are more complex than a simple yes or no.

3.4 Study Population and Sample

Babbie (2007) defined a population as an aggregation of elements from which a sample is actually selected. Hair (2008), defined a population as an identifiable group of elements of interest to the researcher. Khan (1993) says that a population is a group of individuals that have one or more characteristics in common that are of interest to the researcher. For this research, the population was drawn from Harare and comprised of both sexes. A sample as described by Barnett (2000) is a portion of the population selected by some clearly defined procedures or a set of respondents selected from a larger population. Thus the sample is taken to represent the entire population in order to gain data and insights on the under study.

3.5 Purposive Sampling

Sharon (2010), defined purposive sampling as selecting a sample on the basis of one's knowledge of the population, its elements and the nature of the research aims. Thus the population is non-randomly selected based on a particular characteristic. This method is useful if the researcher wants to study a small subset of a larger population in which many members of the subset are easily identified but enumeration of all is nearly impossible. This is mainly focused on those aligned to the field of International Relations.

3.6 Data Collection Methods

The study used key informant interviews and documentary search.

3.6.1 Key Informant Interviews

Key informant interview as noted by Borg (2003), involve interviewing a selected a small group of participates who are likely to provide needed information, ideas, and insights on a particular subject. Key informant interviews were drawn from the Ministry of ICT in Zimbabwe, Zimbabwe Republic Police (ZRP) Internet Services Provider representative from Dandemutande ISP-the Manager for Dandemutande ICT and

Networks, the Chinhoyi University of Technology Deputy Dean for the School of Engineering Sciences and Technology The Senior Editor for Technomag and the Information Officer for Harare Institute of Technology.

3.6.2 Documentary Research

Secondary data will also be used to complement the research. This study involved a comprehensive desk study aimed at collecting secondary data from various sources such as online and hard copy books and periodicals, journals, research reports, policy documents, strategic plans, websites and newspapers. Since these developments are still going on a larger proportion shall necessarily entail extensive research on various electronic and print media.

3.7 Data Presentation and Analysis

Data analysis involves sifting through the data in a systematic way so that conclusions may be reached about the issue under investigation. It also entails editing, coding, classification and tabulation of collected data so that they are amenable to analysis and interpretation (Kothari, 2005). Results of the survey were presented using themes generated from respondents' findings. The analysis was based on wide research through the use of interviews, planning and assumptions. The use of qualitative data was there to avoid the issue of bias rather it gave vivid and valid results of the research. Both the primary and secondary data collected fitted the qualitative research paradigm. The basic steps in data analysis process consisted of identifying issues, determining the availability of suitable data and evaluating, summarising and communicating the results. According to Monette (1990), data analysis is unlocking information hidden in a raw data and transforming it into something meaningful.

3.8 Validity and Reliability

Validity and reliability are the most important aspects to be considered when evaluating a particular instrument. Validity can be defined as the correctness or credibility of an account, explanation or interpretation that a researcher may come up with. It is also

"concerned with the integrity of the conclusions that are generated from a piece of research" (McCaig, 2010). Reinhaz (1992: 240) maintains that "validity is the consistency of a measure with some outside criterion or standard by which to judge the test." A measurement's validity depends on how closely the operational definitions overlap with the theoretical definitions of the phenomena being measured. Parasuraman (2004) describes sensitivity as being closely related to reliability and focuses specifically on a scale's ability to detect subtle differences in the attitudes being measured. Reliability is a prerequisite for sensitivity.

Denscombe (2007) mentions that research instruments that are not reliable will render it difficult for the research to tell whether the scores obtained reflect real differences or merely random fluctuations. What this entails is that measuring instruments must be reliable first so that they become sensitive variations in responses that seem difficult to detect. When measuring instruments are unreliable, it is difficult for researchers to conclude whether scores reflect real differences or merely random fluctuations. Measuring instruments must therefore firstly be reliable in order to be sensitive to subtle variations in responses. Attention was paid in the construction of the measuring instruments used in this research so that they complied with the requirements of validity, reliability and sensitivity.

Palys (1997: 4) writes that reliability implies that "repeated observations of the same phenomena should yield similar results, and different observers following the same [research methodology] or procedures should arrive at the same conclusions." This assertion is supported by De Vos (1998:95) who further asserts that reliability is "the extent to which independent administrations of the same instrument yield the same results under comparable conditions and it is synonymous with dependability, stability, consistency, predictability and generalisability." An instrument is said to have a high reliability if it can be trusted to give an accurate and consistent measurement of an unchanging value (Bless and Higson-Smith, 1995). Reliability therefore implies that the study can be repeated with the same results. An important technique to strengthen the reliability and validity of a research design is by combining qualitative and quantitative

methodologies through triangulation, which will be characterised by the use of multiple methods of sampling, research instruments, and statistical analysis. Triangulating qualitative research findings with quantitative methods is also an accepted method of ensuring validity where the sample size is insufficient to offer validity on its own (Maxwell, 1996).

Du Plooy (2002:125) argues that "the face validity, expert validity, criterion-based validity and construct validity" maybe used as procedures or methods to support the validity of a measurement. In this study, construct validity will be used to support the validity of research instruments. It entails assessing the quality of the operational measures of the concepts being studied. It is based on the logical relationships among variables. Wimmer and Domnick (1997) view construct validity as involving a measuring instrument to some overall theoretical framework to ensure that the measurement is actually logically related to other concepts in the framework. Construct validity will be ensured by using the literature review to construct the measuring instrument (interview schedule). To ensure validity and reliability of the research instruments, a preliminary research schedule was piloted among the participants.

Yin (1994) contends that the following issues need to be planned to ensure validity and reliability when collecting data:

(a) Gaining access to the key interviewees; that is, appointments should be made in advance, usually directly with the participants;

(b) A clear schedule of data collection activities within specific periods of time should be developed.

(c) Unanticipated events such as changes in availability of participants must be provided for. Where such problems are experienced, the appointments will be rescheduled and continued at a more suitable time.

Validity essentially asks the question: how might the researcher be wrong? As validity requires the possibility of testability, it relies on others being able to achieve similar

results using the same methods on the same subjects (Dahlberg and McCaig, 2010). However, qualitative research rarely enables directly comparable conditions. Qualitative researchers therefore need to anticipate weaknesses regarding validity in their research design (Maxwell, 1996).

In this study, the reliability and validity of the research was defended by doing the following: spending some time in the field and conducting persistent observations, thereby allowing for sufficient scope and depth of observations; using triangulation which is characterised by multiple methods of sampling; research instruments to allow for the confirmation of data obtained using different instruments; and submitting findings to key informant participants for their validation.

3.9 Ethical Considerations

Research ethics involve requirements on daily work, the protection of dignity of subjects and the publication of the information in the research. However, respondents who participated in this research have been protected through identifying them by organisation.

3.10 Conclusion

This chapter has outlined how the study was conducted. It focused on the methodology used in conducting the empirical study. It explained and justified the specific research design that was used by indicating how the sample was chosen; the methods and instruments used for collecting data and describing the analysis techniques used. The type and number of respondents interviewed was also indicated. The limitations of each method of data collection were outlined and measures to address them have been identified. Triangulation of data was achieved by using a variety of methods and cross-checking. This enhanced the validity of the research findings, as each method was supplemented and checked by the others.

CHAPTER FOUR

4.0 DATA PRESENTATION, ANALYSIS, AND DISCUSSION OF FINDINGS

4.1 Introduction

This chapter presents an analysis of data collected from the sampled respondents using the qualitative research technique. Key informant interviews were conducted specifically targeting a representative from the Ministry of ICT in Zimbabwe, the Chief Superintendent of Zimbabwe Police who carries background experience in dealing with cyber crime, peacekeeping and national security matters, an Internet Services Provider representative from Dandemutande ISP-the Manager for Dandemutande ICT and Networks, the Chinhoyi University of Technology Academic Deputy Dean for the School of Engineering Sciences and Technology who carries vast experience in lecturing ICT and Electronic courses, The Senior Editor for Technomag and the Information Officer for Harare Institute of Technology. This chapter constitutes analysis and discussion of key findings from data gathered from field. Data was gathered through key informant interviews and documentary search. The statements presented in this chapter are entirely subjective opinions of the respondents who participated in the research. The views of the respondents include both positive and negative responses, to present as balanced and impartial a view as possible. In order to protect the anonymity of the respondents who took part in the research, their actual identity is not revealed. Data was presented using a thematic structure which discussed the view of the respondents under common themes which were directly linked to the objectives of the study.

1. Understanding of cyber crime.

The research posed a question on what respondents understood by the term cyber crime. According to the Chinhoyi University of Technology Deputy Dean of the School of Engineering Sciences and Technology under the ICTs and Electronics department,

> "Cyber crime is any crime committed using electronic information which may or may not be in transit, intended for misuse or harm to, misrepresentation of and/or fraud of any individual, organisation or society".

Based on his knowledge of new media technologies and experiences he has by associating with the Ministry of ICT and also other independent IT companies and ICT researchers, the Editor of Technomag stated that cyber crime is:

> "An attack on information about individuals, corporations, or governments through the use of a digital computer".

The Chief Superintendent from the ZRP indicated that:

> "In my understanding cyber crime has no single definition. The law enforcement sees it as sophisticated criminal attack on individuals, companies or the government through the use of internet and it is also a form of social media abuse, whereby Facebook, Twitter, Whatsapp are used as platform to pass on information that is destructive to the peace and security of the nation".

The Internet Services Provider representative from Dandemutande played a major inspirational role as he tried for the researcher to understand the works of internet and electronics thereby unpacking the background of cyber crime as well as trying to define it at with hands on knowledge,

> "Everyone has internet these days. All age groups have access to it and the technological advancements in electronic devices have made this access much easier and because of this networking environment people have made themselves vulnerable to digital crimes. So I believe that cyber crime is where perpetrators victimise people using the Internet and computer as the avenue".

The recent experience of cyber attack on the Harare Institute of Technology made the researcher realise the need to hear more from the Information Officer at this University. He explained cyber crime as,

> "An electronic assault on people's data threatening them to comply to perpetrators' demands".

An Officer from the former Ministry of ICT said that,

> "Cyber crime to me refers to a criminal act perpetrated by hackers or cyber criminals with the sole purpose of stealing valuable assets, for instance such things as organizational data or customer records thereby disrupting the smooth functioning and operation of Internet-based infrastructures such as servers, workstations, routers and so on" .

A broader definition is provided in Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the "Stanford Draft"), which points out that cybercrime refers to acts in respect to cyber systems. Gecke (2010) also says that some definitions try to take objectives or intentions into account and define cybercrime more precisely, such as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.

2. Cyber crime as a threat to peace and security.

In trying to understand how cyber crime is a threat to peace and security of either individual, group, companies or governments the respondents gave different lines of thoughts. The representative from the former Ministry of ICT clearly reiterated his thoughts,

> "Cyber crime is a threat to peace and security in the sense that it can be used to bring down the critical infrastructure upon which the country depends, for example, the banking system. It can also be used to disrupt communication thus bringing down communication networks. Societies are becoming more and more dependent on Internet-based services and cyber criminals have the potential to bring down these services through denial of service attacks or through viruses and worms that can cause the infrastructure to behave in a way other than it were programmed to behave. There are also patients who rely on devices such as pace makers. These devices can potentially be hacked and reprogrammed to behave in a way that the hacker intends."

Another opinion arose from the Dandemutande Manager for ICT and Networks,

> "We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. Therefore we are saying that it is inevitable that cybercrime becomes the greatest threat to every profession, every industry, every company in the world. Cyber criminals can also be a threat to democratic institutions of the country by interfering in the election systems as happened in the 2016 USA presidential elections when Russian hackers are alleged to have interfered in the US election

process. With biometric voting systems being introduced in Zimbabwe, it is conceivable that the biometric database can be hacked thereby compromising the election process. Thus cyber crime poses a serious threat to peace and security of individuals or governments".

The Chief Superintendent from the ZRP was of the view that,

> "Cyber space because of its borderless nature and cyber crime because of its nonlocal character, actions can occur in jurisdictions separated by immeasurable distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. People now take advantage of social media to abuse individuals or governments' right or even pass on wrong information through whatsapp or facebook and twitter platforms about their own countries. This is causing serious cyber damage to reputations and images of people trying to do business and even causing instabilities to operations of the country. For example what recently happened here in Zimbabwe, news was spread on social media that food stuffs will vanish from shops and this caused mayhem as people started looting such things as cooking oil, flour, sugar and in no time they had run out of their hard earned salaries and at the same time stuck with goods they do not really need and could not even sell off. This is how dangerous cyber crime is as it can quickly disturb peace in a split of a second"

The Technomag Editor was of the view that:

"Cyber crime pauses huge threats to organisations and the nation as a whole. Every organization that is connected to the Internet is at risk of having their data stolen, destroyed, disrupted, or changed and the risk is across every single sector in this country. This is mainly because it's very easy for information to go viral while it's difficult to trace the perpetrators who usually hide behind the screens. Huge amounts of

dollars have been lost from stolen intellectual property, disruption of businesses process, such as the ability to communicate or provide services to clients. The hacking case of the Harare Institute of Technology leaves a lot to desire. It shows that business in our country due to the high need to grasp new technologies is at high risk of cyber attacks. The WannaCry ransom ware attack was a worldwide cyber attack by the WannaCry ransom ware crypto worm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin crypto currency".

The Editor also indicated how businesses are threatened by cyber terrorists when he mentioned the National University of Science and Technology and the OK Zimbabwe cases.

> "OK Zimbabwe suffered a $70 000 hit in their finances through the OK's Money Wave system hack."

The Chinhoyi University of Technology Deputy Dean explains cyber crime as a difficult animal to control as its threat increases everyday in the lives of people because,

"The advances in information technologies and modern society's dependence on digital infrastructure have generated these new threats. Threats are encountered when IT is used to one; access and/or publicise state security information, two; circumvent state security missions and strategies, three; distribute otherwise state secret information that causes disharmony in civil society and mass civil unrest or to distribute propaganda and lastly and most importantly cyber crime is a major threat when it distorts or defrauds institutions of large financial resources thus placing a nation at disadvantage causing economic data distortion".

In addition, the researcher learnt from the Information Officer at HIT that,

> "Cyber crime happens on a daily basis and that no organisation could really be prepared for a major attack because the number one problem to this new threat is human kind. The risks associated with weak protection measures are affecting organisations more intensely, due to their less strict safeguards and protection. Our case here at HIT is not an exception. The recent attack by the Ransom ware virus is a clear indication that cyber crime is inevitable and threatening to everyone existing on email and is here to stay".

Much broader knowledge from other researchers indicated that cyber-crime is on the rise, as the fast growth of information and communications technologies have transformed the world into a global village, with profound impacts on all aspects of social and economic life, including security. The world is becoming a community of common destiny bound by intertwined interests in cyberspace and because of this interrelations aspect in the cyberspace, nations' peace and security in social, economic and military aspects have been made vulnerable to cybercriminals or terrorists (Ecuador, 2015).

Similarly, the representative of the United Nations on Cyber Warfare and Security said that each individual on the planet could communicate with any other through technology; the world has discovered mechanisms of global vigilance that do not distinguish between borders, or between criminals and law-abiding citizens, and does not respect sovereignty and privacy. The discussions above and some real life examples given on cyber attacks illustrate that cyber threats are real, they are not virtual but very real and therefore serious considerations on how to curb these threats have to be urgently sought by all.

3. Effectiveness of Zimbabwe's legislatures in promoting cyber security.

Further investigations in trying to reveal Zimbabwe's legislative position, the Technomag Edior indicated that:

> “I don't know of any in Zimbabwe, the bill is still yet to be passed. But fundamentally these laws are meant to protect the consumers of online content and the producers as well while they should not infringe in anyone's right as pronounced by any national charter. However the effectiveness of these can only be measured through the training that was invested into trainers and recipients. Millions to date do not apply basic online security and no laws can protect an ignorant user while those abused through cyber bullying can easily lodge a complaint it's only easier if the perpetrator is known otherwise...Talking of our neighbor South Africa Our neighbour South Africa, all they launched their cyber bill in 2016 it is ranked the world’s third highest cyber crime victims. If you follow their local news and reports you will see that they lose R2.2bn every year to internet fraud and phishing attacks”.

The Chief Superintendent from the ZRP was of the view that:

> “Well much can be said by the Ministry of ICT however what I know is Zimbabwe is still behind although in the process of legalising the cyber crime bill. Therefore we cannot mention as yet of effectiveness on legislations that we currently do not have in place. South Africa claims to be successfully driving its legislation on the use of ICTs and punishable offences on these cyber related issues. But I really think it has not fully manifested into what they expect, although on the positive end we see that a number of people have been convicted and sentenced to years in prison after they committed cyber fraud and also some employees as recorded, were dismissed from work after they had spread negative publicity about their companies on Social Media”

It was also made clear by the Dandemutande Manager for ICT and Networks that,

> "Zimbabwe does not have any legislation in place that stipulates how to enforce the law governing cybercrime or to determine appropriate correctional sentencing for those convicted of such offences. This relaxation in trying to curb or find solutions to such international threatening matters has put quite a number of individuals and organisations to serious cyber risks. Cyber bullying as recorded in Durban South Africa whereby one teenager was abused on facebook and other social media sites by an unknown person is interesting to look at apart from other many cases, cyber criminal cases, that happen every day in South Africa yet they have laws that are supposed to guard against that"

The Researcher gathered from the representative from the Ministry of ICT,

> "To my knowledge there is very little protection in Zimbabwe as far as legislation is concerned. There is not enough institutional capacity to deal with these problems for example to protect Zimbabwean businesses and the public. There are also not enough private companies developing solutions to protect citizens and organizations from cyber criminals"

The Information Officer for Harare Institute of Technology believes that,

> "Although South Africa has laws against cyber crimes it hasn't really worked for the citizens because attacks are still being reported every day. This now raises the question of whether our own legislatures will work now that we are anticipating the launch of the Zimbabwe cyber bill".

According to the Deputy Dean for Chinhoyi University of Technology, she said that,

> "Zimbabwe is yet awakening to the real threat of cybercrime even though the long known WikiLeaks (over 5 years old) should have alerted them to this threat, seeing WikiLeak actually destroyed International relations amongst countries and has led slowly to the disharmony of the European Union".

4. Measures by SADC to combat cyber crime.

Most respondents in tackling this question made it clear that SADC has not done enough to protect Southern African region from this emerging threat on cyber security. The official in the Ministry of ICT said that,

> "Although the SADC board launched the Model Law on Computer Crime and Cybercrime which was adopted by SADC ministers for telecommunications and ICT, SADC still has a long way to go in designing effective ways to restrain cyber crime. The discussion on establishment of harmonised cyber laws has been sitting for years now and no action has been taken as yet to put this in place. This has to be done quickly because this scourge of crime is not confined to individual countries because the world today is interlocked."

The SEST Deputy Dean at Chinhoyi University of Technology expressed fears at the relaxation by the SADC board on this global threat of cyber security.

> "Of course certain policies have been put in place, they have also activated the Interpol unit, which surveys all incoming and outgoing communications to detect threats. But there is a lot they still don't have access to or control of. This relaxation by SADC to explore further and upgrade ICTs may slow the process to control this animal and lead to even more major attacks".

The Technomag Editor said that:

> "Nothing to my knowledge, one would expect a specialized centre (manned by cyber security experts) that is based in one of the member countries to provide an early warning system to the region and also device strategies to deal with cyber crimes across the region. Such a centre should be run by well-trained experts and have state of the art equipment"

According to the Dandemutande Manager,

> "SADC has made some strides in response to the rising of cyber crime. You will realise that members of SADC are strengthening their legal frameworks to fight cyber crimes and protect citizens. However they need to invest in new ICT technologies and also train staff on professional handling of cyber crimes".

Scholars such as Schjolberg (2011) in his book *The History of Cyber Crime*, reveal some efforts carried out by SADC in a bid to curb cyber crime. Schjolberg states that in the year 2005, SADC member states such as Zambia, Zimbabwe, Malawi, South Africa and Mozambique initiated efforts to harmonise cyber crime laws. He also said that a connect Africa initiative was launched in October 2007. It was a global multi-stakeholders partnership aimed at assisting Africa to develop ICT infrastructures. The author also reveals importantly that a Cybercrime and Computer related Crimes (Act 22,2007) was adopted in Botswana as the date of commencement being December 2007. The Act was established to combat cyber crime and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence".

5. Effectiveness of SADC in combating cyber crime

> "It is not effective at all. SADC member countries seem to treat cyber crime as a peripheral issue" expressed the Technomag Editor.

The CUT SEST Deputy Dean said that,

> "it is not that effective because the technologies they use are way behind those who hack into systems. Their legislation is still very weak. Their limited understanding of the technical issues in cybercrime makes it difficult to produce well-crafted legislation. The ways to aid in combating cybercrime start from the basic user level, who is still not convinced that such issues can happen to them. A country-wide survey needs to be carried out to ascertain the user's basic understanding of cybercrime and the ways in which they are helping themselves"

The researcher realised the importance of SADC's role in curbing cyber crime through responses from the Chief Superintendent of Police. He says,

> "SADC member states are working in collaboration as law enforcement and public security agencies in the SADC region to increase effectiveness. They are working together as a board to combat cyber fraud and other related digital crimes. Although they are limited by inexperienced staff since this threat is regarded as new in Africa. SADC countries are working effectively together to protect the people and safeguard the development of the Region against instability arising from the breakdown of law and order, inter-state conflict and aggression that also bring in the cyber crime aspect. This is shown by all the efforts being made by SADC countries to come up with workable policies and legislations against cyber crime although this still is challenging to their role"

6. Challenges being faced by Zimbabwe in combating cyber crime.

> "SADC's lack of resources is the main reason for failing to set up innovative infrastructure for monitoring and controlling cybercrime, to educate all users of smart phones, mobile money, electronic debit cards, computers and the Internet on the measures they can take to minimise the risk of cyber crime or even to invest in developing proper legislature against cyber crime" said the Deputy Dean for CUT SEST.

The Technomag Editor says that,

> "There is lack of support from governments and there is no coordinated approach to addressing the problem within SADC. There is no specialized centre that is operated by experts that man the cyber space to ensure that companies, organizations and citizens are not impacted by cyber crimes"

Dandemutande ICT and Electronics manager was more determined to say that,

> "Poor infrastructural development in our African countries is our major setback. Our governments are not investing enough in ICT therefore you realise that this remains our biggest challenge in trying to fight this virtual threat. The other challenge is lack of harmony amongst regions which causes cyber criminals to easily penetrate one country's computer network and quickly spread harm to other countries. For instance the well known recent malware virus attack which affected the whole world in no time. Weak legislation on cyber crime and security is also our downfall in trying to keep with the pace of cyber crime and to tone it down because basically it may not really be stopped but as Zimbabwe and South Africa by strengthening our legislations and investing more into technology and ICT we can reduce the risk of being attacked".

The representative from the Ministry of ICT expressed a slightly differently angle when he said,

> "It is because of economic sanctions and the issues of power struggle that the smaller nations suffer from poor development in ICTs. You see that the bigger nations pull everything their side and a little is done to develop Africa. This is one of the challenges we face as SADC as we try and access financial help internationally to improve our infrastructure or sponsor the rightful expertise in IT. This then leaves us at such risks as cyber crimes and lack of proper security against these criminal acts".

The Chief Superintendent from the ZRP indicated that:

> "Our main challenge solely lies on the fact that we lack on trained staff who really know how to go about combating this type of crime. This is because as I highlighted before cyber crime is new to us, although not very new but it is starting to be seriously considered in Zimbabwe and even South Africa. Therefore as police, security, government, agencies and so on we really need to invest on training our staff to become the rightful experts to fight against cyber criminals".

4.4 Summary

This chapter outlined the key findings of the research. The study deduced that Zimbabwe is vulnerable to cyber-attacks though no significant attacks have been witnessed. The motivation of cyber crime such as increased technological advancements, weaknesses and outdated information systems as well as political drives are catalysts for cyber-attacks. The chapter also examined the country's vulnerability to cyber crime on key national infrastructure.

CHAPTER FIVE

5.0 SUMMARY, CONCLUSIONS, RECOMMENDATIONS AND AREAS FOR FURTHER RESEARCH

5.1 Introduction

This Chapter presents research conclusions, recommendations and suggest methods to alleviate problems identified in the research. It generally presents a summary of the research. The research findings are highlighted and the research questions posed in Chapter 1 are addressed. The chapter further indicates how the objectives of the study were met. The conclusions were drawn from the previously discussed chapters. During the course of the research, the study identified a major problem brought about by the emergencies of ICTs in international relations focusing on the Southern region of Africa particularly on Zimbabwe and South Africa. To be more specific the study dwelt on cyber crime challenges and therefore offered a number of recommendations to reduce the risk of cyber attacks on individuals, organisations or governments. The recommendations are based on contemporary literature and empirical findings in the current study. Finally areas for further research are suggested.

5.2 Summary

Chapter one introduced and defined the study. This chapter provided the background of the study; problem statement; purpose and objectives of the study; the research questions to be answered; the methodology employed; importance and contribution of the study and the scope and limit of the study. A summary on the emergencies of ICTs in Africa and therefore the introduction of cyber crime was also specified.

Chapter two covered the literature review and theoretical framework guiding the study. It discussed widely the modernisation and commodisation theories. It traced the History and the role of ICTs in International relations, rather more specifically the background

of Internet and the beginning of cyber crime thereof. The chapter revealed cyber crime as a new threat in Southern Africa while focusing on Zimbabwe and South Africa and it tried to explore whether at all the Southern African Development Committee is doing anything to curb cyber crime in the SADC countries. The study focused on cyber crime as a threat to SADC's peace and security with maximum concentration on the case of South Africa and Zimbabwe. The Chapter also identified a number of International experiences on cyber crime, cyber terrorism and cyber security issues and it also tackled on legislations that were made in an effort to combat cyber crime.

The research took a qualitative research approach in order to address the research questions and objectives of the study in Chapter three. Purposive sampling technique was employed and the key informants subjectively selected. Challenges experienced were also described. The means of data collection was described and it was concluded that the selected method was an objective and appropriate method of research because it allows in-depth understanding and explains how cyber crime is feared a threat to SADC's peace and security. The study used qualitative research methodology and was a case study of Zimbabwe and South Africa threatened by cyber or virtual attacks and what they are putting in place to safeguard their people. Key informant interviews and the use of authentic secondary or documentary sources to collect data informed this study. These two techniques had the merit of digging beyond into the respondents' experiences and point of analysis with regards to cyber crime as a threat to SADC's peace and security. The chapter also discussed measuring instruments and techniques drawn to analyse data. These are validity and reliability.

Chapter four discussed and analysed the key findings of the research. It unpacked the complications behind the cyber crime and the causes of cyber crimes and major implications this have on Zimbabwe and South Africa's peace and security. It also pondered on the initiatives made by SADC and SADC member states to counter cyber crime and provide security to SADC countries. The effectiveness of the SADC role in trying to combat cyber crime was also discussed.

Chapter five provides the summary, key recommendations and conclusions of the study. Implications of the study and areas for further research are also provided. This final chapter sums up the study and makes knowledgeable recommendations. The study initiated the respondents to provide possible recommendations and measures that could be implemented to combat this new threat under discussion, that is cyber crime.

5.3 Conclusions

The main purpose of this research was to understand the challenges brought about by ICTs in international relations. The study sought to understand the threats of cyber crime to Zimbabwe and South Africa and to assess the effectiveness of South Africa and Zimbabwe legislatures in promoting cyber security. The chapter also sought to provide recommendations that improve SADC roles in combating cyber crime. The findings of the research addressed research questions which were posed in Chapter 1. The first question sought to unpack the term cyber crime and its complications in the study of international relations. The research findings described cyber crime as any crime committed using electronic information which may or may not be in transit, intended for misuse or harm to, misrepresentation of and/or fraud of any individual, organisation or society. It also refers it to a criminal act perpetrated by hackers or cyber criminals with the sole purpose of stealing valuable assets, for instance such things as organizational data or customer records thereby disrupting the smooth functioning and operation of Internet-based infrastructures such as servers, workstations, routers and so on.

The research gathered that, cyber crime has no single definition. According to the Computer crime and Cybercrime framework Bill of Zimbabwe, it explains that definitions if not consistent with international use will create difficulties when faced with cross border cyber offences as what might be defined as an offence in one country could potentially be trivial or not any offence in the other country. This means that the fast evolution of technologies might entail that the definitions can easily become

obsolete, for instance a device today might not be a device tomorrow. The Absence of precision in the definitions might also create an omnibus approach with almost everything becoming criminalized. Therefore society and individuals will find it difficult to regulate their behaviour. The issue of trying to define cyber crime was revealed as a complicated matter in this chapter. Aghatise (2014) underlies the same complication when he say that cyber crime are crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. He continues to say that even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the computer and the person behind it as victims, it just depends on which of the two is the main target.

Research question number two was concerned with understanding how cyber crime is a threat to peace and security of individuals, groups, companies or governments. The findings reveal that cyber crime is a threat to peace and security in the sense that it can be used to bring down the critical infrastructure upon which the country depends, for example, the banking system. It can also be used to disrupt communication thus bringing down communication networks. Societies are becoming more and more dependent on Internet-based services and cyber criminals have the potential to bring down these services through denial of service attacks or through viruses and worms that can cause the infrastructure to behave in a way other than it were programmed to behave. Devices can be hacked and reprogrammed to behave in a way that the hacker intends thereby posing serious threat to democratic institutions of the country by interfering with important digitalised systems. Every organization that is connected to the Internet is at risk of having their data stolen, destroyed, disrupted, or changed and the risk is across every single sector in this country. This is mainly because it’s very easy for information to go viral while it’s difficult to trace the perpetrators who usually hide behind the screens.

According to Ecuador (2015), cyber-crime and cyber-terrorism are on the rise, as the fast growth of information and communications technologies have transformed the world into a global village, with profound impacts on all aspects of social and economic life, including security. The world is becoming a community of common destiny bound by intertwined interests in cyberspace and because of this interrelations aspect in the cyberspace nations' peace and security in social, economic and military aspects have been made vulnerable to cybercriminals or terrorists

The findings conceived that each individual on the planet could communicate with any other through technology; the world has discovered mechanisms of global vigilance that do not distinguish between borders, or between criminals and law-abiding citizens, and does not respect sovereignty and privacy. It is because of this that the research gathered that the target is the end user and that virtual terrorism is real and here to stay. It is because of this that the research proposes a totally different approach from the traditional approaches to fight against cyber criminals. Much stronger border cooperation and orientation is needed. New partners need to be found as incorporated into existing frameworks.

The third question ventured into figuring out on how effective the Zimbabwe and South Africa's legislatures are in promoting cyber security. The study reveals that Zimbabwe's bill is still yet to be passed. The fundamental aspect however is that these laws are meant to protect the consumers of online content and the producers as well while they should not infringe in anyone's right as pronounced by any national charter. However the effectiveness of these can only be measured through the training that was invested into trainers and recipients. Millions to date do not apply basic online security and no laws can protect an ignorant user while those abused through cyber bullying can easily lodge a complaint it's only easier if the perpetrator is known. South Africa launched its cyber bill in 2007 but it is ranked the world's third highest cyber crime victims. They lose R2.2bn every year to internet fraud and phishing attacks.

The research also posits that there is very little protection in Zimbabwe as far as legislation is concerned. There is not enough institutional capacity to deal with these problems for example to protect Zimbabwean businesses and the public. There are also not enough private companies developing solutions to protect citizens and organizations from cyber criminals. Although the WikiLeaks should have awakened Zimbabwe to this threat of cyber crime considering that it is five years old, Zimbabwe still lags behind and South Africa remains under attack because of its weak cyber crime legislation.

Loxton (2014), informs his research when he indicates that South Africa does not take cyber crime seriously enough even though it is recorded to be currently carrying the highest number of cyber attacks in Africa. Its legislation is not strong enough to put in force the adherence to cyber crime and cyber security issues. The Deloitte current report on cyber crime further unpacks that major threats and risks to data, information, assets, and transactions are continually evolving, and typical approaches to cyber security are not nearly keeping pace. It also says that current security models are minimally effective against cyber criminals and organizations remain unaware of that fact.

The fourth research question was concerned with what SADC has done to combat cyber crime. The study gathers that although SADC has put policies in place and have activated the Interpol unit, which surveys all incoming and outgoing communications to detect threats, there is a lot they still don't have access to or control of and they still haven't designed effective ways to curb cyber crime. The discussion on establishment of harmonised cyber laws has been sitting for years now and no action has been taken as yet to put this in place since the research gathered that this scourge of crime is not confined to individual countries because the world today is interlaced and border cooperation and partnerships are encouraged. Moreover one would expect a specialized centre (manned by cyber security experts) that is based in one of the member countries to provide an early warning system to the region and also device strategies to deal with cyber crimes across the region. Such a centre should be run by well-trained experts and have state of the art equipment.

According to the ITU recent report, initiatives have been made such as the connect Africa initiative which was launched in October 2007. It was a global multi-stakeholders partnership aimed at assisting Africa to develop ICT infrastructures and most importantly that a Cybercrime and Computer related Crimes Act (2007) was adopted in Botswana. The Act was established to combat cyber crime and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence. Amidst all of this the research reveals that SADC still lacks adequate cybercrime legislation and this continuously deprives law enforcement agencies of effective tools to support citizens that have become victims of cybercrime. This also might protect or encourage offenders from abroad to move their illegal activities to countries with such legislation.

The research question number five tackled on the effectiveness of the SADC role in combating cyber crime. Evidence gathered showed that SADC's role is not very effective in curbing cyber crimes and providing security. One of the major reasons highlighted revealed that SADC does not have the required capacity in terms of ICT related infrastructures. Most of the technologies they use are way behind those who hack into systems. Their limited understanding of the technical issues in cybercrime make it difficult to produce well-crafted legislation and therefore the legislation is weak which compromises their role to protect the SADC region.

Sikuka (2012) reflects that SADC is making strides in harmonising its cyber relate laws. As the world is fast becoming one big digital globe, cyber security threatens to undermine this envisaged man-made wonder that promises to simplify life in a way too complex to imagine. He said the only way SADC can address the challenge was to harmonise its cyber-related laws since cyber crime does not recognise geographical borders.

5.4 Recommendations

The strategy and execution of cyber security needs to be developed with clear vision for addressing challenges related with cybercrime. The following recommendations were extended by the respondents:

(i) Prevention and Awareness- The fight against cybercrime must start with preventing it in the first place. Users such as individuals should be proactive, not reactive. This fight against cybercrime starts even in own home. Individuals should not reply any e-mail from unknown persons, they should learn to report spam mails to the e-mail server or other known cybercrime research sites. If there is one thing that makes committing cybercrime lucrative, it is the fact that victims rarely have the required knowledge or presence of mind to handle the situation. The law enforcement should run public awareness on cyber crime risks and prevention together with IT industries and Institutions of learning.

(ii) Training and Education- Mass education and training on reducing cyber risk and on conscientising people on new legislature is encouraged. Cybercrime is neither "armed robbery", nor "pen and paper crime" and should not be handled as such. Fighting Cybercrime requires intelligent IT knowledge and that begins with equipping individuals with basic education or skills in IT. People should also be taught to use original computer software rather than pirated software since pirated software is usually unprotected and this brings harm through computer machines or digital devices.

(iii)Introduction of New Laws and Updating of Existing Laws- One of the biggest challenges the African government and other nations face is the enactment of adequate cyberspace laws. For a start, there has to be recognition that cyber crime poses a serious threat to security and peace in SADC this then leads to the appreciation of creating suitable legal

frameworks and safe and effective computer software in order for Zimbabwe and South Africa to address cyber terrorism at national and regional levels. Cybercrime is evolving every single day therefore the need for new laws to tackle this particular crime, although these laws can be circumvented in a matter of weeks, thus comes up the issue of constant law updates.

(iv) Surveillance Infrastructural Development- These must continuously be upgraded, that is skills training of hacking teams, equipment upgrade, development of new innovations and own techniques, linking with other Interpol networks for collaborated efforts. These must be done regularly and never stop, including information on the new ways being used by criminals at any given time. They must be continuously revised so that it is in tandem with new criminal strategies, including those being used in other countries (they will eventually filter), and also in line with the shift to worldwide adoption of digital currencies (e.g. BITCOIN) and new financial systems. Since cyber crime is a new threat in Zimbabwe and South Africa general police force should not be allowed to investigate crimes committed over the internet. IT experts should be recruited into law enforcement agencies to assist in the fight. There is also a need for SADC to establish a centre that will be manned by cyber security experts who will be equipped with knowledge and skills to understand cyber threats around the world. The centre will monitor, detect and prevent cyber crimes in SADC as well as documenting the attacks and developing strategies for combating the threats.

(v) Develop New Technology and Online Assistance- SADC countries should develop technology of encryption and anonymity and also for protecting infrastructure as hackers or cyber terrorists can attack over any nation's infrastructure resulting in massive losses. There is also need for organisations or institutions to develop regular online assistance to

employees, learn Internet to one's advantage only and understand all tips to stay safe online.

(iv)International and Regional Collaboration and Cooperation- Victims of cybercrime, be it individuals or organizations, need to cooperate with law enforcement agencies for effective response. It is only through cooperation with each other that all stakeholders will be best-placed to understand the complexities involved in cyber crime and security, work together to build systematic and workable situations. SADC should harmonise its cyber-related laws since cyber crime does not recognise geographical borders. Such regional and international partnerships can help the countries to use combined force in the fight against cyber criminals.

5.5 Areas for Further Research

Cyber crime is a broad topic of study and many areas have been left out which can be broadly explored further, such areas as cyber terrorism, cyber war or cyber security can be tackled in order to gain a deeper understanding of the field cyber crime.

REFERENCES

Ayofe, A. N., & Irwin, B. (2010). *Cyber Security: Challenges and the Way Forward:* Computer Science and Telecommunications.

Calder, A. & Watkins, S. (2012), IT Governance: An international guide to data security and ISO27001/ISO27002 (5th Ed.), Croydon, CPY Group Ltd

Cassim F, (2009), "Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study" *PER*

Cassim F, (2011), "Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players" *CILSA* XLIV

Cassim F (2011) "Combating Cyber Terrorism in South Africa: Are Adequate Measures in Place?"*Proceedings of the Third Annual Conference of Asian Criminological Society (ACS)* Taiwan 96-105

Cassim F; (2012): Addressing the Spectre of Cyber Terrorism: A Comparative Perspective; UNISA; South Africa.

Conway M, (2007), "Terrorism and New Media: the Cyber Battle Space" in *Countering Terrorism and Insurgency in the twenty first century, Praeger Security International, Greenwood Publishing*

Hoscheidt M. M; and Eichner E. F; (2012); Legal and Political Measures to Address Cyber Crime; UFRGSMUN, UFRGS Model; UN

ITU (2014, September 20) Cybersecurity. ITU News. Retrieved from https://www.itu.int *ITU-ABIresearch (2015). Global Cyber security Index & Cyber wellness Profiles Report: Telecommunication Development Bureau; Brahima Sanou.*

KaMtuze S. L. S; (2015); Cyber Crime and Cyber Security Legislation in Africa; Fort Hare University; South Africa.

Kim, W., & Jeong O., & So, J. (2011).The dark side of the Internet: Attacks, costs and responses. *Information Systems 36, 675-705.*

Kizza J.M. (2013). Computer Communications and Networks: *Guide to Computer Network Security*, 465 -489, Spring

Manacorda, S, (2012), *Cyber-criminality: finding a balance between freedom and security* International Scientific and Professional Advisory Council

Schjolberg S, (2008), The History of Global Harmonization on Cyber Crime Legislation; The Road to Geneva, Oslo, Norway

Sikuka K (2012), SADC Responds to Cyber Crime; Southern Africa Response Documentation Centre; SADC

Basdeo V "Terrorist financing in Southern Africa: African commitment to combating terrorism" *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)* 15-17 January 2011 Jaipur 49-52

Brunst PW "Terrorism and the Internet: New Threats Posed by Cyber terrorism and Terrorist Use of the Internet" in *A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications* Wade M and Maljevic A (ed) (2010 *Springer*) 51-78

Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study" 2009 *PER* 36-79

Cassim F "Combating Cyber Terrorism in South Africa: Are Adequate Measures in Place?" *Proceedings of the Third Annual Conference of Asian Criminological Society (ACS)* 17-19 December 2011 Taiwan 96-105

Conway M "Terrorism and New Media: the Cyber Battle Space" in *Countering Terrorism and Insurgency in the twenty first century* James F Forest (ed) (2007 *Praeger Security International – Greenwood Publishing*) 1-31

Guru A & Mahishwar U "Terror Networking via Social Networking: Are the Laws adequate" *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)* 15-17 January 2011 Jaipur 71-73

Young R "Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislations 2006 *Boston College International and Comparative Law Review* 29(1) 23-103

ANNEXURES

APPENDIX A

Interview Guide for the Chief Superintendent of the Zimbabwe Police.

Bindura University of Science Education.

Title of Research: Cyber Crime as a threat to SADC's peace and security. A case of Zimbabwe and South Africa

The researcher is a Master student in International Relations. The information you are asked to provide is required for research purposes only and will not be used to jeopardise your position or compromise the integrity or status of your organization. Your responses will be kept in confidence and used solely for the purpose of this study. Anonymity is strictly guaranteed. Your cooperation will be greatly appreciated.

1. What do you understand by the term cyber crime?
2. How is cyber crime a threat to peace and security?
3. How effective are the Zimbabwe and South Africa legislatures in promoting cyber security?
4. What has SADC done to combat cyber crime?
5. How effective is the SADC role in combating cyber crime?
6. What challenges are being faced by Zimbabwe and South Africa in combating cyber crime?
7. What measures can be put in place to combat cyber crime?

APPENDIX B

Interview Guide for the Dandemutande ICT and Electronics Manager

Bindura University of Science Education.

Title of Research: Cyber Crime as a threat to SADC's peace and security. A case of Zimbabwe and South Africa

The researcher is a Master student in International Relations. The information you are asked to provide is required for research purposes only and will not be used to jeopardise your position or compromise the integrity or status of your organization. Your responses will be kept in confidence and used solely for the purpose of this study. Anonymity is strictly guaranteed. Your cooperation will be greatly appreciated.

1. What do you understand by the term cyber crime?
2. How is cyber crime a threat to peace and security?
3. How effective are the Zimbabwe and South Africa legislatures in promoting cyber security?
4. What has SADC done to combat cyber crime?
5. How effective is the SADC role in combating cyber crime?
6. What challenges are being faced by Zimbabwe and South Africa in combating cyber crime?
7. What measures can be put in place to combat cyber crime?

APPENDIX C

Interview Guide for the Deputy Dean of CUT School of Engineering and Sciences.

Bindura University of Science Education.

Title of Research: Cyber Crime as a threat to SADC's peace and security. A case of Zimbabwe and South Africa

The researcher is a Master student in International Relations. The information you are asked to provide is required for research purposes only and will not be used to jeopardise your position or compromise the integrity or status of your organization. Your responses will be kept in confidence and used solely for the purpose of this study. Anonymity is strictly guaranteed. Your cooperation will be greatly appreciated.

1. What do you understand by the term cyber crime?
2. How is cyber crime a threat to peace and security?
3. How effective are the Zimbabwe and South Africa legislatures in promoting cyber security?
4. What has SADC done to combat cyber crime?
5. How effective is the SADC role in combating cyber crime?
6. What challenges are being faced by Zimbabwe and South Africa in combating cyber crime?
7. What measures can be put in place to combat cyber crime?

APPENDIX D

Interview Guide for the Information Officer of the Harare Institute of Technology .

Bindura University of Science Education.

Title of Research: Cyber Crime as a threat to SADC's peace and security. A case of Zimbabwe and South Africa

The researcher is a Master student in International Relations. The information you are asked to provide is required for research purposes only and will not be used to jeopardise your position or compromise the integrity or status of your organization. Your responses will be kept in confidence and used solely for the purpose of this study. Anonymity is strictly guaranteed. Your cooperation will be greatly appreciated.

1. What do you understand by the term cyber crime?
2. How is cyber crime a threat to peace and security?
3. How effective are the Zimbabwe and South Africa legislatures in promoting cyber security?
4. What has SADC done to combat cyber crime?
5. How effective is the SADC role in combating cyber crime?
6. What challenges are being faced by Zimbabwe and South Africa in combating cyber crime?
7. What measures can be put in place to combat cyber crime?

APPENDIX E

Interview Guide for the Technomag Senior Editor.

Bindura University of Science Education.

Title of Research: Cyber Crime as a threat to SADC's peace and security. A case of Zimbabwe and South Africa

The researcher is a Master student in International Relations. The information you are asked to provide is required for research purposes only and will not be used to jeopardise your position or compromise the integrity or status of your organization. Your responses will be kept in confidence and used solely for the purpose of this study. Anonymity is strictly guaranteed. Your cooperation will be greatly appreciated.

1. What do you understand by the term cyber crime?
2. How is cyber crime a threat to peace and security?
3. How effective are the Zimbabwe and South Africa legislatures in promoting cyber security?
4. What has SADC done to combat cyber crime?
5. How effective is the SADC role in combating cyber crime?
6. What challenges are being faced by Zimbabwe and South Africa in combating cyber crime?
7. What measures can be put in place to combat cyber crime?

APPENDIX E

Interview Guide for the representative of the Ministry of Information Communication Technology, Postal and Courier Services in Zimbabwe.

Bindura University of Science Education.

Title of Research: Cyber Crime as a threat to SADC's peace and security. A case of Zimbabwe and South Africa

The researcher is a Master student in International Relations. The information you are asked to provide is required for research purposes only and will not be used to jeopardise your position or compromise the integrity or status of your organization. Your responses will be kept in confidence and used solely for the purpose of this study. Anonymity is strictly guaranteed. Your cooperation will be greatly appreciated.

1. What do you understand by the term cyber crime?
2. How is cyber crime a threat to peace and security?
3. How effective are the Zimbabwe and South Africa legislatures in promoting cyber security?
4. What has SADC done to combat cyber crime?
5. How effective is the SADC role in combating cyber crime?
6. What challenges are being faced by Zimbabwe and South Africa in combating cyber crime?
7. What measures can be put in place to combat cyber crime?