

**BINDURA UNIVERSITY OF SCIENCE EDUCATION**  
**FACULTY OF SOCIAL SCIENCES AND HUMANITIES**  
**DEPARTMENT OF PEACE AND GOVERNANCE**



**AN ASSESSMENT OF ZIMBABWE'S CYBERSECURITY**  
**FRAMEWORK: IMPLICATIONS FOR DIGITAL RIGHTS AND**  
**FREEDOMS.**

BY: TINOTENDA SABAMBA (B211375B)

**SUPERVISOR: MR MHURI**

**A DISSERTATION SUBMITTED TO THE DEPARTMENT OF PEACE AND**  
**GOVERNANCE IN PARTIAL FULFILMENT FOR THE REQUIREMENTS FOR**  
**THE BACHELOR OF SCIENCE HONOURS DEGREE IN PEACE AND**  
**GOVERNANCE**

Bindura, Zimbabwe

March, 2025

## **ABSTRACT**

The study looked at the effectiveness of Zimbabwe's cybersecurity framework in protecting people's digital rights and freedoms. Particularly the research aimed to explore the nature of Zimbabwe's cybersecurity framework, to examine the effectiveness of Zimbabwe's cybersecurity framework in protecting citizen's personal data and preventing cyber threats, to identify gaps in Zimbabwe's cybersecurity framework that compromise digital rights and freedoms and to propose strategies that improve Zimbabwe's cybersecurity framework capacity to protect people's digital rights and freedoms. The study used qualitative approach. Ministry of Information Communication Technology, Postal and Courier Services, Postal Telecommunication companies and social media users were targeted in Harare. Purposive sampling was used to select social media users. The total respondents were 20. Furthermore, semi structured interviews and document analysis was used to collect data. Findings revealed that while data protection exist, their practical enforcement and public awareness of them are limited hence, the lack of public awareness regarding online safety practices further compounds the issue, leaving citizens vulnerable to cyberattacks. The research concluded that the framework exists as a work in progress whereby various gaps point the need for a more human rights centered approach to cybersecurity policy development and implementation, ensuring that digital innovation does not come at the expense of fundamental rights and freedoms. The study recommended awareness campaigns, prioritizing resource allocation and capacity building as well as enhancing data protection legislation and enforcement.

## DECLARATION FORM

I, Tinotenda Sabamba, do hereby declare that this dissertation represents my own work, except where otherwise acknowledged and that it has never been previously submitted at Bindura University of Science Education or any other university.

Student's signature: ..........

Date: .....17/08/2025.....

Supervisor's Name.....Mr K Mhuri.....

Supervisor's signature..........

Date.....17/08/2025.....

Chairperson's Name.....DR J KUREBWATIRA.....

Chairperson's signature..........

Date.....18/08/2025.....

**DEDICATION**

This dissertation is dedicated to my parents and my siblings who rendered support, love and encouragements during my course of study.

## **ACKNOWLEDGEMENTS**

I am sincerely grateful to my supervisor for providing both academic, guidance and supervisory role throughout my study. I say thank you for building me up.

I also wish to thank the following lecturers: Dr. J. Kurebwatira, Dr. Nyoni, Dr. Muchemwa and Dr. Mbanje. I also thank my classmates, namely: Nheweyembwa T., Nyikadzino M and Mudimu A.

Further, I would like to thank all the individuals and institutions who provided data and other forms of help and support, such as Ministry of Information Communication Technology (ICT), Postal and Courier Services as well as those from telecommunication companies.

The acknowledgements can never be complete without expressing my genuine gratitude to my parents and siblings for their encouragement, support and love during the entire course of my study.

## **LIST OF ABBREVIATIONS AND ACRONYMS**

AIPPA	ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT
AU	AFRICAN UNION
CDPA	CYBER AND DATA PROTECTION ACT
CERTS	COMPUTER EMERGENCY RESPONSE TEAMS
CMM	CYBERSECURITY MATURITY MODEL
CSCCU	CYBER SECURITY AND CYBER CRIME UNIT
G20	GROUP OF 20
GDPR	GENERAL DATA PROTECTION REGULATION
ICA	INTERCEPTION OF COMMUNICATIONS ACT
ICCPR	INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS
ICT	INFORMATION COMMUNICATION TECHNOLOGY
ID	IDENTIFICATION
IOS	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ITU	INTERNATIONAL TELECOMMUNICATION UNION
NGOS	NON-GOVERNMENTAL ORGANIZATIONS
POTRAZ	POSTAL TELECOMMUNICATIONS REGULATORY AUTHORITY OF ZIMBABWE
RISA	RWANDA INFORMATION SOCIETY AUTHORITY
SADC	SOUTHERN AFRICAN DEVELOPMENT COMMUNITY
SI	STATUTORY INSTRUMENT
UN	UNITED NATIONS
ZCSA	ZIMBABWE CYBER SECURITY AGENCY
ZICT	ZIMBABWE INFORMATION AND COMMUNICATION TECHNOLOGY
ZNSA	ZIMBABWE NATIONAL SECURITY AGENCY

**LIST OF TABLES AND FIGURES**

Table 4.1: Response Rate.....	50
Fig 4.2.1: Gender Respondents.....	52
Fig 4.2.2: Age Group.....	53
Fig 4.2.3:Level of education.....	53

## TABLE OF CONTENTS

ABSTRACT.....	2
DECLARATION FORM.....	3
DEDICATION.....	4
ACKNOWLEDGEMENTS.....	5
LIST OF ABBREVIATIONS AND ACRONYMS.....	6
<b>CHAPTER ONE.....</b>	<b>12</b>
<b>1.0 INTRODUCTION.....</b>	<b>12</b>
1. Background to the Study.....	12
1.2 Purpose of the Study.....	14
1.3 Statement of the Problem.....	14
1.4 Research Objectives.....	15
1.5 Research Questions.....	15
1.6 Assumptions.....	16
1.7 Significance of the Study.....	16
1.8 Delimitations of the Study.....	17
1.9 Limitations of the Study.....	18
1.10 Definition of Key Terms.....	18
1.11 Dissertation Outline.....	19
<b>CHAPTER TWO.....</b>	<b>20</b>
<b>LITERATURE REVIEW AND THEORETICAL FRAMEWORK.....</b>	<b>20</b>
2.0 Introduction.....	20
2.1 Theoretical framework.....	20
2.1.1 Digital Authoritarianism theory.....	20
2.1.2. Cybersecurity Maturity Model (CMM) Framework.....	21
2.2 Cybersecurity framework consist of the following.....	23
2.3 Implications for digital rights and freedoms.....	26



2.4 Case Studies on Cybersecurity and Digital Rights.....	27
2.5 The nature of Zimbabwe's cyber security framework.....	28
2.6 The effectiveness of Zimbabwe's cybersecurity framework in protecting citizens' personal data and preventing cyber threats.....	29
2.7 Gaps in Zimbabwe's cybersecurity framework that compromise digital rights and freedoms.....	31
2.8 Strategies on literature to address the gaps.....	33
2.9 Research gap.....	35
2.10 Chapter summary.....	35
<b>CHAPTER THREE.....</b>	<b>37</b>
<b>RESEARCH METHODOLOGY AND DESIGN.....</b>	<b>37</b>
3.0 Introduction.....	37
3.1 Research philosophy/ paradigm.....	37
3.2 Research methodology.....	38
3.3 Research design.....	38
3.4 Population and sample.....	39
3.5 Sampling method.....	39
3.6 Data collection methods.....	40
3.7 Validity and reliability.....	41
3.8 Data presentation and analysis.....	42
3.9 Pilot testing.....	42
3.10 Ethical considerations.....	43
3.11 Summary.....	44
<b>CHAPTER FOUR.....</b>	<b>45</b>
<b>DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS.....</b>	<b>45</b>
4.0 Introduction.....	45
4.1 Response rate.....	45
4.2 Demographic data of respondents.....	46

4.2.1. Gender of respondents.....	46
4.2.2 Age group.....	47
4.2.3 Level of education.....	47
4.3 The nature of Zimbabwe's cyber security framework.....	48
4.4 The effectiveness of Zimbabwe's cyber security framework in protecting citizens' personal data and preventing cyber threats.....	50
4.5 Gaps in Zimbabwe's cyber security framework that compromise digital rights and freedoms.....	53
4.6 Strategies that improve Zimbabwe cyber security framework capacity to protect people's digital rights and freedoms.....	55
4.7 Chapter Summary.....	57
<b>CHAPTER FIVE: SUMMARY, CONCLUSIONS, RECOMMENDATIONS AND AREAS FOR FURTHER RESEARCH.....</b>	<b>58</b>
5.0 Introduction.....	58
5.1 Summary of Findings.....	58
5.2 Conclusions.....	58
5.2.1 The nature of Zimbabwe's cyber security framework.....	58
5.2.2 The effectiveness of Zimbabwe's cyber security framework in protecting citizens' personal data and preventing cyber threats.....	59
5.2.3 Gaps in Zimbabwe's cyber security framework that compromise digital rights and freedoms.....	59
5.2.4 Strategies that improve Zimbabwe cyber security framework capacity to protect people's digital rights and freedoms.....	60
5.3 Recommendations.....	60
<b>REFERENCES.....</b>	<b>62</b>
ANNEXURE 1: Interview guide.....	71
ANNEXURE 2: Permission letter.....	73



## CHAPTER ONE

### 1.0 INTRODUCTION

#### 1. Background to the Study

As economies not to mention societies become more digital, the risks of cybersecurity are increasing because critical services such as energy, banking, education and healthcare depend on internet connected systems, hence, threats are growing more quickly than many developing countries can manage. According to Freedom House, digital rights fell for the sixth year in a row in 2016 (Turianskyi, 2018). In order to limit digital rights and enable monitoring, both authoritarian and democratic governments enacted new cyber and security legislation. Cyber monitoring represents growing, as well as progressively citizens being coerced either arrested due to their cyber behavior. The worst case examples are in authoritarian governments such as China, Saudi Arabia, Iran, Egypt and Turkey among others whereby authorities are using national security to restrict civil liberties. Authorities shut down the internet during protests to quell dissent.

The other countries like United States, Australia, India, Singapore, Germany, France, Japan and countless others have adapted existing security regulations for aged populations, revising them to accommodate emerging technologies and social media as a strategy to combat cyber threats. Governments face the danger of sacrificing significant benefits due to the internet's expanded access to information, transparency, real time reporting of governmental misconduct and discrepancies, and its capacity for mobilization, all of which lead to increased online monitoring. The Canadian government expanded its authority to Canadian Security Intelligence Services to monitor individual's internet activities in 2015 (Chika, 2018). The rationale is that a transparent and unrestricted cyberspace is progressively facing

assaults, and various states seek to regulate either the entirety or at least a portion concerning it.

Regionally, Africa has experienced considerable growth in internet penetration and digital adoption, with Zimbabwe being among the country's leaders in this category. Concurrently, the same growth has exposed the continent to increased cybersecurity risks with the majority of countries lacking any viable cybersecurity system to protect the digital liberties and rights of their citizens (African Union, 2014). In trying to try and protect state and cybersecurity, internet shutdowns are getting more common in African countries. Ten countries in Africa, such as Zimbabwe, have limited the availability of online platforms and chatting platforms, frequently severing internet access in the course of voting periods or amidst demonstrations, similar to events observed in 2016. In 2020, African governments enacted 25 internet blackouts, an increase from 21 in 2019 with Algeria, Ethiopia, and Sudan facing the most significant effects among these nations (Taye, 2020). Therefore, due to this kind of digital disruptions of national wide blackouts, it calls for more studies that would protect civic space and protect digital rights.

In Southern Africa, cybersecurity has become a pressing concern with many countries facing challenges in protecting their critical infrastructure, personal data, digital rights (SADC, 2019). Internet blackouts are increasingly common in various African nations, according to Roberts & Ali (2021), according to the Zambian country report, government actions in 2016 included restricting access to sites focused on accountability like Zambian Watchdog. Therefore, this raises a concern for research study as Angola, Botswana along with Zimbabwe are obliged to ensure that its cybersecurity framework aligns with sectoral along with global standards and to ensure digital rights.

At local level, Zimbabwe is among the rising nations that have adopted digital solutions over the past twenty years, resulting in online access increasing to 55.4% in the final quarter of 2018, as reported by POTRAZ 2018 (Kabanda, 2018). Meanwhile, the country's cybersecurity framework remains weak with little legislation, policy and institutional capacity to protect citizens' digital freedoms and rights (Moyo, 2021). This can be seen when the tendencies of digital authoritarianism by Zimbabwe became pronounced at the onset of the 21st century when the nation was hit by massive social protests online, that's when Zimbabwe experienced its initial internet disruption in July 2016 and a subsequent disruption one in January 2019, with both incidents coinciding with periods of social unrest. These interruptions resulted in major internet services failures as authorities attempted to curb communication during the turmoil. For its execution, the Zimbabwean administration utilized laws like the Interception of Communications Act from 2007. Within its arsenal for digital repression, the Zimbabwean government additionally employs methods of online monitoring and coercion. Therefore, digital rights of the citizens are being suppressed through government's use of social media handles to intimidate, silence and arrest other citizens on matters that affect the party or the state of the government of Zimbabwe.

## **1.2 Purpose of the Study**

To assess the effectiveness pertaining to Zimbabwe's cybersecurity framework in protecting people's digital rights and freedoms.

## **1.3 Statement of the Problem**

The accelerated growth pertaining to digital technologies in Zimbabwe has outpaced the existing legal framework whereby there is increased internet access, social media usage, mobile money transactions and government digitalization, leading to a lack of protection of citizen's digital rights and freedoms. In early 2024, Zimbabwe had 5.48 million digital audience, representing a coverage rate of 32.6 percent, as reported by Kemp (2024).

However, there have been enormous vulnerabilities in digital freedoms and rights that have been brought in. These include lack of data protection laws, inadequate online privacy, rising instances of cybercrime and harassment, spread of misinformation, potential government surveillance, inadequate digital literacy among citizens and inadequate infrastructure and security that is affecting the people, businesses and digital economy. According to Munoriyana & Chiumbu (2019), the government of Zimbabwean has restricted expression rights via the Interception of Communications Act, a legislative measure governing oversight, which has led to a stifling impact on the profession of journalism. Recent research studies about cybersecurity in Zimbabwe depicts that there is need for effective cybersecurity frameworks which values digital rights and freedoms. Therefore, there is need to examine the effectiveness of cybersecurity laws and regulations that balance digital innovation with the protection of digital rights and freedoms.

#### **1.4 Research Objectives**

- a) To explore the nature of Zimbabwe's cyber security framework.
- b) To examine the effectiveness of Zimbabwe's cyber security framework in protecting citizens' personal data and preventing cyber threats.
- c) To identify gaps in Zimbabwe's cyber security framework that compromise digital rights and freedoms.
- d) To propose strategies that improve Zimbabwe cyber security framework capacity to protect people's digital rights and freedoms.

#### **1.5 Research Questions**

- a) What is the nature of Zimbabwe's cyber security framework?
- b) How effective is Zimbabwe's cyber security framework in promoting citizens' personal data and preventing cyber threats?

- c) What are the gaps in Zimbabwe's cyber security framework that compromise digital rights and freedoms?
- d) How can Zimbabwe's cyber security framework be strengthened or improved to prevent cyber threats and protect digital rights and freedoms.

## **1.6 Assumptions**

- The research assumes that the current cybersecurity framework is inadequate in protecting digital rights.
- The study assumes that stakeholder engagement is critical for effective cybersecurity policy development.
- The research assumes that there is a direct relationship between robust cybersecurity measures and safeguarding individual freedoms

## **1.7 Significance of the Study**

The following people will benefit from the study

- **Policy makers**

The research is anticipated to engage the attention of the Ministry of Justice, Legal Affairs and Parliamentary Matters, as well as the Ministry of Information and Communication Technology (ICT) as well as Postal and Courier Services along with other pertinent governmental bodies including (POTRAZ), Zimbabwe Cyber Security Agency (ZCSA) and Zimbabwe Information and Communication Technology (ZICT) Division. It is important because policy makers will make use of this study in coming up with policies and digital frameworks which promote the rights and freedom of citizens. Therefore, policy makers can develop effective policies and strategies to protect digital rights of citizens. Hence, informed policy decisions lead to improved laws and policies that promotes digital rights and freedoms of people.



- **Civil society**

This research can also help NGOs, Community Based Organizations and human rights organization and advocacy groups to become aware of the challenges that people are facing in application of digital innovation and online platforms. This study is important because civil societies will have access to advocate for digital rights, support policy reform, educate the public on cyber security and monitor and report human rights violation, thus, leading to stronger human rights protection. Cybersecurity research can inform advocacy efforts, empowering citizens to demand better online protections from the governments.

- **Researcher**

The research benefits the researcher as it adds new knowledge, builds research skills, improves research methods, helps policy makers to create better policies through recommendations, develops new theories and fosters collaboration about cybersecurity framework. This research is important as it may assist the researcher to gain a more profound insight into the difficulties encountered by users in the digital realm.

- **Zimbabwean citizens (online users)**

The research is important as it may empower citizens through a balanced approach to security and human rights in Zimbabwe's digital space by highlighting concerns and opportunities that supports safe online environments, respect for fundamental rights and inclusive digital growth. Hence, people will be safe online.

### **1.8 Delimitations of the Study**

Research centered on the effectiveness of Zimbabwe's cybersecurity framework in protecting people's digital rights and freedoms specifically examining the country's laws, regulations, policies, and institutions related to cyber security. This study was carried out in Harare, Zimbabwe. The researcher also looked other studies which aligned with

cybersecurity as of 2014 to 2024. The study also focused on the implications of Zimbabwe's cyber security framework for digital rights and freedoms. Hence, the study did not examine other aspects of cyber security, such as economic or political implications.

### **1.9 Limitations of the Study**

Examiner encountered some obstacles which includes respondent bias, limited knowledge of participants, access to sensitive information and the refusal of other participants to disclose the information whereby some participants did not consent to be recorded during the interview. Rapid evolution of technology also rendered research outdated quickly, necessitating continuous awareness of current trends and threats were also a challenge. Another challenge was access to key participants for example those who work in government which led to bias or unrepresentative samples. Henceforth, the researcher find it difficult to access sensitive information and limited cooperation from government agencies or private organizations. Therefore, the research was complemented with secondary data which includes journals and books among others.

### **1.10 Definition of Key Terms**

- Cyberspace is the information environment created by human beings where computers and similar telecommunication gadgets and other components that allow rapid movement of large quantity of data are connected (Williams, 2014).
- Cybercrime has been used as a generic term for describing crimes that occur in cyberspace (Kurebwa, 2021).
- Surveillance is the application of technological tools for the purpose of gathering or retrieving information about individuals or groups, often in a manner that is concealed or unnoticed by them (Marx, 2016).

- According to Jang (2014), cybersecurity is defined as protecting information and communication networks, and information cyber from cyberthreats or cyberattacks that occur in the cub we space or networks.

### **1.11 Dissertation Outline**

Chapter one provides introduction; the background to the study, its purpose, statement of the problem, research objectives and questions, assumptions, significance of the study, limitations and delimitation of the study as well as definition of key terms and summary.

Chapter two covers literature review and theoretical frameworks, the effectiveness of cybersecurity in protecting digital rights, research gaps, solutions to cover the gaps and summary.

Chapter three covers research paradigm, research methodology, research design, population sample, sampling methods, data collection methods, validity and reliability, data presentation and analysis, pilot testing, ethical considerations and summary.

Chapter four present and analyze the results of the findings using a thematic approach which entails coding of data from in depth interviews which answers the research objectives/questions.

Chapter five presents a summary, conclusions, and suggestions derived from the research results.

## **CHAPTER TWO**

### **LITERATURE REVIEW AND THEORETICAL FRAMEWORK**

#### **2.0 Introduction**

Research consists international treaties, regional agreements and local laws designed to govern the digital environment. There is also theoretical framework which includes digital authoritarianism theory and cybersecurity maturity model framework. Furthermore, the research is directed by the questions posed in the study which includes nature pertaining to Zimbabwe's cybersecurity, its effectiveness, the gaps of Zimbabwe's cybersecurity and strategies or possible solutions to the gaps as well as the research gap and a summary.

#### **2.1 Theoretical framework**

Cybersecurity frameworks are vital in safeguarding digital rights and freedoms in an increasingly interconnected world. The study is guided by two theoretical frameworks which are digital authoritarianism theory and the cybersecurity maturity model (CMM) framework. These frameworks provide a view for examining the nature, effectiveness, and gaps within Zimbabwe's cybersecurity policies.

##### **2.1.1 Digital Authoritarianism theory.**

Digital authoritarianism theory examines the state sponsored technology initiatives to control, monitor, as well as repress their citizens. It highlights how governments exploit cybersecurity laws and policies to consolidate power and suppress dissent, often under the guise of national security (Gorwa & Milan, 2021). One of the assumptions of this theory is that, governments deploy surveillance technologies to monitor citizens, collect personal data, and track dissenting voices. Therefore, this assumption is of the view that, states can use these tools to suppress opposition (Feldstein, 2019). Moreover, authoritarian regimes often control access to information by censoring critical voices and manipulating online content.

According to Bradshaw & Howard (2019), there is blocking of websites, removing content, and spreading propaganda as a way of suppressing citizens. In addition, cybersecurity laws and policies can serve as instruments for legitimizing authoritarian practices. In addition, digital authoritarianism undermines privacy rights through government's means of collecting and storing of personal data. Therefore, this assumption is of the view that weakened privacy protections paves way for broader abuses of digital rights (Haggart et al., 2021).

In addition, the cybersecurity paradigm in Zimbabwe may be analyzed critically with the theory of digital authoritarianism. For instance, the Zimbabwean Cyber and Data Protection Act has provisions that are problematic regarding potential state's surveillance. The Act's wide definitions of cybercrimes and data processing may be utilized to repress dissent and infringe on the right to privacy. Henceforth, by applying digital authoritarianism theory, this study investigates how Zimbabwe's cybersecurity policies might promote state surveillance, censorship, and the erosion of digital rights. Therefore, this theory highlights the need to balance national security objectives with the protection of fundamental freedoms.

### **2.1.2. Cybersecurity Maturity Model (CMM) Framework**

The cybersecurity maturity model (CMM) framework provides an approach to evaluate the effectiveness of cybersecurity policies and practices. It emphasizes the development of robust cybersecurity systems through progressive maturity levels, from basic awareness to full optimization (Gill et al., 2018). One of the assumptions of this study is that, cybersecurity structures advanced through five levels of maturity which are initial, managed, defined, quantitatively managed, and optimizing. Every level signifies a development in organization's abilities and strength in tackling cybersecurity issues (Caralli et al., 2010). Moreover, effective cybersecurity requires collaboration as it is essential among governmental bodies, private sector participants, and civil society. The framework assumes that multi-stakeholder

engagement enhances policy effectiveness (Singer & Friedman, 2014). Moreover, the cybersecurity policies should be informed by risk assessments to target resources and address vulnerabilities. The assumption is that a risk-based approach leads to more effective outcomes (Gordon et al., 2020).

In addition, cybersecurity requires continuous evaluation for better improvement. The framework assumes that organizations and governments must adapt to emerging threats and technologies (Gill et al., 2018). Therefore, the CMM Framework is important in assessing Zimbabwe's cybersecurity framework. Hence, by examining the maturity levels of policies and practices, this study evaluates their effectiveness in addressing cyber threats and protecting digital rights. For example, the framework can help identify whether Zimbabwe's policies are reactive or proactive, as well as the extent of stakeholder collaboration in policy implementation.

To add on, digital authoritarianism theory and the CMM Framework complement each other by providing both critical and developmental opinions on cybersecurity. In light of this, digital authoritarianism theory offers a critical view for examining the potential misuse of cybersecurity policies, highlighting risks to digital rights. In contrast, the CMM Framework focuses on feedback or analysis, providing a strategy for improving policy effectiveness.

Furthermore, these theories intersect in evaluating surveillance practices whereby digital authoritarianism theory critiques the misuse of surveillance, while the CMM Framework assesses whether such practices align with best practices and maturity standards. In addition, the CMM Framework's emphasis on multi-stakeholder collaboration aligns with the advocacy for transparency and accountability in digital authoritarianism theory. Both frameworks underscore the importance of inclusive policymaking to protect digital rights. The combination of digital authoritarianism theory and the CMM Framework provides a comprehensive approach to assessing Zimbabwe's cybersecurity framework. Digital

authoritarianism theory critiques the potential misuse of policies, while the CMM Framework offers tools for evaluating and improving their effectiveness. Collectively, these theories steer the research towards tackling essential inquiries regarding the equilibrium the balance between ensuring public safety and upholding digital privileges and freedoms.

## **2.2 Cybersecurity framework consist of the following**

The incorporation within the global framework for cybersecurity includes international treaties, regional agreements, and national legislations with an overall objective of governing the virtual environment. There are several treaties and agreements globally that influences cybersecurity frameworks as well as affects national laws in different countries such as Zimbabwe. For instance, UN Human Rights Council Resolution 20/8 asserts in particular that the same rights people have offline are to be enjoyed online (UN General Assembly, 2015), providing a guiding principle which Zimbabwe's cybersecurity policy should adhere to. Besides, it also encompasses the Budapest Convention on Cybercrime in Europe that contains principles which emphasized the need for international cooperation in combating cybercrime as well as safeguarding basic human dignity that serve as a guide to the creation of national legislation addressing cybercrime and related cybersecurity problems (Council of Europe, 2001). Hence, Budapest Convention calls upon the member states to adopt provisions that respect and protect core human rights like freedom of expression and privacy and reasser the importance of aligning national laws with international norms.

Moreover, there are global initiatives, such as the G20 Digital Economy that also advance policies that are both focused on digital rights and cybersecurity. Therefore, these initiatives challenge countries to adopt best practices that respect privacy and freedom of expression o n the web, thus exerting pressure on Zimbabwe's policy trajectory (G20, 2020). In addition, the Universal Declaration of Human Rights, established in 194 mandates safeguarding of rights related to free expression and personal privacy. Hence, these provisions are critical in

deciding whether cybersecurity laws encroach digital freedoms or not. Likewise, there is the International Covenant on Civil and Political Rights of 1966 in Articles 17 and 19 of the ICCPR which emphasises the protection of human beings from arbitrary interference with privacy and preserve the entitlement to express oneself freely. United Nations (1966) argues that, cybersecurity measures should be in agreement with these rights. All nations, therefore, ought to bring its cybersecurity legislation in accordance with international standards.

In addition, at continental level, African Union (AU) has a vital role in influencing Africa's cybersecurity policies. As a result, there is African Union Agreement regarding Cybersecurity as well as the data privacy information established in 2014, aimed primarily at enhancing cybersecurity measures and ensuring the safeguarding of information throughout continent associated with Africa. African Union (2014) suggests that the convention emphasized protection of civil liberties and essential rights online. Thus, Zimbabwe's adherence to this convention is important since it is essential to bring the country's national cybersecurity policies up to regional standards.

Further, at regional level, Southern African Development Community (SADC) through Model Law on Cybercrime and Cybersecurity introduced in 2012, make guidelines on how cybercrime and cybersecurity must be regulated by its members. Therefore, it encourages cooperation among member states in combating cybercrime to strengthen national computer emergency response teams (CERTs) and improve cybersecurity measures while safeguarding individual rights (SADC, 2012). Therefore, SADC framework is supportive of best practices in cybersecurity that may inform policies in Zimbabwe. Therefore, commitment by Zimbabwe to this framework is essential in ensuring that its cybersecurity does not violate digital rights and freedoms.

At local level, Zimbabwe has implemented multiple regulations related to digital rights and access. Consequently, these regulations encompass the Access to Information and Protection



of Privacy Act (AIPPA) from 2003, the Interception of Communications Act (ICA) established in 2007, the Cyber and Data Protection Act (CDPA) enacted in 2021 and SI 155 of 2024, along with various other laws. Therefore, these legislations followed as the trend showed people were more accessing cyber space through online services. As Karekwaivanane & Msonza (2021) explain, the legislation allows the state to establish a monitoring center for Intercepting Communications, leading to the government focusing on dissent through intrusive surveillance under the pretext of protecting national security. This is outlined in section 9 of the Interception and Communications Act of 2007, which compels telecommunication companies to supply the government with continuous and real time monitoring capabilities for communication interception, or face penalties, including fines or sentences of up to three years in prison. Henceforth, this study is of the view that Zimbabwe's cybersecurity laws is enabling the government to conduct online surveillance to its citizens, hence, violating privacy rights and freedom of expression rights.

To add on, the Cybersecurity and Data Protection Act of 2021 represents foundational element of Zimbabwe's cybersecurity infrastructure because it emphasizes the safeguarding of data while also tackling cybersecurity challenges via modifications to current legislation. This includes changes to Chapter VIII of the Criminal Law (Codification and Reform Act) Chapter 9:23, which focuses on crimes associated with computers, the Criminal Procedure and Evidence Act Chapter 9:07, along with the Interception of Communications Act. Consequently, the main objective of the legislation revolves around safeguarding data privacy and the security of any information collected by data handlers both domestically and internationally. Subsequently, data controllers must adhere to the requirements of the Act by managing data in an ethical and lawful way, making sure that data is gathered solely for defined and legitimate purposes. This Act, according to Ndlovu (2021), criminalizes various cybercrimes like hacking, data breaches, and computer system unauthorized access, thereby

offering a legal ground for prosecuting offenders. Nevertheless, enforcing such provisions can be concerning regarding their misapplication to stifle dissidence and limit freedom of expression.

### **2.3 Implications for digital rights and freedoms**

The relationship or connection between Zimbabwe's cybersecurity framework and digital rights and freedoms shows several implications. In this regard, while the cybersecurity framework aims to protect national security and fight cybercrime, there is a risk that such measures may violate individual rights. The use of surveillance and monitoring to enforce cybersecurity laws can lead to violations of privacy and freedom of expression (Mabika, 2021). According to Zetter (2020), cybersecurity measures should not become tools for political repression. In addition, the potential misuse of cybersecurity laws can create restrictive effect on freedom of expression. When citizens fear surveillance or legal repercussions for their online activities, it may discourage open dialogue and dissent, which are essential for democratic governance (Nyoni, 2020). The Cybersecurity and Data Protection Act's provisions on hate speech and cyberbullying could be interpreted broadly, leading to the limitation of valid speech.

Moreover, the gathering and handling of individual information within the context of the cybersecurity framework raise significant privacy concerns. If not adequately regulated, the accumulation of personal data can lead to unauthorized access and breaches, compromising individuals' privacy rights (Goucher, 2018). Therefore, this research is of the view that weak data protection enforcement worsens privacy issues. Hence, aligning Zimbabwe's cybersecurity framework with international standards and best practices is essential for safeguarding digital rights. International cooperation can facilitate knowledge sharing and

capacity building, ensuring that cybersecurity measures respect human rights while enhancing national security (Goldsmith & Wu, 2006).

## **2.4 Case Studies on Cybersecurity and Digital Rights**

In Northern Europe, Estonia is widely recognized as a global leader in cybersecurity and digital rights. Following the 2007 cyberattacks, the country established the National Cybersecurity Strategy, emphasizing resilience and collaboration (Vaarandi et al., 2022). The government's e-Estonia initiative integrates cybersecurity into all digital services, encompassing e-governance, e-health, and e-residency. Key achievements include decentralized digital identity. Estonia's advanced ID card system ensures secure access to digital services while safeguarding personal data. Moreover, collaboration between government, academia, and industry enhances the country's ability to respond to cyber threats effectively (Kaska & Ottis, 2021). In addition, Estonia's framework aligns with the EU's General Data Protection Regulation (GDPR), ensuring compliance with international standards for digital rights. Estonia's success demonstrates the importance of transparency, technological innovation, and multi-stakeholder collaboration in building effective cybersecurity frameworks.

In Africa, Rwanda's National Cyber Security Policy, established in 2015, provides a comprehensive framework for securing the country's digital infrastructure. The Rwanda Information Society Authority (RISA) oversees the implementation of cybersecurity measures (Ndahiro, 2022). RISA's centralized approach ensures effective coordination of cybersecurity initiatives. Moreover, investments in cybersecurity training and education have enhanced the country's ability to tackle cyber threats (Ndahiro, 2022). In addition, Rwanda's alignment with international human rights norms has strengthened trust in its cybersecurity framework (Mugisha et al., 2023). Rwanda's progress illustrates the potential for emerging economies to develop resilient and rights-focused cybersecurity frameworks.

The comparative analysis of these countries reveals that Estonia and Rwanda demonstrate the importance of strong institutions in implementing effective cybersecurity frameworks.

## **2.5 The nature of Zimbabwe's cyber security framework.**

Zimbabwe's cybersecurity framework has improved in response to increasing global and local cyber threats, focusing on the protection of national security, economic interests, and individual rights. This framework includes laws, policies, institutional arrangements, and technical measures that aim to safeguard the digital landscape while exploring the challenges of digital rights and freedoms.

### **(a) Legislative framework**

The legislative aspect of Zimbabwe's cybersecurity framework is primarily centred in the Cybersecurity and Data Protection Act (2021). This law was established to provide a comprehensive legal framework for addressing cybersecurity issues and protecting personal data (Zimbabwe Government, 2021). The Act aims to prevent cybercrime, protect information systems, and establish protocols for data protection. However, its implementation has raised concerns about potential challenges on individual freedoms, particularly regarding freedom of expression and privacy rights. Critics argue that, while the legislation seeks to enhance cybersecurity, it may also be employed as a tool for political repression. According to Moyo (2020), the Act has provisions that can be interpreted to restrict freedom of speech and dissent, thereby posing risks to digital rights. The challenge lies in ensuring that laws are applied transparently and do not serve as instruments of control.

### **(b) Institutional framework**

Zimbabwe has established various institutions tasked with overseeing cybersecurity initiatives. The Cyber Security and Cyber Crime Unit (CSCCU) within the Zimbabwe Republic Police is responsible for investigating cyber-related offenses, while the Zimbabwe National Security Agency (ZNSA) plays a critical role in coordinating national cybersecurity efforts (Matsika, 2020). These institutions are intended to facilitate cooperation among

government agencies, civil society, and the private sector in addressing cybersecurity challenges. However, there are concerns about the adequacy of resources and expertise within these institutions to effectively combat sophisticated cyber threats. A report by the Internet Governance Forum (2021), highlighted the need for capacity-building initiatives to enhance the skills and knowledge of personnel involved in cybersecurity efforts in Zimbabwe.

**(c) International engagement and compliance**

Zimbabwe's approach to cybersecurity also involves engagement with international frameworks and norms. Participation in regional and global initiatives, such as the African Union's Cybersecurity Strategy, underscores the importance of collaboration in addressing cross-border cyber threats (African Union, 2020). Moreover, compliance with international standards for cybersecurity, such as those outlined by the International Telecommunication Union (ITU), is crucial for enhancing Zimbabwe's cybersecurity posture. Adopting international best practices can help Zimbabwe align its cybersecurity efforts with global expectations while fostering trust among international partners (Zhou, 2019).

**2.6 The effectiveness of Zimbabwe's cybersecurity framework in protecting citizens' personal data and preventing cyber threats.**

Cybersecurity has become a pivotal issue in Zimbabwe, given the rapid digitization across various sectors. With an increasing number of Zimbabweans relying on digital platforms for communication, banking, and government services, ensuring the safety and privacy of personal data has become critical. Zimbabwe has witnessed a growing trend towards digital transformation. According to Ncube (2024), the rise in internet usage has brought along a surge in cyber threats, including data breaches and financial fraud. The country's cybersecurity framework is primarily governed by the Cyber and Data Protection Act of 2021. This law was established to regulate how personal data is collected, processed, and stored. Gwagwa (2021), argues that while the law is a step in the right direction, its

enforcement has been less than optimal due to weak institutional capacity and limited public awareness.

Furthermore, one of the critical functions of cybersecurity frameworks is to protect personal data from unauthorized access. According to Matunhu & Mazambani (2021), Zimbabwe has lagged in adopting data protection technologies such as encryption and multi-factor authentication. They suggest that while the legal framework exists, the lack of technical infrastructure weakens its implementation, leaving citizens vulnerable to data theft. Additionally, in a report by Zimbabwe Information and Communication Technologies (ZICT) Institute (2022), it was revealed that over 60% of Zimbabwean businesses and public institutions do not fully comply with global data protection standards, creating significant loopholes in the system.

In addition, Zimbabwe has recently made a significant advancement in the protection of confidential information through Statutory Instrument 155 of 2024 as internet access becomes more affordable, particularly following the launch of Starlink, which has significantly reduced broadband prices. This regulation requires all entities processing personal data to obtain a data controller license, ensuring accountability and adherence to data security standards (Zimpricecheck, 2024). Therefore, Statutory Instrument 155 states that, data protection officer oversees compliance, the requirement to report data breaches within 24 hours and informing affected individuals within 72 hours if there is a risk or harm. The timing of these regulations is critical as the increased internet availability encourages more organizations to digitize processes and handle large volumes of personal data including sensitive information.

However, several challenges hinder the effective implementation of cybersecurity in Zimbabwe. The Zimbabwe National Cybersecurity Policy was designed to provide a strategic framework, but according to Biti (2020), limited funding and inadequate policy coordination between government agencies hamper its success. Moreover, Zimbabwe's

economic challenges, including hyperinflation and lack of right towards international funds, make the matter challenging regarding state and businesses to invest in cutting-edge cybersecurity solutions (Nyamunda, 2021). This has led to over-reliance on outdated software and security systems, making networks vulnerable to attacks

The global nature of cybersecurity threats necessitates international cooperation and alignment with international standards. Zimbabwe's cybersecurity framework has the potential to benefit from engaging with regional and global partners to share best practices and enhance its capabilities (Schmidt, 2020). Collaborative efforts can also help improve the nation's response to cyber incidents and provide access to resources for capacity building. However, there is still a need for Zimbabwe to actively participate in international cybersecurity forums and adopt recognized frameworks, such as those proposed by the International Organization for Standardization (IOS), to enhance its security posture (Alder 2020). Engaging in international dialogues can help Zimbabwe stay updated on emerging threats and strategies, which is essential for protecting citizens' personal data.

## **2.7 Gaps in Zimbabwe's cybersecurity framework that compromise digital rights and freedoms.**

### **(a) Lack of comprehensive legal protections**

One of the significant gaps in Zimbabwe's cybersecurity framework is the absence of comprehensive legal protections for digital rights. While the Cybersecurity and Data Protection Act (2021) aims to establish guidelines for data privacy and cybersecurity, it lacks robust provisions that explicitly protect individual rights, such as freedom of expression and privacy (Moyo, 2020). Scholars argue that legislation should not only focus on security aspects but also ensure that it upholds human rights principles. Without explicit legal protections, citizens may find themselves vulnerable to arbitrary surveillance and restrictions on their digital freedoms (Cohen, 2019). Moreover, existing laws often provide vague definitions and broad powers to authorities, which can lead to misuse. As Nyoni (2020)

notes, such ambiguities create an environment where state actors can exploit the law to suppress dissent and control information flow, thereby infringing on civil liberties.

**(b) Insufficient accountability mechanisms**

Accountability mechanisms are crucial for ensuring that cybersecurity practices do not infringe on individual rights. However, Zimbabwe's framework currently lacks robust mechanisms for oversight and accountability concerning the actions of state agencies involved in cybersecurity (ZIMRA, 2019). The absence of independent bodies to review cybersecurity practices means that abuses, such as unwarranted surveillance or data breaches, may go unchecked. Research indicates that strong accountability frameworks are essential to prevent governmental overreach and to protect citizens from potential abuses of power (DeNardis, 2016). Without such mechanisms, there is little recourse for individuals whose rights may be violated under the guise of cybersecurity enforcement.

**(c) Limited public awareness and engagement**

Public awareness and engagement are critical components of any effective cybersecurity strategy. In Zimbabwe, there is a notable gap in programs designed to enhance public knowledge about their digital rights as well as the implications of existing cybersecurity measures. As Renaud & Goucher (2020) highlight, citizens must be informed about their rights to effectively advocate for them. The lack of public awareness campaigns and educational programs regarding cybersecurity means that many individuals remain uninformed about their rights, making them more susceptible to violations. Moreover, when citizens are not engaged in discussions surrounding cybersecurity legislation, policies may fail to reflect their needs and concerns. Nyoni (2020) emphasizes that inclusive policymaking processes are essential for ensuring that laws protect rather than hinder digital rights.

**(d) Surveillance provisions**



The provisions related to surveillance within Zimbabwe's cybersecurity framework are often ambiguous and can lead to potential abuses. The Cybersecurity and Data Protection Act (2021) allows for extensive data collection and monitoring without clearly defined limits, raising concerns about the right to privacy (Moyo, 2020). Scholars argue that surveillance laws must include specific guidelines to prevent the misuse of surveillance technologies, especially in contexts where state surveillance may be used to target dissenters or marginalized groups (Lyon, 2015). Additionally, without stringent oversight on surveillance practices, there is a risk that authorities may engage in mass surveillance, infringing on individual privacy rights (Taddeo & Floridi, 2018). This gap has a significant threat to freedom of expression, as individuals may self-censor themselves due to the fear of being monitored.

## **2.8 Strategies on literature to address the gaps**

Looking forward, Zimbabwe must take critical steps to improve its cybersecurity framework. Gwagwa (2021), suggests that the government should prioritize partnerships with international cybersecurity organizations to boost its technological capacity. In addition, Mandishona (2023), argues for the need to create a centralized cybersecurity command centre that can monitor threats in real-time, enabling rapid response to breaches. The African Union Convention on Cybersecurity and Personal Data Protection, to which Zimbabwe is a signatory, could also provide a blueprint for future legislative reforms. However, the key to success lies in the successful execution of these policies necessitates a collaborative endeavor involving both public and private sectors. The literature suggests a critical need for reforms that prioritize human rights in the development of cybersecurity legislation, ensuring that citizens are protected against state overreach (Moyo, 2020).

Moreover, the study points to the importance of public awareness and education in navigating the complexities of digital rights and cybersecurity. Renaud & Goucher (2020), note that empowering citizens with knowledge about their rights can foster a more informed

public that actively engages in protecting its freedoms. In Zimbabwe, where access to information and digital literacy may be limited, enhancing public understanding of cybersecurity issues is essential. This approach not only helps individuals to recognize potential violations but also encourages civic engagement in advocating for more transparent and accountable governance.

In Zimbabwe, where surveillance practices are a concern, there is need for international laws that govern digital rights and freedoms. Taddeo and Floridi (2018), argue that ethical frameworks must guide cybersecurity policies to ensure they respect individual rights. The study argues that, there is need for international cooperation in shaping effective cybersecurity policies. As Schmidt (2020) suggests, global collaboration can help countries adopt best practices and develop norms that safeguard digital rights. For Zimbabwe, engaging with international frameworks and organizations can facilitate the establishment of a cybersecurity environment that respects individual freedoms while addressing national security concerns.

## **2.9 Research gap**

Zimbabwe's cybersecurity framework remains a critical area for scholarly examination due to its implications for digital rights and freedoms specifically privacy, unrestricted speech, as well as public access to information. Studies such as those by Nyakudya (2022), focus on data breaches but neglect the broader socio-political implications of these frameworks on digital freedoms. Although global studies like those by Deibert (2019), discuss the relationship between cybersecurity and digital rights, there is limited research on how this relationship manifests in Zimbabwe. However, academic research into how cybersecurity policies facilitate such actions remains limited. Henceforth, this study is of the view that by addressing this gap requires an exploration of whether these policies prioritize national security at the expense of fundamental freedoms. To add on, studies by Tade and Adeniran

(2020), emphasize the importance of multi-stakeholder collaboration in cybersecurity policy development but fail to address how this dynamic develops in Zimbabwe. This research is of the view that, including stakeholders' decision is essential for identifying gaps between policy making and implementation. To add on, Zimbabwe has been cited in reports by Freedom House (2022), as a country with increasing tendencies towards digital authoritarianism. However, academic studies have not thoroughly examined how the cybersecurity framework enables or limits such practices. This study argues that, there is limited research on whether these measures are justified by security concerns or represent an overreach that violate digital rights.

## **2.10 Chapter summary**

This Chapter has reviewed literature on an assessment of Zimbabwe's cybersecurity framework: "Implications for digital rights and freedoms.". The Digital Authoritarianism theory and the Cybersecurity Maturity Model (CMM) Framework are theories that guide this study. The review and framework were done in fulfilment of the research aim and objectives. The next chapter is going to present research methodology and design.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY AND DESIGN**

#### **3.0 Introduction**

This chapter outlines the various methodologies employed to gather and analyze data that was crucial to the research. This document encompasses detailed information regarding the research methodology employed in this investigation focused on comprehending the assessment of Zimbabwe's cybersecurity framework: Implications for digital rights and freedoms, for instance, the tools used, sources of data, methods of collection, and research methodologies. The research used a qualitative methodology and it was conducted in Harare, specifically focusing on social media users who were willing to express their views on the cyber security framework and its implications for digital rights and freedoms as well as government officials. Semi structured interviews were used for information gathering. Purposive sampling technique was used to select key informants like government officials. The data that was collected was later analyzed to establish the challenges faced by citizens in navigating their rights on digital platforms.

#### **3.1 Research philosophy/ paradigm**

Research paradigm is also important in this research. In the words of Davies & Fisher (2018), paradigms can be defined as various ways of looking at the world and are frequently the basis upon which research is conducted, they are a collection of presumptions regarding what is reality, how knowledge is produced and what is worth knowing. This study employed the constructivist paradigm. In this regard, constructivists, like interpretivists, believe in more than one reality rather than a single truth. The constructivism paradigm is centered on the idea that individuals create their own understanding of the world based on experiences and reflection. Constructivism, according to Cresswell (2014), deals with the building of subjective interpretations and meanings of one's own experience on some matters based on

their social and historical context. Research in this area focuses on the meanings people assign to their experiences, often using qualitative methods like interviews and case studies. This approach seeks to uncover the reasons behind events. Therefore, in this research participants were interviewed regarding their experiences in cyberspace, how they understand Zimbabwe's cybersecurity frameworks and how effective are those frameworks in protecting digital rights and freedoms.

### **3.2 Research methodology**

Research methodology is a scientific process of solving an issue by explaining, describing and forecasting. It can also be termed as the scientific investigation of approaches to knowledge acquisition. Research methodology is meant to act as a broad guideline in order to facilitate and direct the whole process of a research activity within any discipline, according to Mukherjee (2019). In this study qualitative research was utilized. Qualitative research is a process of understanding grounded in a particular methodological orientation to pursue knowledge that examines an issue or human/social problem. Qualitative methodology focuses on acquiring in-depth understanding of various contexts, perspectives, and viewpoints (Boru, 2018). The researcher thus, constructs an in-depth, integrative picture by examining words, hears rich accounts of participants and conducts the study under natural conditions.

### **3.3 Research design**

Case study research design was used because it helps to strengthen the study; it is more of a decision regarding what to study than a methodological as it is time and context place bounded. According to Ridder (2017), case study research scientifically investigates into a real-life phenomenon in depth and within its environmental context as such a case can be an individual, a group, an organization, an event, a problem, or an anomaly. Therefore, in this research, case study design allows one to have an in-depth examination of Zimbabwe's

cybersecurity frameworks and to understand its implications on digital rights and freedoms. For creating valid and reliable knowledge, there must be a strong research design (Bhatia, 2018). It also assists one in having contextual knowledge in terms of political, economic and social factors influencing it. There were a few data collection methods employed in this study that include interviews, document analysis and observations to understand how digital freedom and rights are practiced using purposeful sampling.

### **3.4 Population and sample**

The study consisted of two different categories of participants which are key informants consisting of government officials, and non-governmental officials as well as the subjects of the study who are social media users and bloggers. Cresswell (2014) highlighted the significance of steering clear of research environments where results could potentially align with personal interests. Hence, the study was interested in the government officials which comprised of Ministry of Information Technology (ICT) officials, cybersecurity agency officials, law enforcement officials and policymakers. Non-governmental officials include social media users, human rights defenders, online activists, businesses, telecommunication companies, e-commerce platforms, media organisations among others were also targeted. Therefore, by targeting these participants, the researcher had deeper understanding of the implications of digital rights and freedoms in Zimbabwe. The sample size consisted of 25 participants (10 Information and communication Officers and 15 people who are victims of the cyber security framework).

### **3.5 Sampling method**

This study utilized non-probability sampling (where one does not randomly choose the participants), hence, the study utilized purposive sampling approach in conducting interviews. Non probability sampling, according to Etikan & Bala (2017), is a method of sampling procedure that will never provide a foundation for any probability opinion that the

universe elements will have a chance to be represented in the study sample since purposive sampling is all about judgement by a researcher of who will provide the best information in order to survive for the sake of study. Hence, the participants were selected non-probability based on some features, characteristics, or targets. Non probability is easier to achieve by dealing with experienced, knowledgeable or with special knowledge in cybersecurity and digital rights and freedoms participants.

### **3.6 Data collection methods**

Data collection is a procedure where the researcher acquires the information required to solve the research problem. Data collection method allows a researcher to obtain first-hand information and fresh ideas on research problem.

#### **(a) Primary data collection methods**

##### **(i) Semi structured Interviews**

In qualitative research interviews, researchers employ open ended and expansive questions directed at one or more participants, recording their replies. Creswell (2012) adds that, audiotapes are usually used to produce more accurate transcription. Closed-ended questions may prompt participants to respond in a specified direction, but open-ended questions are typically used in interviews with a desire for unbiased responses (Creswell, 2012). According to Kombo and Tromp (2014), interviews allow the researcher to gain more specific information from the primary informants on a problem that is under investigation. Sugiono (2008) characterizes an interview as a dialogue between two individuals intended to exchange information and ideas through a series of questions and answers, which facilitates the revelation and construction of meaning regarding a specific topic. Ultimately, this yielded a significant volume of descriptive data from participants, as semi structured interviews facilitate two way communication and allow interviewers to grasp not only the answers to the questions but also the rationale behind those responses, which is why the

researcher utilized them. All the interviews were taped on a telephone. The researcher took written notes. Field notes that were taken during the interviews were taken with the respondents's consent. Each interview lasted between 2 minutes and 9 minutes. Interviews allowed participants to answer in their own words.

## **(b) Secondary data collection methods**

Secondary sources were also used to fill the gaps of primary data collection.

### **(i) Document analysis**

Document analysis has been used within the study to provide an insider information that the participants would suppress because it is sensitive information, as well as its ability to provide a good source of background information. Morgan (2022) prescribes that, document analysis is a thoughtful provoking research tool that has been utilized to investigate various forms of documents. Therefore, these documents include policy documents, letters, agendas, minutes, administrative reports, files, books, journals, news clippings among others. Therefore, secondary sources were used in this study to examine the effectiveness of Zimbabwe's cybersecurity framework in promoting and protecting digital rights and freedoms. Thus, data from the review document analysis was combined with data from interviews.

## **3.7 Validity and reliability**

Validity is how accurately a measuring device measures what it is designed to measure. According to Truscott (2023), validity will depend on if the research actually answers the question intended to answer, if the conclusions drawn from it by its authors, and by subsequent reviewers, are true, thus validity depend on the aims of a research. For instance, an intelligence test must measure intelligence alone and must be designed for the same reason. Thus, it can be valid by using appropriate methods of measurement and appropriate



methods of sampling to determine your subjects. Validity can also be measured by construct validity, content validity, criterion validity as well as internal and external validity by way of expert judgement.

To end this, reliability refers to the consistency of responses in measurements so that when asked repeatedly, the same answer is to be provided. In the event that the answers do not match, then reliability is lost. According to Middleton (2024), reliability can be achieved by standardizing research conditions, interviewing among other things. Moreover, reliability can be measured through test-retest reliability, interrater reliability as well as internal consistency. Reliability can be ensured through pilot testing, training data collectors and using multiple measures to test the research instrument and make necessary adjustments.

### **3.8 Data presentation and analysis**

The interviews were all translated and transcribed word for word into English and quotations were extracted from the transcripts. Data analysis involves the examination and classification of interview transcripts, observational notes, and various forms of non textual data gathered by a researcher, aiming to gain a deeper understanding of a phenomenon (Bhatia, 2018). Major ideas and themes were identified and coded to enable a thick grid of analysis, comparisons, and data presentation. The personal experiences, opinions and comments of the respondents were then categorized according to recurring selected themes of all the interview transcripts.

### **3.9 Pilot testing**

Pilot testing allows researchers to assess how accurately participants comprehend survey questions, which in turn has implications for the reliability of findings. Through Brooks, Reed & Savage (2016), pilot studies have the potential to uncover the time it takes to complete the surveys and interviews, practice doing extensive quantitative and/or qualitative

analysis to assist in reviewing the question areas, provide meaningful data on the environment for the research and provide room for reflection to direct the main research study and perhaps increase the potential for success. Through pretesting with a smaller group of people, researcher can identify questions that are ambiguous or confusing and rephrase them. So an argument may be made that pilot testing enables researchers to try and conduct an interview with some questions for some individuals to try and gauge their responsiveness and recognize some confusing or tricky questions and fix them prior to submission to government agencies and non governmental persons.

### **Benefits of pilot testing**

- Pilot testing help identify and resolve problems with research design, methodology and data collection, thereby reducing errors in larger studies and saving time and resources.
- They allow researchers to refine their research questions and objectives, thereby ensuring their fit with the study's objectives.
- Pilot testing also provides valuable information on practical aspects such as participant recruitment and retention strategies which are essential to the success of the main study.
- They also ensure that the research is ethically sound by allowing researchers to test procedures on a smaller scale and address potential ethical concerns.

### **3.10 Ethical considerations**

Prior to conducting the interviews, initial meetings and phone discussions took place with the potential participants, during which the researcher clarified the nature and objectives of the study. Respondents were informed that their involvement was completely voluntary and that they had the right to withdraw from the study at any point without needing to provide any

justification. Additionally, the prospective participants were assured that the information they provided would be handled with the utmost confidentiality and their identities would remain anonymous. They were also made aware that the data collected would solely be utilized for academic purposes and not for any other reasons.

### **3.11 Summary**

The chapter delineated a systematic approach for collecting data from both primary and secondary sources by detailing the essential procedures. The study utilized various methods, such as interviews, field observations, and secondary data, to generate information pertinent to the research question. The research implemented a purposeful sampling technique. In accordance with established ethical standards, the research was conducted ethically. The methods employed for data analysis are emphasized in the concluding section. This chapter equips the reader for the presentation of results in the subsequent chapter that follows.

## CHAPTER FOUR

### DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

#### 4.0 Introduction

This chapter outlines the key data gathered from the research concerning the nature of Zimbabwe's cybersecurity framework. The data was obtained through fieldwork utilizing semi-structured interviews. The chapter will commence by emphasizing the response rate of the study and subsequently analyze the demographic traits of the respondents.

#### 4.1 Response rate

A total of 25 participants, comprising Information and Communication Officers from the Ministry of Information Technology (ICT) as well as social media bloggers and participants from telecommunication companies were targeted at random. A total of 20 respondents were interviewed for the study. This represented an 80% response rate, which was regarded adequate for informing analysis and drawing conclusions. The outcomes are listed below:

##### 4.1.1: Response rate

<b>Customer group</b>	<b>Targeted population</b>	<b>Number of people interviewed</b>	<b>Response rate</b>
Information and communication Officers.	5	3	60%
Social media bloggers	15	15	100%
Respondents from telecommunication	5	2	40%

companies			
<b>Total</b>	<b>25</b>	<b>20</b>	<b>80%</b>

Table 4.1.1

The response rate shows 80% out of 100%.

## 4.2 Demographic data of respondents

The researcher's initial goal was to identify the biographical information of the sample that was used to gather primary data. The background data on the respondents' age, gender, and educational background were specifically examined and listed in the section that follows.

### 4.2.1. Gender of respondents

According to the survey findings, 55% of the respondents were females whilst 45% were males. These findings are were illustrated below:

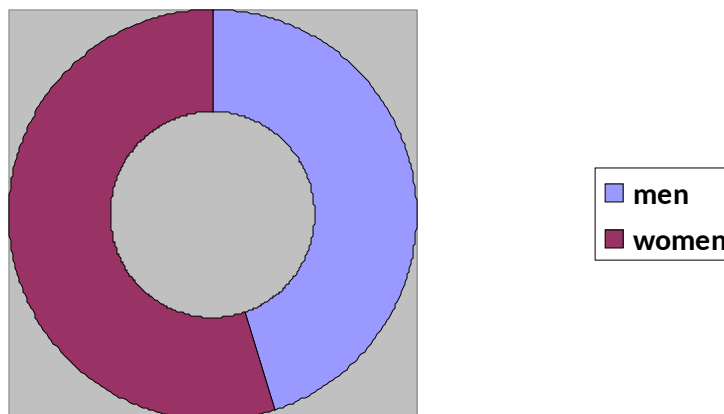


Figure 4.2.1

The majority of the respondents under examination were female, according to the results. This is especially true considering that women typically respond or participate in most spheres higher rate than males. The slight discrepancy between the sexes can be linked to the

female populations being higher. Gender discrepancies raise issues regarding how the two sexes may relate when it comes to participation in surveys.

#### 4.2.2 Age group

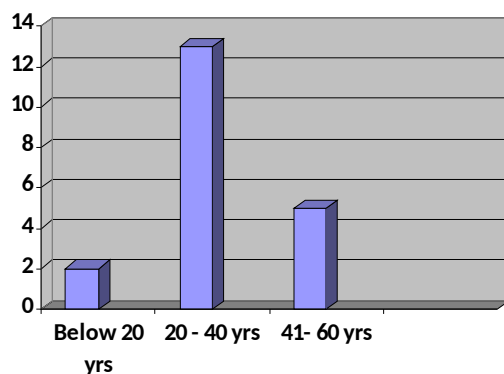


Figure 4.2.2

#### 4.2.3 Level of education

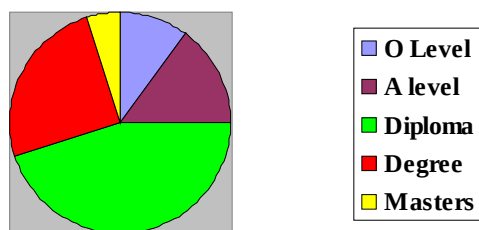


Figure 4.2.3

In accordance with the results, 10% obtained ordinary level education, 15% advanced level, 45% a diploma, 25% an undergraduate degree and 5% masters. As a result, they have the education necessary to comprehend concerns about the knowledge of Zimbabwe's cybersecurity framework. This would lend the credibility to the survey's conclusions by showing that it was completed by participants who could read, understand and interpret the questionnaire on their own. The excellent academic credentials demonstrate that the respondents chosen from the population have knowledge about Zimbabwe's cybersecurity

framework. Therefore, it might be stated that the majority of survey participants were literate enough to respond to the questions.

#### **4.3 The nature of Zimbabwe's cyber security framework.**

The research revealed a multifaceted picture of Zimbabwe's cybersecurity framework, characterized by a combination of existing legislation, policies, and ongoing efforts to strengthen digital security. Interviews with key informants, including Communication Officers from the Ministry of Information Communication Technology (ICT), shed light on the foundational elements of this framework. One Communication Officer emphasized:

*‘Zimbabwe has recognized the growing importance of cybersecurity and has taken steps to establish a legal and regulatory framework. The Computer Crime and Cybercrime Act is a cornerstone, outlining provisions for cybercrime offenses and penalties.’*

This Act serves as a crucial legal instrument in addressing cyber threats and ensuring accountability. Furthermore, the research highlighted the purpose of various state agencies and organizations in contributing to the cybersecurity framework. The Cybersecurity and Data Protection Act, for instance, plays a significant role in coordinating cybersecurity efforts, conducting risk assessments, and issuing advisories on emerging threats. Interviews with representatives from telecommunication companies underscored the collaborative nature of cybersecurity initiatives. One representative stated,

*‘The industry recognizes the shared responsibility in safeguarding cyberspace. We actively engage with government agencies, law enforcement, and cybersecurity experts to share threat intelligence, conduct joint exercises, and implement best practices.’*

This collaborative approach is crucial for addressing the evolving nature of cyber threats and ensuring a coordinated response. However, the research also revealed challenges and gaps in the existing framework. While legislation provides a foundation, its implementation and enforcement can be complex. Concerns were raised regarding the adequacy of resources and capacity within relevant government agencies to effectively monitor and respond to cyber threats. Additionally, the rapid evolution of technology and the emergence of new threats pose ongoing challenges to maintaining a robust and up to date framework. One social media blogger expressed concerns about the speed at which new technologies and vulnerabilities emerge, stating,

*'The framework needs to be agile or quick and adaptable to keep pace with the constantly changing threat.'*

The nature of Zimbabwe's cybersecurity framework is characterized by a combination of existing legislation, ongoing policy development, and collaborative efforts between government, industry, and other stakeholders. While progress has been made, challenges remain in areas such as resource allocation, infrastructure, and adapting to the rapidly evolving threats. The findings align with the observations of scholars who have emphasized the multi-layered nature of cybersecurity frameworks in contemporary societies for example (Whitman & Mattord, 2021). The presence of legislation like the Computer Crime and Cybercrime Act, as highlighted by the Communication Officer, is a crucial step, showing the importance of legal frameworks in establishing a foundation for cybersecurity efforts. Heim (2023) argue that, the way to deal with this plural normative system is to take into account a “rich coherence”, seeking equilibrium with a plural set of beliefs. This aligns with the concept of "legal pluralism" in cybersecurity, where multiple legal instruments and regulatory bodies interact to govern cyberspace.



The involvement of various government agencies, such as the Cybersecurity and Data Protection Authority, mirrors the trend towards multi-stakeholder collaboration in cybersecurity governance as Ciglic and Hering (2021) argued that, the internet continues to be the greatest experiment in human history a global network for connectivity and sharing of information that has been built, maintained and enabled by a wide range of multi-stakeholder partners. The emphasis on collaboration between government, industry, and other stakeholders have impact with the concept of "public-private partnerships" in cybersecurity (Chingoriwo, 2022). The telecommunications company representative's statement emphasizes the shared responsibility where all stakeholders play a crucial role in cybersecurity.

However, the findings also highlight the challenges associated with implementing and maintaining an effective cybersecurity framework. There are concerns regarding resource constraints and capacity building. Also, rapid evolution of technology causes cyber threats as argued by Al-Ghamdi (2021) that, basic threats in cyberspace are foreign threats, internal threats, threats in the supply chain of goods and services, and threats due to insufficient operational capability of local forces. Therefore, the coming in of new technologies causes cyber threats.

#### **4.4 The effectiveness of Zimbabwe's cyber security framework in protecting citizens' personal data and preventing cyber threats.**

The research shows a mixed picture when assessing the effectiveness of Zimbabwe's cybersecurity framework in protecting citizens' personal data and preventing cyber threats. While progress has been made with the establishment of data protection regulations and collaborative efforts between stakeholders, significant challenges remain. The research states that Zimbabwe has taken steps to safeguard personal data through the implementation of Data Protection Act of 2021. Interviewees from the Ministry of Information Technology

(ICT) highlighted the existence of data protection regulations, emphasizing key principles such as data minimization, purpose limitation, and accountability. One Communication Officer stated,

*'We have regulations in place that outline data protection principles such as data minimization, purpose limitation, and accountability. These regulations aim to protect citizens' personal data from unauthorized access, use, and disclosure.'*

However, the effectiveness of these regulations in practice raises questions. Concerns were raised regarding enforcement mechanisms, awareness among citizens and businesses, and the ability to keep intact with the evolving digital technologies. The research revealed varying levels of success in preventing cyber threats. While law enforcement agencies have made efforts to combat cybercrime, challenges persist. One representative from a telecommunications company acknowledged the increasing prevalence of cyber threats, stating,

*'We have seen an increase in cyber threats, including phishing attacks, malware, and ransomware. While we collaborate with law enforcement agencies, the scale of these threats requires a more comprehensive and proactive approach.'*

This highlights the need to update the current framework in response to the evolving threats.

In 2018, over 4,000 cases of cybercrime were handled by Zimbabwean police, and the country lost US \$40 million to cybercrime in 2018 ( Bulawayo24, 2021). Furthermore, the research emphasizes the importance of public awareness in mitigating cyber threats. Interviews with social media bloggers revealed a concerning lack of awareness among some individuals regarding online safety practices and the risks associated with online activities. One social media blogger expressed concern, stating,

*'I often receive suspicious emails and messages, but I don't always know how to identify and respond to them'*

To add on, lack of awareness campaigns can significantly increase the vulnerability of individuals to phishing attacks, malware infections, and other cyber threats. The prevalent forms of cybercrime in Zimbabwe include identity theft, hacking, email phishing, and the use of malware victimization (Reserve Bank of Zimbabwe, 2015). Furthermore, insufficient funding and personnel were consistently cited as significant obstacles by government officials and business people. Inadequate resources hinder effective implementation of cybersecurity measures, investigation of cybercrimes, and the development of robust cybersecurity capabilities. The rapid evolution of technology causes a constant challenge. New technologies and vulnerabilities emerge continuously, requiring the cybersecurity framework to be updated. This necessitates ongoing research, development, and implementation of new security measures to stay ahead of the threats.

Furthermore, the recognition of progress in data protection regulations reflects the growing global emphasis on data privacy and the development of comprehensive data protection frameworks, as observed by Solove (2022). However, the concerns regarding enforcement, awareness, and the dynamic nature of the digital landscape echo the challenges highlighted.

While efforts are in progress to enhance coordination among stakeholders, challenges remain in ensuring coherent information sharing and collaborative responses to cyber threats. Improving communication and information sharing between government agencies, law enforcement, the private sector, and academia is crucial for an effective and coordinated cybersecurity response. The research findings suggest that Zimbabwe's cybersecurity framework has made progress in protecting citizens' personal data and preventing cyber threats. However, significant challenges remain. Addressing these challenges requires a

multi-faceted approach that includes strengthening data protection regulations, enhancing law enforcement capabilities, increasing public awareness, and fostering greater collaboration among stakeholders.

#### **4.5 Gaps in Zimbabwe's cyber security framework that compromise digital rights and freedoms.**

The research identified several gaps in Zimbabwe's cybersecurity framework that have the potential to compromise digital rights and freedoms. The gaps that were mentioned by the respondents includes, lack of comprehensive data protection policies. While some data protection regulations still exist, there are insufficient to adequately safeguard citizens' personal data. This raises concerns about the potential for data breaches, misuse of personal information, and the erosion of privacy rights. One social media blogger expressed concern, stating,

*'I worry about how my data is being used by companies and the government. I don't always understand what information is being collected and how it is being used'*

Concerns were raised regarding the potential for overbroad surveillance powers, which could violate citizens' rights to privacy and freedom of expression. Some interviewees expressed concerns about the potential for surveillance and the lack of adequate safeguards to prevent misuse of surveillance powers. Lack of transparency and access to information regarding cybersecurity policies and practices can hinder public trust and accountability. Citizens may not have sufficient information to understand how their data is being used, how their rights are being protected, and how they can exercise their digital rights. One representative from a telecommunications company emphasized the importance of transparency, stating,

*'It is crucial for citizens to understand how their data is being used and to have confidence in the measures taken to protect their privacy'*

Limited access to technology and digital literacy can hinder individuals' ability to exercise their digital rights and participate fully in the digital economy. Another significant gap identified in the research was a lack of public awareness and education regarding cybersecurity issues and digital rights. Many citizens may not be aware of their rights online, how to protect themselves from cyber threats, and how to exercise their digital rights responsibly. This lack of awareness can contribute to the success of phishing attacks, the spread of misinformation, and the erosion of digital rights.

Addressing these gaps requires a multi-faceted approach that includes strengthening data protection policies, ensuring transparency and accountability, bridging the digital divide, and investing in public awareness and education programs. The identified gaps align with critical concerns raised by scholars in the field of digital rights. The lack of comprehensive data protection legislation, as highlighted by the research, raises the concerns of scholars like Solove (2022), who emphasize the need for robust legal frameworks to protect individual privacy in the digital age. The worries expressed by the social media user about the use of their personal data also raises concerns.

The concerns about overbroad surveillance powers resonate with the work of scholars like Greenleaf (2010), who have analyzed the potential for mass surveillance to incite violence upon fundamental rights such as freedom of expression and association. The emphasis on transparency and accountability aligns with the recommendations of scholars like Lessig (1999), who argue for greater public participation and oversight in the development and implementation of cybersecurity policies.

#### **4.6 Strategies that improve Zimbabwe cyber security framework capacity to protect people's digital rights and freedoms.**

The research identified several key strategies to strengthen Zimbabwe's cybersecurity framework and enhance its ability to protect digital rights and freedoms. These strategies include strengthening existing data protection legislation is crucial. This includes expanding the scope of the policies to cover a wider range of data processing activities, strengthening enforcement mechanisms, and increasing awareness among the public and businesses about their rights and obligations under the law. One Communication Officer from the Ministry of Information Technology (ICT) emphasized the need for,

*'Clearer guidelines and more robust enforcement mechanisms to ensure compliance with data protection regulations'*

Investing in human capital development is essential to build a skilled cybersecurity workforce. This includes training and capacity building programs for government officials, law enforcement agencies, and private sector professionals. One representative from a telecommunications company highlighted the importance of

*'Investing in cybersecurity training and education programs to equip individuals and organizations with the knowledge and skills to identify and respond to cyber threats'*

Raising public awareness about cybersecurity threats and online safety practices is critical. This includes public education campaigns, awareness programs in schools, and the development of user-friendly resources and tools to help citizens understand and mitigate online risks. One social media blogger emphasized the need for,

*'More public education campaigns to teach people about online safety best practices, such as recognizing phishing emails, using strong passwords, and protecting their personal information online'*

Promoting cooperation and the exchange of information between governmental bodies, law enforcement, the private sector, and academia is crucial for an effective and coordinated cybersecurity response. This includes establishing secure channels for information sharing, conducting joint exercises and threat assessments, and promoting the development of public-private partnerships.

Bridging the digital divide is essential to ensure that all citizens have access to the benefits of the digital world and can exercise their digital rights. This includes expanding access to affordable internet connectivity, promoting digital literacy programs, and addressing the digital divide in rural and underserved communities. Enhancing transparency and accountability in cybersecurity practices is crucial to build public trust and confidence. This includes providing clear and accessible information about cybersecurity policies and practices, establishing independent oversight mechanisms, and ensuring that surveillance powers are used responsibly and lawfully. The identified strategies align with key recommendations from cybersecurity experts and scholars. The emphasis on strengthening data protection legislation echoes the calls of scholars like Solove (2022), who advocate for comprehensive and robust data protection frameworks to safeguard individual privacy in the digital age. Therefore, these strategies need to be practiced to ensure a better cybersecurity framework.

The telecommunications company representative's emphasis on training and education programs aligns with the recommendations of scholars who advocate for investing in cybersecurity education and awareness programs to empower individuals and organizations to mitigate cyber risks (Nurse, 2021). The social media user's emphasis on practical skills like recognizing phishing emails and using strong passwords aligns with the need for practical education and awareness campaigns to equip individuals with the knowledge and skills to protect themselves online.

The emphasis on cooperation and the exchange of information resonates with increasing acknowledgment of the significance of multi-stakeholder collaborative efforts in tackling cybersecurity issues (Ciglic & Hering, 2021). Finally, the emphasis on transparency and accountability aligns with the recommendations of scholars who argue for greater public participation and oversight in cybersecurity governance (Frاندell & Feeney, 2022). Therefore, collaboration and ensuring transparency is important in cybersecurity.

#### **4.7 Chapter Summary.**

The chapter has provided an analysis of the research, along with the results and data presentation, which includes the perspectives of the respondents as well as various academic viewpoints. Additionally, the data was presented in accordance with the established objectives.



## **CHAPTER FIVE**

### **SUMMARY, CONCLUSIONS, RECOMMENDATIONS AND AREAS FOR FURTHER RESEARCH**

#### **5.0 Introduction**

This segment offers an overview of the results from the research and also conclusions anchored from study objectives, recommendations and areas for further research arising based on the results of the research.

#### **5.1 Summary of Findings**

The study's findings revealed that Cybersecurity and Data Protection Act is not static as it has challenges in adapting to new evolving threats, hence, its a work in progress. The research also revealed other challenges such as surveillance, lack of awareness campaigns, limited access to information and transparency among others.

Hence, participants recommended ideas that will cover all these challenges for instance, enhancing data protection legislation and enforcement, to develop a comprehensive public awareness campaign, prioritizing resource allocation and capacity building.

#### **5.2 Conclusions**

##### **5.2.1 The nature of Zimbabwe's cyber security framework.**

The research concludes that Zimbabwe's cybersecurity framework is characterized by a foundational legal structure, primarily built upon the Cybersecurity and Data Protection Act. This framework also involves the participation of various government agencies, notably the Cybersecurity and Data Protection Authority, and fosters collaborative efforts with private sector stakeholders, particularly telecommunications companies. However, the framework's nature is not static, as it has challenges related to resource constraints, capacity building, and the need to adapt to the rapidly evolving technological threats. The framework, therefore,

exists as a work in progress, balancing legislative purpose with practical implementation in a resource constrained environment.

### **5.2.2 The effectiveness of Zimbabwe's cyber security framework in protecting citizens' personal data and preventing cyber threats.**

The research concludes that the effectiveness of Zimbabwe's cybersecurity framework is mixed. While data protection regulations exist, their practical enforcement and public awareness of them are limited. Similarly, efforts to prevent cyber threats are ongoing, but hampered by resource constraints and the sheer scale of emerging threats. The lack of public awareness regarding online safety practices further compounds the issue, leaving citizens vulnerable to cyberattacks. Therefore, while the framework provides a foundation, its practical effectiveness in protecting citizens' data and preventing threats is hindered by implementation challenges and the need for greater public engagement.

### **5.2.3 Gaps in Zimbabwe's cyber security framework that compromise digital rights and freedoms.**

The research concludes that significant gaps exist within Zimbabwe's cybersecurity framework that compromise digital rights and freedoms. These gaps include lack of comprehensive data protection legislation, concerns regarding overbroad surveillance powers, limited access to information and transparency, lack of public awareness and education regarding cybersecurity issues and digital rights. These gaps point to a need for a more human rights centered approach to cybersecurity policy development and implementation, ensuring that digital innovation does not come at the expense of fundamental rights and freedoms.

#### **5.2.4 Strategies that improve Zimbabwe cyber security framework capacity to protect people's digital rights and freedoms.**

The research concludes that strengthening Zimbabwe's cybersecurity framework requires a multifaceted approach. Proposed strategies include enhancing data protection legislation, investing in cybersecurity capacity building, enhancing public awareness and education, promoting collaboration and information sharing, addressing the digital divide, and ensuring transparency and accountability. These strategies aim to address the identified gaps and challenges, fostering a more robust and resilient cybersecurity framework that effectively protects digital rights and freedoms while enabling digital innovation. The successful implementation of these strategies would require sustained commitment from the government, private sector, and civil society, ensuring a more secure and rights-respecting digital environment for all citizens.

### **5.3 Recommendations**

#### **➤ Prioritize resource allocation and capacity building**

A significant challenge for many developing nations is the allocation of sufficient resources to cybersecurity initiatives. Therefore, the Zimbabwean government should prioritize increasing budgetary allocations for cybersecurity infrastructure, technology, and personnel. This includes investing in training programs for law enforcement, judiciary officials, and cybersecurity professionals to enhance their skills in investigating and prosecuting cybercrimes, as well as developing and maintaining robust cybersecurity systems. Furthermore, partnerships with international organizations and developed nations should take place to leverage technical expertise and access funding opportunities for capacity building in this critical area.

#### **➤ Develop a comprehensive public awareness campaign**

Research often reveals a gap in public awareness regarding online safety and digital rights. Public awareness campaign is crucial to educate citizens about potential cyber threats, data protection best practices, and their digital rights. It is essential to employ a range of channels, such as social media, traditional media, educational institutions, and community centers, to reach all citizens. The message should reach to different demographics, emphasizing practical tips for online safety, such as recognizing phishing scams, using strong passwords, and protecting personal information. Empowering citizens with knowledge will significantly enhance the overall cybersecurity posture of the nation.

➤ **Enhance data protection legislation and enforcement**

Robust data protection legislation is fundamental to safeguarding citizens' personal information. The existing data protection regulations should be reviewed and strengthened to align with international best practices. Also, enforcement mechanisms must be strengthened to ensure compliance. This requires empowering the relevant regulatory bodies with the necessary authority, resources, and expertise to investigate data breaches, impose penalties, and provide guidance to organizations on data protection best practices.

#### **5.4 Areas for further research**

Subsequent investigations could explore the specific the influence of new technologies, for instance, artificial intelligence and blockchain, on cybersecurity and digital rights within the Zimbabwean context. A comparative analysis with other developing nations facing similar challenges could offer valuable lessons and best practices. Further research could also look into the efficacy of particular cybersecurity training initiatives and public awareness efforts, assessing their impact on citizen behavior and understanding.

## REFERENCES

African union. (2014). *African union convention on cybersecurity and personal data*

African union.

Alder, A. (2020). blockchain information services, 276-7 ByteDance, 216 Cambridge

Analytica, 186 Canada cybersecurity breaches, 107. *regulation*, 113, 276-7.

Al-Ghamdi, M. I. (2021). Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings*, 10.

Ankumah, E. A. (2023). *The African Commission on Human and Peoples' Rights: Practices and Procedures* (Vol. 16). BRILL.

Assembly, U. G. (2015). UN General Assembly. *Resolution Adopted by the General Assembly on 25 September 2015. A/RES/70/1, Transforming our world: the 2030 Agenda for Sustainable Development*.

Bárd, P., Bardutzky, S., Baumbach, T., Belov, M., Besselink, L., Biernat, S., ... & Chronowski, N. (2019). Anneli Albi Law School, University of Kent, Canterbury, UK Marje Allikmets Supreme Court of Estonia, Tartu, Estonia Pierre-Vincent Astresses Sorbonne Law School, University Paris 1 (Panthéon-Sorbonne), Paris, France. *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law: National Reports*.

Bhatia, V. (2018). *Research methodology: Techniques and tools*. SAGE Publications Limited.

Biti, O. (2020). Narratives about work in Croatian celebrity culture. *Traditiones*, 49(3), 163-184.

- Boru, G. H. (2018). A handbook of research methods and writing for business & education students. African Books Collective.
- Brooks, J., Reed, D. M. & Savage, B. (2016). Taking off with a pilot: The importance of testing research instruments. *ECRM2016-Proceedings of the 15<sup>th</sup> European Conference on Research Methodology for Business Management: ECRM2016. Academic Conference and publishing limited, 51-59.*
- Calder, A. (2018). NIST Cybersecurity Framework: A pocket guide. *IT Governance Publishing Ltd.*
- Chika, A. (2018). Fear of communicating fear versus fear of terrorism: a human rights violation or a sign of our time? *International journal of speech language pathology 20 (1), 26-33.* Cohen, S. A. (2019). Cybersecurity for critical infrastructure: addressing threats and vulnerabilities in Canada.
- Chingoriwo, T. (2022). Cybersecurity challenges and needs in the context of digital development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies, 3(2), 77-104.*
- Ciglic, K., & Hering, J. (2021). A multi-stakeholder foundation for peace in cyberspace. *Journal of Cyber Policy, 6(3), 360-374.*
- Crabbe, S., Roß, K., Köpke, C., Faist, K., Medina, E. V., Siebold, U., ... & Costa, E. (2022). SAFETY4RAILS Information System platform demonstration at Madrid Metro simulation exercise. In *Proceedings of the 32nd European safety and reliability conference, copyright.*
- Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2012). Qualitative research & evaluation methods. SAGE Publications Limited.

- Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed method approaches*. Thousand Oaks, CA: SAGE.
- Davies, C. & Fisher, M. (2018). Understanding research paradigms. *Journal of the Australasian Rehabilitation Nurses Association* 21 (3), 21-25.
- DeNardis, L. (2016). One internet: An evidentiary basis for policy making on internet universality and fragmentation.
- Dube, H. (2024). DIGITAL VULNERABILITIES AND THE. *Data privacy law in Africa:Emerging perspectives*, 159.
- Etikan, I. & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal* 5 (6), 00149.
- Frاندell, A., & Feeney, M. (2022). Cybersecurity threats in local government: A sociotechnical perspective. *The American Review of Public Administration*, 52(8), 558-572.
- Floridi, L., Cath, C., & Taddeo, M. (2019). Digital ethics: its nature and scope. *The 2018 yearbook of the digital ethics lab*, 9-17.
- Gambanga, N. (2016). *Here's the Zimbabwean government's warning against social media abuse*. TechZim, (Accessed 1 September 2022).
- Goucher, W. F. (2018). *Investigation of the shoulder surfing risk in relation to mobile working* (Doctoral dissertation, University of Glasgow).
- Government of Zimbabwe. (2020). *Cybersecurity and Data Protection Bill*. Government Printer.
- Group of 20 (G20) Digital Economy Ministers (2020). Extraordinary G20 Digital Economy Ministerial Meeting: COVID-19 Response Statement. Virtual Meeting,

30 April. Available at: <http://www.g20.utoronto.ca/2020/2020-g20-digital-0430.html> (accessed 15 July 2020)

Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg, I., de Beer, J., Oguamanam, C., ... & Van Wiele, B. The AfricAn JournAl of informATion And communicATion (AJIC).

Heim, T. N. (2023). Global governance and regulation of cybersecurity: Towards coherence or fragmentation?

Horne, C. L. (2021). Internet governance in the “post-truth era”: Analyzing key topics in “fake news” discussions at IGF. *Telecommunications Policy*, 45(6), 102150.

Howard, R. (2023). *Cybersecurity First Principles: A Reboot of Strategy and Tactics*. John Wiley & Sons.

ICB, Z. (2021). Government of Zimbabwe.

Jang, Y. (2014). *A study on the national cybercrime strategy: Toward the improvement of Korean cyber policing policies applying a logic model* (Unpublished doctoral thesis). Korea University, Seoul.

Jenerette, G. D., Wu, W., Goldsmith, S., Marussich, W. A., & Roach, W. J. (2006). Contrasting water footprints of cities in China and the United States. *Ecological economics*, 57(3), 346-358.

Kabanda, G. (2018). A Cybersecurity culture framework and its impact on Zimbabwean organizations. *Asian Journal of Management, Engineering and Computer Science*, 3(4), 17-34.

Karekwaivanane, G., & Msonza, N. (2021). Zimbabwe digital rights landscape report. In T. Roberts (Ed.), *Digital rights in closing civic space: Lessons from ten African*



countries. *Institute of Development Studies*. <https://doi.org/10.19088/IDS.2021.003>.

Khalil, L. (2020). Digital authoritarianism, China and COVID.

Kombo, D. K. and Tromp, D. (2006). Proposal and thesis writing: An introduction. Makuyu: Pauline's Publications.

Kurebwa, J. (2021). Understanding cyber security: *A review of the cyber security and data protection bill in Zimbabwe. International Journal of systems and service-oriented engineering, Volume 11, Issue 1.*

Lyon, A. (2015). *Deliberative acts: Democracy, rhetoric, and rights*. Penn State University Press.

Mabika, A. H., & London, L. (2007). Implications of the GATS and TRIPS agreements for the Right to Health in Malawi. *EQUINET: Harare*.

Mare, A. (2020). Internet shutdowns in africa| state ordered internet shutdowns and digital authoritarianism in Zimbabwe. *International Journal of Communication*, 14, 20.

Marx, G. T. (2016). Windows into the soul: Surveillance and society in an age of high technology. University of Chicago Press.

Middleton, F. (2024). Reliability vs. Validity in Research. *Difference, Types and Examples*.

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, 27(1), 64-77. <https://doi.org/10.46743/2160-3715/2022.5044>.

- Moyo, J. (2021). Be Wary of rising cybercrimes. The Sunday Mail.  
<https://www.aa.com.tr/en/africa/zimbabwean-regime-shifts-oppression-to-social-media/2146273>. Accessed 3 September 2022.
- Moyo, T. (2020). Sexuality as a tool to gain political power: an introspection of Zimbabwean elections of 2013. *African Identities*, 18(4), 421-434.
- Mpofu, S., & Mare, A. (2020). #ThisFlag: Social media and cyber-protests in Zimbabwe. In M. Ndlela & W. Mano (Eds.), *Social media and elections in Africa: Challenges and opportunities* (2, pp. 153–173). Palgrave Macmillan.
- Mukherjee, S.P. (2019). A Guide to Research Methodology: An Overview of Research Problems, Tasks and Methods. CRC Press.
- Munoriyarwa, A. (2021). The growth of military-driven surveillance in post-2000 Zimbabwe. *The Media Policy and Democracy Project May 2021*.
- Munoriyarwa, A., & Chiumbu, S. H. (2019). Big Brother is Watching: Surveillance Regulation and its Effects on Journalistic Practices in Zimbabwe. *African Journalism Studies*, 40(3), 26-41.
- Ncube, Z. M. (2024). Emerging Threats in Cybersecurity: Risk and Vulnerability Management. *Journal of Innovative Technologies*, 7(1).
- Ndlovu, S. (2021). Provision of assistive technology for students with disabilities in South African higher education. *International Journal of Environmental Research and Public Health*, 18(8), 3892.
- Nurse, J. R.C. (2021). Encyclopedia of Cryptography, Security and Privacy, University of Kent.

- Nyamunda, J. (2021). Mandatory Business-To-Government Data Sharing: Exploring data protection through International Investment Law.
- Nyoni, P., Velempini, M., & Mavetera, N. (2020). Emerging internet technologies and the regulation of user privacy. *The African Journal of Information Systems*, 13(1), 1.
- Peters, J. G. (2024). *A life cycle perspective on business models in the smart home device industry*. (Master's thesis, University of Twente).
- Peters II, M. T. (2023). Fixing American Cybersecurity.
- Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: *The Russian and Chinese digital models*. [https://www.brookings.edu/wpcontent/uploads/2019/08/FP\\_20190827\\_authoritarianism\\_polyakova\\_meserole.pdf](https://www.brookings.edu/wpcontent/uploads/2019/08/FP_20190827_authoritarianism_polyakova_meserole.pdf) (Accessed 20 April 2022).
- POTRAZ. (2013). *Circular on bulk SMS*. POTRAZ (accessed 1 September 2022).
- POTRAZ. (2019). Abridged postal and telecommunications sector performance report: *First quarter 2019*. [https://t3n9sm.c2.acecdn.net/wp-content/uploads/2019/07/A\\_bridged-Sector\\_Performance\\_report-1st-Quarter-2019\\_final-hmed.pdf](https://t3n9sm.c2.acecdn.net/wp-content/uploads/2019/07/A_bridged-Sector_Performance_report-1st-Quarter-2019_final-hmed.pdf).
- Ridder, H. G. (2017). The theory contribution of case study research designs. *Business research* 10, 281-305.
- Roberts, T., & Ali, A. M. (2021). Opening and closing online civic space in Africa: An introduction to the ten digital rights landscape reports. *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*.

- Schmidt, V. A. (2020). Theorizing institutional change and governance in European responses to the Covid-19 pandemic. *Journal of European Integration*, 42(8), 1177-1193.
- Solove, D. J. (2022). The limitations of privacy rights. *Notre Dame L. Rev.*, 98, 975.
- Taye, B. (2020). Targeted, Cut Off and Left in the Dark: The #KeepItOn Report on internet shutdowns in 2019, Access Now (accessed 26 January 2021).
- Truscott, J. (2023). What about validity? Thoughts on the state of research on written corrective feedback. *Feedback in Second Language* 1, 33-53.
- Turianskyi, K. (2018). Balancing cyber security and internet freedom in Africa. Johannesburg, South Africa: South African Institute of International Affairs.
- Union, A. (2020). The Digital Transformation Strategy for Africa (2020-30).
- Vassilakos, A., & Martin, R. (2023). Understanding the Challenge of Cybersecurity in Africa: A Holistic Analysis of Southern African Development Community (SADC) and Foundation for Future Research. *HOLISTICA–Journal of Business and Public Administration*, 14(1), 162-172.
- Whitman, M. E., CISM, C., & Mattord, H. J. (2021). A Model Curriculum for Programs of Study in Information Security/Cybersecurity March 2021.
- Wiklund, K. (2022). The States as Guardian: Toeing the Line Between Defender and Oppressor of Rights-An Examination of the Limits to Covert Surveillance from a Democratic and European Human Rights Approach.
- Williams B.T. (2014): The joint force commander's guide to cyberspace operations. *Joint Force Quarterly*, 73(2): 12–19.

- Wilson, A., & Tewdwr-Jones, M. (2021). *Digital participatory planning: Citizen engagement democracy, and design*. Routledge.
- Yayboke, E., & Brannen, S. (2020). Promote and build: *A strategic approach to digital authoritarianism*. CSIS Briefs. <https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism>.
- Zetter, K. (2020). Fixing Democracy: The Election Security Crisis and Solutions for Mending It (Fall 2020).
- Zhou, F., & Huang, J. (2024). Cybersecurity data breaches and internal control. *International Review of Financial Analysis*, 93, 103174.
- Zimpricecheck. (2024). Zimbabwe's New Cyber and Data Protection Law: What You Need to Know.

## **ANNEXURE 1: Interview guide**

My name is Tinotenda Sabamba a student at Bindura University of Science Education. I am undertaking a research study titled “An assessment of Zimbabwe’s cybersecurity framework: implications for digital rights and freedoms” in partial fulfilment of the requirement of a BSc Hons Degree in Peace and Governance. I am kindly requesting you to participate in the research, your participation will be greatly appreciated. The study is purely for educational purposes and information will be treated with the utmost confidentiality. You are also assured that your responses will be treated with anonymity and that users of the final research report will not be able to trace the responses to you, your family or your organisation. To help uphold anonymity, you are encouraged not to state your name or any information that may disclose your personal information. Please note that participation in this study is voluntary.

### **Demographic Data**

#### **(a) Gender**

*Male*

☐

*Female*

☐

#### **(b) Age group**

*Below 20 yrs*

☐

*20-40 yrs*

☐

*41-60 yrs*

☐

*61 and above*

☐

#### **(c) Highest Qualification**

*Diploma level* ☐

*Degree level* ☐



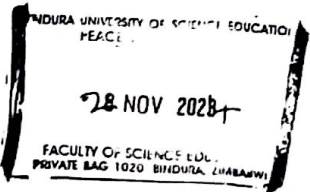
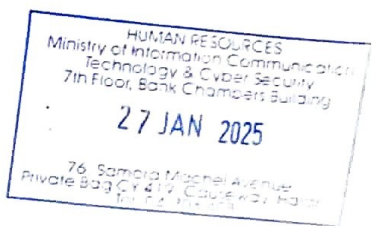
*Masters Level* ☐

#### **(e) Work Experience**

5 years & below ☐      6- 9 years ☐      10 years & above ☐

1. What is the current state of cybersecurity in Zimbabwe?
2. How would you describe the current cybersecurity framework in Zimbabwe?
3. How effectively does the current framework protect citizens' personal data?
4. In your experience, how well does the framework prevent cyber threats?
5. What are the biggest challenges or gaps in the current cybersecurity framework?
6. How does the current framework impact digital rights and freedoms?
7. What specific improvements or changes would you suggest to strengthen the cybersecurity framework?
8. How can we better protect digital rights and freedoms within the context of cybersecurity in Zimbabwe?

## ANNEXURE 2: Permission letter

<h1 style="text-align: center;">BINDURA UNIVERSITY OF SCIENCE EDUCATION</h1>	
	<h2 style="text-align: center;">FACULTY OF SOCIAL SCIENCES AND HUMANITIES</h2>
<h3 style="text-align: center;">DEPARTMENT OF PEACE AND GOVERNANCE</h3>	
<p>28 November 2024</p>	
<p>TO WHOM IT MAY CONCERN</p>	
<p><b>RE: REQUEST TO UNDERTAKE RESEARCH IN YOUR ORGANISATION</b></p>	
<p>This serves to introduce the bearer, <u>Tinashe Sabamba</u>, Student Registration Number <u>B2113756</u>, who is a <b>HBSC PEACE AND GOVERNANCE</b> student at Bindura University of Science Education and is carrying out a research project in your area/institution.</p>	
<p>May you please assist the student to access data relevant to the study, and where possible, conduct interviews as part of a data collection process.</p>	
<p>Yours respectfully</p>  <p><b>J. KUREBWA (DR)</b> <b>Acting Chairperson</b></p>	
	



## Final dissertation

## ORIGINALITY REPORT

8%

SIMILARITY INDEX

6%

INTERNET SOURCES

4%

PUBLICATIONS

2%

STUDENT PAPERS

## PRIMARY SOURCES

1

Karwan Mustafa Kareem. "The Intelligence Technology and Big Eye Secrets: Navigating the Complex World of Cybersecurity and Espionage", PsyArXiv, 2024

Publication

1%

2

Edwin Yingi, Everisto Benyera. "The Future of Democracy in the Digital Era: Internet Shutdowns, Cyber Laws and Online Surveillance in Zimbabwe", Alternatives: Global, Local, Political, 2024

Publication

&lt;1%

3

dspace.unza.zm

Internet Source

&lt;1%

4

listens.online

Internet Source

&lt;1%

5

Kaja Ciglic, John Hering. "A multi-stakeholder foundation for peace in cyberspace", Journal of Cyber Policy, 2022

Publication

&lt;1%

6

pmc.ncbi.nlm.nih.gov

Internet Source

&lt;1%

7

Submitted to Graduate School of Human Sciences (English)

Student Paper

&lt;1%

8

ir.buse.ac.zw

Internet Source

&lt;1%

www.scribd.com

