



UNIVERSITY of LUSAKA
Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

**A CRITICAL ANALYSIS OF THE CYBER SECURITY ACT AND THE CYBER
CRIMES ACT OF ZAMBIA: EXAMINING THEIR APPROPRIATENESS IN
UPHOLDING CONSTITUTIONAL RIGHTS.**

By:

NTAZANA YAMBALA KANCHULE

LLB20120299

**AN OBLIGATORY ESSAY SUBMITTED TO THE UNIVERSITY OF LUSAKA IN
PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE
BACHELOR OF LAWS (LLB) DEGREE.**

2025

DECLARATION

I declare that this dissertation entitled, **A CRITICAL ANALYSIS OF THE CYBER SECURITY ACT AND THE CYBER CRIMES ACT OF ZAMBIA: EXAMINING THEIR APPROPRIATENESS IN UPHOLDING CONSTITUTIONAL RIGHTS.**

which is hereby submitted in partial fulfilment of the requirement for the award of a Bachelor's Degree at the University of Lusaka is my own original work and it has not been previously submitted for the award of a degree at this university or any other tertiary institution. I understand what plagiarism entails and I'm aware of the University's policy in this regard. Thus, where other people's work is cited, I have duly acknowledged. The errors or omissions in this work are solely mine.

NTAZANA YAMBALA KANCHULE



.....
2025

RECOMMENDATION

I **THOMAS MALAMA** recommend that this dissertation prepared under my supervision by **NTAZANA YAMBALA KANCHULE, LLB20120299**, entitled **A CRITICAL ANALYSIS OF THE CYBER SECURITY ACT AND THE CYBER CRIMES ACT OF ZAMBIA: EXAMINING THEIR APPROPRIATENESS IN UPHOLDING CONSTITUTIONAL RIGHTS** be accepted for examination. I have checked it carefully and I'm satisfied that it fulfils the requirement pertaining to the format laid down in the regulations governing directed research.

TK. malama

.....
THOMAS K. MALAMA

21st November 2025

ACKNOWLEDGEMENTS

Firstly, I thank Jehovah God for his grace throughout this journey. Indeed, his mercies have been new every single day of this journey. Gratitude is extended to my supervisor Mr Thomas Malama for the guidance, insights and suggestions offered towards the completion and success of this research, I literally gave up but for this man, his passion and sacrifices kept me going. Blessed man. Special mention goes to my wife, Rachel for the constant support and motivation to strive on. To my beloved children, Niza, Walusungu and Kuzipa, you have been the reason for all my energy and strength to do this. To my colleagues and classmates who have shown that the Bible is right when it says there is a friend who sticks closer than a brother I celebrate you. May I thank the University of Lusaka for the opportunity to pursue my degree and the knowledge that has been imparted in me throughout the course of my study.

DEDICATION

This paper is dedicated to Rachel, Niza, Walu and Ms. Kuku for always believing in me. Thank you for your smiles of assurance, love, unwavering support, and sacrifice of time and financial resources. It has kept me striving for excellence and better even when I was in doubt.

TABLE OF CONTENTS

DECLARATION.....	ii
RECOMMENDATION	iii
ACKNOWLEDGEMENTS.....	iv
DEDICATION.....	v
ABSTRACT	ix
CHAPTER ONE	1
INTRODUCTION	1
1.0 INTRODUCTION	1
1.1 BACKGROUND OF THE PROBLEM.....	3
1.2 STATEMENT OF THE PROBLEM	5
1.3 RESEARCH OBJECTIVES	6
1.5 SIGNIFICANCE OF THE STUDY	7
1.6 SCOPE OF THE STUDY	7
1.7 DEFINITION OF KEY TERMS AND ACRONYMS	7
1.8 LITERATURE REVIEW	8
1.9 RESEARCH METHODOLOGY	13
1.10 RESEARCH OUTLINE	15
1.12 TIMETABLE AND INTENDED TIMELINE.....	16
CHAPTER TWO.....	17
EXPLORING THE CONCEPTS OF CYBER-CRIME, CYBER SECURITY AND CONSTITUTIONAL RIGHTS.....	17
2.0 INTRODUCTION	17
2.1 DEFINITIONS OF CYBER-CRIME AND CYBER SECURITY.....	17
2.2 THE RATIONALE BEHIND CYBER-CRIME AND CYBER SECURITY.....	19
2.3 CONSTITUTIONAL RIGHTS ON CYBER-CRIME AND CYBER SECURITY	21

2.4 CONCLUSION	25
CHAPTER THREE.....	27
EXPLORING THE LEGAL FRAMEWORK GOVERNING CYBER-CRIME, CYBER SECURITY AND CONSTITUTIONAL RIGHTS IN ZAMBIA.....	27
3.0 INTRODUCTION	27
3.1.1 THE CONSTITUTION.....	28
3.1.2 CYBER SECURITY ACT, NO. 3 OF 2025.....	31
3.1.3 CYBER CRIMES ACT, NO. 4 OF 2025	33
3.2 CONCLUSION.....	36
CHAPTER FOUR.....	37
CRITICAL ANALYSIS OF THE APPROPRIATENESS OF THE CYBER SECURITY ACT AND CYBER CRIMES ACT IN UPHOLDING CONSTITUTIONAL RIGHTS: LESSONS FROM INTERNATIONAL BEST PRACTICE	37
4.0 INTRODUCTION	37
4.1 GENERAL OVERVIEW OF GOALS OF THE CYBER SECURITY ACT 2025 AND CYBER CRIMES ACT 2025 AND GENERAL SHORTCOMINGS RAISED BY CRITICS.....	38
4.1.1 The Cyber Crimes Act.....	38
4.1.2 Cyber Security Act.....	38
4.2 KEY SPECIFIC CONSTITUTIONAL RISKS AND CRITIQUE	39
4.3 SPECIFIC CRITIQUE OF FREEDOM OF EXPRESSION – RELATED PROVISIONS.....	43
4.4 INSTITUTIONAL DESIGN: INDEPENDENCE OF THE CYBER SECURITY AGENCY.....	45
4.5 INTERNATIONAL AND REGIONAL BEST PRACTICE LESSONS	47
4.6 CONCLUSION	48
CHAPTER FIVE	50
CONCLUSIONS AND RECOMMENDATIONS	50

5.0 INTRODUCTION 50

5.1 SUMMARY OF CHAPTERS..... 50

5.2 RECOMMENDATIONS..... 54

ABSTRACT

The purpose of this research was to critically analyse the Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No. 4 of 2025, with a focus on identifying the legal and institutional gaps that limit Zambia's ability to address emerging digital threats while upholding constitutional rights. The study examined the evolving nature of cyber threats in Zambia, assessed the adequacy of the statutory and institutional frameworks governing cybersecurity and cybercrime, evaluated the constitutional implications of the 2025 Acts, and proposed reforms to establish a clearer, more accountable, and rights-compliant cyber governance regime.

Chapter One introduced the research problem, outlined the significance and scope of the study, reviewed relevant literature, and presented the methodological and ethical framework guiding the inquiry. Chapter Two explored the conceptual and constitutional foundations of cybercrime and cybersecurity. It demonstrated that rising internet penetration, expanding digital participation, and sophisticated cyberattacks have increased Zambia's exposure to cyber risks. The chapter highlighted incidents such as the Golden Top scam, the NAPSA data breach, and the compromise of the Bank of Zambia's social media accounts as evidence of the growing complexity of digital threats. It further showed that while cybersecurity is essential for protecting digital infrastructure, it must operate within the constitutional safeguards for privacy, fair trial, and freedom of expression under Articles 17, 18, and 20. The analysis revealed that Zambia's cyber governance is shaped by both escalating digital vulnerabilities and the need to uphold fundamental rights.

Chapter Three analysed the statutory and constitutional framework governing cybercrimes and cybersecurity. It demonstrated that the Cyber Security Act introduced institutional reforms for protecting critical information infrastructure and regulating cybersecurity service providers, while the Cyber Crimes Act modernised criminal law by defining and penalising a broad range of digital offences. However, the chapter showed that the effectiveness of these reforms depends on constitutional conformity, judicial oversight, clarity of definitions, and enforceability.

Chapter Four critically assessed whether the 2025 Acts met their intended objectives while remaining consistent with constitutional and regional human-rights standards. The analysis revealed significant risks arising from vague definitions, speech-related offences, broad surveillance powers, and the limited independence of the Cyber Security Agency. These weaknesses were shown to undermine legality, accountability, and the protection of privacy and expression, diverging from best practices under African and international norms.

The study concludes that although Zambia has made substantial progress in constructing a cyber regulatory framework, the Acts contain constitutional, institutional, and procedural gaps that require reform. The research recommends narrowing vague offences, strengthening judicial and parliamentary oversight, enhancing the independence of the Cyber Security Agency, incorporating public-interest protections, refining statutory definitions, and expanding stakeholder participation. Implementing these reforms would help ensure a balanced, transparent, and constitutionally grounded approach to cybersecurity in the digital age.

CHAPTER ONE

INTRODUCTION

1.0 INTRODUCTION

The concept of cybercrime, which was long limited to the technical sphere of computer specialists, has recently moved to the front lines of legal, political, and scholarly discourse. As digital technologies have grown increasingly important in governance, commerce, and social interaction, their abuse for criminal purposes has emerged as one of the twenty-first century's defining concerns.¹ Cybercrime is the current face of multinational and organized crime: invisible, international, and extremely disruptive. It goes beyond conventional criminal activities to include sophisticated digital crimes including hacking, phishing, identity theft, data manipulation, and online financial fraud.

Earliest discussions concerning computer crime in the 1970s and 1980s focused mostly on insider misuse of mainframe systems, which was frequently disregarded as a violation of business policy rather than criminal behaviour. However, as the internet evolved and information and communications technology (ICT) has integrated into every area of modern life, the scope and character of these offences has shifted. The growing interconnectedness of digital networks has made civilizations more efficient, but also more vulnerable. By the early 2000s, international instruments such as the Budapest Convention on Cybercrime recognized the critical need for harmonised legal frameworks, establishing regulations for criminalizing and investigating computer-related offenses.²

Cybercrime has increased tremendously throughout Africa, corresponding with rising digitalization. According to the INTERPOL Africa Cyberthreat Assessment (2025) report, cyber-enabled offences currently make up more than 30 percent of all reported crimes in Western and Eastern Africa.³ The most common types are ransomware, corporate email

¹ G Sarkar and S K Shukla, 'Behavioural analysis of cybercrime: Paving the way for effective policing strategies' (2023) *Journal of Economic Criminology* <https://www.sciencedirect.com/science/article/pii/S2949791423000349> accessed 13 November 2025.

² *ibid*

³ INTERPOL, *Africa Cyberthreat Assessment Report 2025* (4th edn, June 2025) https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf accessed 13 November 2025

compromise (BEC), phishing, and online sextortion. These occurrences are not isolated, but rather part of a regional trend characterized by rising complexity among criminal networks and insufficient capacity of law enforcement organizations to respond.⁴

Zambia's digital landscape has grown substantially during the last decade. Internet penetration, e-commerce, mobile money, and digital governance have all opened up new avenues for economic development and public service delivery. However, these innovations have exposed individuals and institutions to substantial cyber dangers. Recent events, like a high-profile fraud syndicate involving 13,000 Sim Cards uncovered in Zambia, leading to the arrest of 77 people, including 22 Chinese nationals⁵ demonstrates the scope and complexity of the problem. Recognizing the significance of these developments, the Zambian government passed two new statutes in April 2025: the Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No. 4 of 2025, which repealed previously combined 2021 legislation.

This legislation aims to modernize the country's cyber governance structure, criminalize digital offences, enhance investigative powers, and establish a dedicated agency, the Zambia Cyber Security Agency (ZCSA).⁶ However, these measures have not been without criticism. Legal scholars and civil-society organisations have expressed concerns that some aspects of the new Acts are excessively broad, allowing vast powers of surveillance and interception with little or no judicial oversight⁷. Furthermore, ongoing institutional issues, such as overlapping mandates among the Drug enforcement commission, Anti-Corruption Commission and the Zambia Police Service's Cybercrime Unit, may impede efficient coordination and enforcement.

The Zambian experience exemplifies a larger issue - potential conflict between national security on the one hand and digital rights on the other: How to confront cyber threats

⁴ *ibid*

⁵ BBC, Zambia Uncovers 'Sophisticated' Chinese Cybercrime Syndicate <https://www.bbc.co.uk/news/world-africa-68777137> Accessed 16th November 2025

⁶ International Center for Not-for-Profit Law (ICNL), 'Five Things to Know: Zambia's Cyber Security Act 2025' (ICNL, April 2025) <https://www.icnl.org/wp-content/uploads/Zambia-Five-Things-Cyber-Security-Act-2025-final.pdf> Accessed 13 November 2025

⁷ Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> Accessed 13 November 2025.

without jeopardizing constitutional freedoms including Freedom of Expression, Right to Privacy and Right to access, use, create, and publish digital media, as well as to use computers and networks. As technology advances, this balance becomes more delicate leading to the need to conduct a critical analysis of the adequacy and appropriateness of Zambia's 2025 cyber legislation.

This study aims to examine the Cyber Security Act 2025 and the Cyber Crimes Act 2025, with a focus on their substantive and procedural provisions, institutional arrangements, and compliance with best practice drawn from international norms such as the Budapest Convention and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The purpose of this analysis is to identify legal and institutional weaknesses that may weaken Zambia's cybercrime regime's effectiveness, as well as to recommend improvements that promote a safe, responsible, and rights-based digital governance framework.

1.1 BACKGROUND OF THE PROBLEM

Zambia's digital landscape has developed significantly in recent years, offering both new opportunities and sophisticated cyber threats. Across Africa, cybercrime currently accounts for a significant share of criminal activity: according to INTERPOL's 2025 African Cyberthreat Assessment, cyber-enabled offenses account for around 30% of all reported crimes in Western and Eastern Africa.⁸ The most commonly reported threats include online scams (particularly phishing), ransomware, corporate email compromise (BEC), and digital sextortion. Indeed, ransomware attacks increased in 2024, with South Africa and Egypt alone reporting over 17,000 detections, and similar fraud schemes have extended regionally⁹. Zambia-specific data are limited, but the country has previously witnessed high-profile cyber-enabled fraud. In one case, 22 foreign people were arrested for running an international "SIM swap" scheme utilizing over 13,000 Zambian SIM cards. cards.

⁸ Interpol, 'New Interpol Report Warns of Sharp Rise in Cybercrime in Africa' (23 June 2025) <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-African-cybercrime> accessed 13 November 2025.

⁹ *ibid*

In response to increased digital vulnerability, Zambia's Parliament passed two new laws in April 2025: the Cyber Security Act and the Cyber Crimes Act, 2025¹⁰. These Acts repealed the previous 2021 legislation and are aimed at improving Zambia's cyber defences by criminalizing offenses (such as unauthorized access, data interference, and cyber extortion) and empowering institutions to investigate and combat cybercrime. However, observers have already raised significant concerns. Civil society organizations and technology policy experts point out that in both 2025 Acts the scope of what constitutes the term "law enforcement officer" may risk allowing disproportionate surveillance capabilities with insufficient oversight¹¹. Critics also point to a lack of accountability: the Cyber Security Act creates a Zambia Cyber Security Agency under presidential administration and provides for the Central Monitoring Centre – the two with broad interception powers, but fails to provide adequately robust judicial oversight.¹² These shortcomings should also be seen against a backdrop of inadequate capacity: there are a number of law enforcement authorities including the Drug Enforcement Commission, Anti-Corruption Commission and the Zambia Police Cyber Unit, with broad enforcement powers and inadequate resources. The number of law enforcement agencies may potentially foster as a lack of coordination.¹³

In short, Zambia faces a critical contradiction between the necessity for strong cyber defences and the safeguarding of constitutional rights. As technology and cybercrime change, it is critical to evaluate whether the new legal framework adequately confronts dangers while protecting human rights. As a result, this paper conducts a critical analysis of the Cyber Security Act of 2025 and the Cyber Crimes Act of 2025, identifying legal and institutional weaknesses in tackling increasing digital threats.

¹⁰ Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 13 November 2025

¹¹ *ibid*

¹² *ibid*

¹³ INTERPOL, 'New INTERPOL report warns of sharp rise in cybercrime in Africa' (23 June 2025) <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-African-cybercrime> accessed 13 November 2025.

1.2 STATEMENT OF THE PROBLEM

Although Zambia's 2025 cyber laws were intended to tackle cybercrime, serious issues remain in their content and implementation. Stakeholders have expressed concern that some provisions are worded in an ambiguous or unduly broad manner. Section 10 of the Cyber Crimes Act No. 4 of 2025 (CCA), prohibits recording a private conversation authorizing the action only in exceptional circumstances including to protect the interests of a party to the conversation. The scope of what amounts to sufficient interest to warrant the recording is any one's guess. Concern has also been raised concerning whether the Cyber Security Act No. 3 of 2025 (CSA) adequately safeguards constitutional rights being derogate from including the Right to Privacy. The Act authorizes a law enforcement officer to, where such law enforcement officer reasonably believes an offence has been committed, is likely to be committed, or is being committed, apply ex-parte to a judge for an interception of communication order. It may be argued that the law enforcement officer should before applying for the Court Order, be compelled to seek the Attorney General's consent. This was as was provided for in the repealed Cyber Security and Cyber Crimes Act No. 2 of 2021.

It has also been argued that important phrases in the Acts, such as "unauthorized access" and "critical infrastructure," lack precise definitions, potentially criminalizing innocent behaviour or permitting unregulated monitoring.¹⁴ Also raised have been arguments that an overlap in agency mandates between ZICTA, the new Cyber Security Agency, and the Police Cyber Unit calling for more coordination among the agencies.¹⁵ Questions regarding the sufficiency of enforcement capabilities of the agencies linger considering that the agencies while requiring special training and increased resources may not be adequately funded. This leaves the agencies in the forefront of ensuring national cyber security unprepared.

Questions exist regarding whether or not the pieces of legislation are consistent with best practice as projected in international instruments. The Acts, should, ideally, align

¹⁴ Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 13 November 2025

¹⁵ *ibid*

with instruments such as the Council of Europe's Cybercrime Convention (Budapest Convention, 2001) and the African Union's Malabo Convention on Cybersecurity and Data Protection (2014.)¹⁶

While Zambia's cybercrime and cyber security – related statutes, are definitely a step forward, they exhibit both institutional as well as substantive shortcomings which have the potential of limiting their effectiveness. The Acts do not, as observed, adequately safeguard Constitutionally guaranteed rights – placing them in jeopardy. This study seeks to conduct a critical analysis of the appropriateness and adequacy of the two pieces of legislation – investigating and highlighting their shortcomings for purposes of informing essential legal reform.

1.3 RESEARCH OBJECTIVES

The study is guided by the following objectives:

1. Exploring the concepts of cyber-crime, cyber security and constitutional rights.
2. Exploring the legal framework governing cyber-crime, cyber security and constitutional rights in Zambia.
3. Critically analyse the appropriateness of the Cyber Security Act and the Cyber Crimes Act in achieving their goals while safeguarding Constitutional Rights with lessons drawn from international best practice.

1.4 RESEARCH QUESTIONS

1. What are the concepts of cyber-crime and cyber security?
2. What are salient provisions of the legal framework governing cyber-crime, cyber security and constitutional rights in Zambia.
3. To critically analyse the appropriateness of the Cyber Security Act and the Cyber Crimes Acts in achieving their goals while safeguarding Constitutional Rights with lessons drawn from international best practice.

¹⁶ Michalsons, 'AU Convention on Cyber Security and Personal Data Protection | Malabo Convention' (Michalsons, 24 April 2023) <https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281> accessed 13 November 2025.

1.5 SIGNIFICANCE OF THE STUDY

This research will provide a critical assessment of Zambia's Cyber Security and Cyber Crimes Acts, highlighting legal and institutional shortcomings. It will inform policymakers, regulatory agencies, and civil society on necessary reforms, capacity building, and best practices to strengthen cyber governance while balancing security and human rights.

1.6 SCOPE OF THE STUDY

While cybercrime encompasses a wide range of offences, this research focuses on Zambia's Cyber Security and the Cyber Crimes Acts, examining their adequacy and appropriateness in combatting cyber-crime, fostering cyber security while also safeguarding constitutional rights. The research analyses the legislative cyber-crime and cyber security framework, including the adequacy of institutions created or alluded to thereunder such as the Cyber Security Agency. The study will seek to draw lessons from best practice where appropriate.

1.7 DEFINITION OF KEY TERMS AND ACRONYMS

In this study, the following terms and acronyms are used as defined below:

“Cybercrime”: Criminal activities carried out using computers, digital devices, or information networks. This includes offenses like hacking, malware distribution, online fraud, and illegal interception of data.

Also defined as a crime committed in, by or with the assistance of, a simulated environment or state of connection or association with electronic communications or networks including the internet.

“Cybersecurity”: The practice of protecting networks, systems, and data from digital attacks or unauthorized access. It encompasses technical measures (firewalls, encryption) and legal measures (laws and regulations) designed to maintain the confidentiality, integrity, and availability of information.

Also defined as tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies used to protect the cyber environment, organisation and user assets.

“Critical Information Infrastructure (CII)”: Computer systems and networks whose disruption or compromise would endanger national security, economic stability, or public safety. Under the Cyber Security Act, “critical infrastructure” broadly includes electronic platforms upon which critical data relating to sectors such as energy, finance, health, and government services sit.

Zambia Information and Communications Technology Authority (ZICTA): The national regulatory body for telecommunications and ICT in Zambia. ZICTA is responsible for, among others, licensing telecommunication and internet service providers, protection of consumers and fostering investment in the ICT sector.

“Zambia Cyber Security Agency (ZCSA)”: A new agency established by the Cyber Security Act, 2025. The ZCSA is empowered to coordinate the national cybersecurity strategy, audit information systems, and support law enforcement in cyber incidents.

“Information and Communications Technology” (ICT): Encompasses all technologies for processing and communicating information, including the internet, computer networks, mobile networks, hardware, software, and related services.

1.8 LITERATURE REVIEW

According to **Edrine Wanyama**¹⁷ of the Collaboration on International ICT Policy in East and Southern Africa (CIPESA), the Cyber Security and Cyber Crimes Acts of 2025 aim to strengthen Zambia's capacity to prevent and respond to digital threats such as cyber fraud, ransomware, and attacks on critical infrastructure.¹ Wanyama warns that loosely defined offenses and unduly wide powers handed to law enforcement may lead to misuse, potentially undermining the intended cybersecurity goals¹⁸. This position is consistent with this current study which demonstrates that, while the Acts contain substantive measures

¹⁷ Edrine Wanyama, ‘Zambia’s Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights’ (CIPESA, 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 13 November 2025

¹⁸ *ibid*

addressing cyber risks, their usefulness is hindered by among others, ambiguous language and inadequate safeguards. The findings further support Wanyama's recommendation for more institutional independence and oversight measures to guarantee that the Acts achieve their intended purposes while protecting privacy and civil rights. Overall, Wanyama's study supports the premise that the legislation has potential, but it needs structural and procedural improvements to be truly effective.

Whereas the above study was, like the current one, based on the same two pieces of legislation, this current study differs from Wanyama's in that it is more detailed and the analysis more critical than Wanyama's. Wanyama's for instance, adopts a very high level consideration of the two pieces of legislation with the study only referring to four sections in total – Sections 4, 21 and 39 of the CSA and Section 22 of the Cyber Crimes Act. The consideration of these sections is not adequately thorough and critical and other shortcomings are not addressed including removal from the CSA of a provision that compelled law enforcement officers to obtain the Attorney General's consent interception communication. Section 10 of the CSA which allows interception for purposes of protecting the interest of a party to the conversation without clarifying what would qualify as adequate interest was not considered.

This current study is thus essential in filling the gap left by the above study.

Wiriranai Brilliant Masara¹⁹ contends in the Journal of Democracy that the Acts serve as weapons for state control rather than instruments to tackle cyber risks. The study contends that criminalising "false information" and content that causes emotional distress facilitates censorship and digital repression, diverting focus away from serious cybersecurity issues²⁰. Masara's point of view differs slightly from this research, since the study acknowledges several provisions aimed at combating cybercrime but warns that their efficiency is undermined by overreach and state monitoring priority. While the study shares Masara's worries about misalignment with democratic ideals, it distinguishes between measures with valid cybersecurity goals and those that are vulnerable to

¹⁹ Wiriranai Brilliant Masara, 'How Zambia's Cyber Laws Rebrand Repression' (Journal of Democracy Online Exclusive, 2025) <https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-laws-rebrand-repression/> accessed 13 November 2025.

²⁰ *ibid*

exploitation. While particular sections of the Acts effectively address specific concerns, including attacks on vital infrastructure, their overall impact may be undermined by inadequate safeguards.

In their 2023 study, **Siampondo and Chansa**²¹ investigate the implementation of Zambia's cyber laws and discover that enforcement agencies lack specialist training, digital forensic equipment, and coordinated frameworks. Their findings highlight the criminalization of offenses such as hacking, data interference, and identity fraud, but also identify inadequacies in addressing emerging threats such as ransomware, phishing, and social engineering. The result coincides with previous research, which identified enforcement capacity as a significant element limiting the Acts' effectiveness. Siampondo and Chansa stress the importance of institutional change, capacity building, and frequent legislative updates in improving the cybersecurity framework's responsiveness.²² This current research supports these recommendations, implying that efficacy is not exclusively determined by legal rules, but also by institutional preparation and practical competence. Their research supports the conclusion that, even though Zambia's 2025 Acts create a significant legal framework, their goals depend on effective enforcement and technological capability.

While Siampondo and Chansa's study may align with this current one in some respect, the latter differs in various ways including holding a different opinion with respect to ransomware and social engineering crimes. This study holds the view that ransomware, for instance, is catered or in the Cyber Crimes Act under Section 13.

M&J Consultants²³ offer a practical viewpoint on the Acts' impact on enterprises and compliance requirements. According to the study, obligatory installation of interception devices and data retention obligations assist law enforcement in detecting cybercrimes but may impose major operational constraints on businesses. This viewpoint is in accord

²¹ G M Siampondo, M Sumbwanyambe & B Chansa, 'A Study on the Existing Cybersecurity Policies and Strategies in Combating Increased Cybercrime in Zambia' (2023) 14 *Journal of Information Security* 294 <https://doi.org/10.4236/jis.2023.144017> accessed 13 November 2025

²² *ibid*

²³ M&J Consultants, 'Zambia's New Cybercrime Law: Essential Knowledge for Entrepreneurs' (M&J Consultants, 2025) <https://mjconsultants.co.zm/zambias-new-cybercrime-law-essential-knowledge-for-entrepreneurs/> accessed 13 November 2025.

with this research, recognizing the Acts' potential to increase security infrastructure while emphasizing limitations in practical implementation.

M&J Consultants' findings are in accord with this study's initial perception that the Acts are fairly effective against cyber risks, but they require clear procedural standards, regulatory clarity, and safeguards to ensure compliance does not jeopardize civil liberties²⁴. The study strengthens the belief that balancing cybersecurity objectives with privacy and operational feasibility is essential.

Kay-Lyne Wolfenden²⁵ criticizes the Acts for undermining constitutional freedoms, particularly privacy and freedom of expression. The analysis agrees with Wolfenden's evaluation of overbroad provisions and a lack of judicial control, concluding that such flaws restrict the Acts' usefulness in countering serious cyber dangers. Wolfenden suggests reforms to maintain proportionality, requiring judicial authorization for surveillance, and establishing public reporting methods.²⁶ These recommendations supplement this study, which emphasizes the need of legislative safeguards and institutional independence in ensuring that the Acts function as intended. Wolfenden's research supports the view that effectiveness is dictated not just by the presence of offenses, but also by procedural and institutional structures that ensure lawful enforcement.

Again, while Wolfenden's study may be based on the same Acts as this current one, the former is not as detailed and thorough as the current study. This may be observed by the fact that the current study includes analysis of provisions in the Cyber Crimes Act that contradict those in the Cyber Security Act.

The **Global Network Initiative (GNI)**²⁷ compares Zambia's cyber regulations to international norms, including the Budapest and Malabo Conventions⁶. The study

²⁴ *ibid*

²⁵ Kay-Lyne Wolfenden, 'LAZ Opposes Zambia's New Cyber Laws Over Rights Infringement' (TechAfrica News, 23 April 2025) <https://techafricanews.com/2025/04/23/laz-opposes-zambias-new-cy-laws-over-rights-infringement/> accessed 13 November 2025.

²⁶ *ibid*

²⁷ Global Network Initiative, 'Five Things to Know: Zambia's Cyber Crimes Act and Cyber Security Act' (ICNL, 2025) <https://www.icnl.org/post/tools/five-things-to-know-zambias-cyber-crimes-act-and-cyber-security-act> accessed 13 November 2025.

identifies flaws such as unlimited data interception, a lack of independent control, and ambiguous definitions of cyber offenses. GNI's study supports this current research, in identifying deficiencies that have the potential of jeopardizing both digital rights as well as the Acts' ability to achieve their intended purpose.²⁸ Global Network Initiative's study suggests several improvements, including multi-stakeholder monitoring, transparency in surveillance operations, and the incorporation of proportionality clauses. This current study will consider and analyse these recommendations to determine their inclusion or otherwise in chapter five.

Global Network Initiative's study, though based on the same Acts as this study, is not as detailed and neither is the analysis as critical as that adopted in this current study.

According to **CIPESA**²⁹, Zambia's cyber laws do not effectively safeguard privacy and data retention rights, and enforcement is centralized in the executive. This current research agrees that institutional centralisation and a lack of adequate judicial safeguards may hinder the Acts' practical realization of its goals. CIPESA suggests combining constitutional and international safeguards, increasing civil society oversight, and clarifying offense definitions.³⁰ These recommendations will be considered for inclusion in this current study's final chapter.

Patricia Nachilima's 2024 dissertation³¹ on African cybercrime regimes emphasizes the issues of enforcement and compliance in nations with inadequate institutional capability. The study supports this current research with both taking the stance that legal provisions alone are insufficient without capable agencies, training, and technology infrastructure. Nachilima emphasizes that inadequacies in enforcement processes can allow cyber risks to spread despite extensive legislation.³² This is consistent with the research problem observed by the author of this current dissertation namely that Zambia's Acts are only partially effective and that institutional preparedness and operational competence should

²⁸ *ibid*

²⁹ CIPESA, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (n 1).

³⁰ *ibid*

³¹ Patricia Nachilima, 'Challenges of Cybercrime Enforcement in Africa: The Case of Zambia' (Dissertation, University of Lusaka, 2024).

³² *ibid*

complement an appropriate legal framework for any legal and regulatory regime to function as intended.

Emmanuel Kunda³³ in 2023, conducted research on Zambia's Cyber Security Act in light of rising risks including ransomware and online financial theft. Kunda claims that, while the Act specifies clear crimes and reporting requirements, enforcement is inconsistent due to low capacity and a lack of public knowledge.³⁴ The author of this dissertation agrees with this assessment, adding that safeguards in the legal framework are insufficient to uphold constitutional rights in the process of combatting cyber-crime and fostering cyber security.

The 2025 ICNL³⁵ assessed the two pieces of legislation under discussion seeking to consider whether they appropriately balance national security with digital rights. The analysis concludes that, while the Acts handle cybercrime holistically, overbroad monitoring and content-related offenses may impede free expression and privacy protections. The ICNL, to guarantee that cybersecurity measures do not jeopardize democratic freedoms, calls for proportionality, judicial scrutiny, and periodical offense review.³⁶

This current dissertation will, following a critical analysis, seek to compare the findings with the above conclusion reached by the ICNL study referred to above.

1.9 RESEARCH METHODOLOGY

Approach: This study will adopt a qualitative, doctrinal research approach. It will involve analysis of legal texts, case law, policy documents, and relevant literature. A qualitative, doctrinal (legal-analytical) approach is appropriate because the research questions centre on examining statutes and institutional frameworks. By critically studying appropriate legislation, parliamentary debates, agency reports, and related publications, the study will interpret the meaning and implications of legal provisions.

³³ Emmanuel Kunda, 'Effectiveness of the Cyber Security Act in Combating Emerging Cyber Threats in Zambia' (ResearchGate, 2023).

³⁴ *ibid*

³⁵ ICNL, 'Five Things to Know: Zambia's Cyber Crimes Act and Cyber Security Act' (n 6).

³⁶ *ibid*

Research Type: This study will be analytical with the researcher using pre-existing facts and information to formulate a hypothesis for evaluation.

Research Design: the design adopted for this study is descriptive and case study in by which a particular legal framework – that obtaining and governing cyber security and cyber-crime in Zambia will be critically analysed for its adequacy and appropriateness.

The study systematically evaluates the substance of the Cyber Security and Cyber Crimes Acts, comparing them against relevant best practice including international instruments. This design will allow the researcher to identify both strengths and weaknesses in the legal framework.

Data Collection: The research will rely primarily on **secondary data**. The researcher will collect and review documents including: the text of the Cyber Security Act, 2025, that of the Cyber Crimes Act, 2025, other relevant legislation, court decisions (if any) interpreting such legislation, relevant official reports from government agencies, as well as other publications by authors, NGOs, and international organizations. Academic books, journal articles, and credible media reports on Zambia's cyber laws will also be gathered and referred to. Where possible, interviews with experts (e.g. legal scholars, ICT officials) could supplement the documentary analysis, although the emphasis remains on published materials.

Data Analysis: The collected qualitative data will be analysed using content analysis. The researcher will systematically code and categorize information from the sources to identify recurring themes and issues. For example, sections of the Acts will be examined to see how they define offences or assign powers, and these will be compared to provisions in the Budapest and Malabo Conventions. Institutional data (e.g. agency mandates, budgets, training records) will be assessed to understand enforcement capacity. The comparative element (international vs. domestic law) will highlight shortcomings or misalignments.

Sampling Technique: A purposive sampling approach will be used to select relevant sources and cases. For legal texts, this means focusing on provisions directly related to cyber offences, enforcement powers, and safeguards. For literature and reports, the study

will prioritize influential or authoritative materials, such as official White Papers, Parliamentary Committee reports, publications by Zambian legal scholars, and regional cybercrime assessments. The aim is to cover a representative range of perspectives (governmental, academic, civil society).

Study Population: The study population will comprise experts in cyber security and cyber-crimes as well as authors on and scholars of the subject matter.

Ethical Considerations: The research will adhere to ethical standards in academic research. All sources will be properly cited to avoid plagiarism. If interviews or consultations are conducted, participants will provide informed consent, and their confidentiality will be respected. The study involves analysis of public documents and does not pose risk to human subjects. The researcher will ensure objectivity, avoid conflicts of interest, and respect Zambian laws and the University's ethical guidelines throughout the research process.

1.10 RESEARCH OUTLINE

The structure of the dissertation will be as follows:

Chapter One: Background of the study; statement of the problem; research objectives and questions; significance; scope; literature review, methodology and ethical considerations.

Chapter Two: Overview of the concepts of cyber-crime, cyber security and constitutional rights.

Chapter Three: select provisions and an overview of the legal framework governing cyber security and cyber-crime.

Chapter Four: A critical analysis of the adequacy and appropriateness of the legal and institutional framework governing cyber security and cyber-crime including consideration of legal, capacity, enforcement, coordination and other challenges. The chapter will consider what lessons Zambia may draw from relevant international instruments such as the Budapest and Malabo Conventions.

Chapter Five: Presentation of research findings and conclusions; synthesis of analyses from Chapters Two to Four; answers to research questions; recommendations for legal and policy reforms to strengthen cyber governance while upholding fundamental rights.

1.11 Conclusion

This chapter was introductory – laying the foundation for the whole dissertation through provision of the background of the study, projecting the problem the dissertation is being written to resolve, conveying what the objectives of the study are, bringing out how significant this study is as well as the scope of the study, literature review, the methodology to be adopted and ethical considerations.

The next chapter will delve into an exploration of concepts that are at the very heart of the study – cyber security and cyber-crime.

1.12 TIMETABLE AND INTENDED TIMELINE

ACTIVITY	TIME ALLOCATION
Submission of Chapter two to supervisor.	1 week
Submission of Chapter three to supervisor.	1 week
Submission of Chapter four to supervisor.	1 week
Submission of Chapter five to supervisor.	1 week
Submission of dissertation to course coordinator.	1 Day

CHAPTER TWO

EXPLORING THE CONCEPTS OF CYBER-CRIME, CYBER SECURITY AND CONSTITUTIONAL RIGHTS.

2.0 INTRODUCTION

This chapter explores the concepts of cyber-crime, cyber security and constitutional rights. The Chapter begins by providing a brief background of the doctrine, followed by a clear definition and explanation of what cyber-crime and cyber security entails. The research proceeds to chapter to look at the rationale behind cyber-crime and cyber security. The research further explores the concepts of cyber-crime, cyber security and constitutional rights. Finally, a conclusion will be drawn.

2.1 DEFINITIONS OF CYBER-CRIME AND CYBER SECURITY

Zambia's digital age offers economic and social benefits, but it also introduces new risks. Cybercrime, or unlawful acts involving computer networks, has emerged as a major concern in Zambia and around the world. In response, Zambia passed the Cyber Security and Cyber Crimes Act No. 2 of 2021 (which was repealed by new legislation in 2025) and participates in regional frameworks (such as the African Union's Malabo Convention) to strengthen cybersecurity. These steps are intended to safeguard the public and institutions from fraud, hacking, malware, and other cyber risks.³⁷ However, strong cybersecurity capabilities must be balanced against Zambia's constitutional safeguards (privacy, free expression, fair trial, etc.).³⁸

Cybercrime refers to any criminal activity that involves computers or networks. It can encompass both new and classic crimes assisted by computers. International instruments and national laws do not have a single definition, but instead list violations.³⁹ For example,

³⁷ National Prosecution Authority, '20 Chinese Nationals and One Cameroonian Convicted in Major Cyber Crime Case' (NPA, 13 June 2024) <https://www.npa.gov.zm/index.php/2024/06/13/20-chinese-nationals-and-one-cameroonian-convicted-in-major-cyber-crime-case/> accessed 18 November 2025.

³⁸ *Zambia, Constitution (1991, rev. 2016)*, Preamble, Constitute Project https://www.constituteproject.org/constitution/Zambia_2016 accessed 18 November 2025.

³⁹ Michael Aaron Dennis, 'Cybercrime' (Encyclopaedia Britannica, updated 11 October 2025) <https://www.britannica.com/topic/cybercrime> accessed 18 November 2025.

Zambia's Cyber Security Act and Cyber Crimes Act (2025) criminalizes "computer-related misrepresentation" and "identity-related crimes" (both of which are utilized in international scams).⁴⁰ Similarly, the AU Malabo Convention on Cybersecurity and Personal Data Protection requires Member States to amend ICT-related laws (e.g., unauthorized access, data interference, cyber-fraud) in response to the changing digital world.⁴¹ Cybercrime in Zambia involves fraudulent internet schemes (such as the 'Golden Top' call-center scams), social media defamation used for extortion, ATM skimming, and other offences targeting digital systems.

Cybersecurity refers to the procedures taken to secure digital systems, networks, and data from attack or exploitation. It consists of technical safeguards (encryption, firewalls, anti-malware), organizational rules (access restrictions, incident response), and legal frameworks. According to the Malabo Convention, cybersecurity is critical to creating "a credible digital space for electronic transactions, personal data protection, and combating cybercrime".⁴² In corporate terms, cybersecurity is defined as "the practice of protecting people, systems, and data from cyberattacks" using technology, processes, and regulations.⁴³ In Zambia, cybersecurity efforts involve both public and private actors. For example, the Zambia Information and Communications Technology Authority (ZICTA) requires service providers to adhere to certain security standards, and the Cyber Act mandates security audits of critical information infrastructure. Cybersecurity focuses on defense and prevention, whereas cybercrime concerns the criminal conduct itself; both are two sides of the same coin.⁴⁴

⁴⁰ National Prosecution Authority, '20 Chinese Nationals and One Cameroonian Convicted in Major Cyber Crime Case' (NPA, 13 June 2024) <https://www.npa.gov.zm/index.php/2024/06/13/20-chinese-nationals-and-one-cameroonian-convicted-in-major-cyber-crime-case/> accessed 18 November 2025.

⁴¹ African Union, *African Union Convention on Cyber Security and Personal Data Protection* (adopted 27 June 2014, entered into force 30 days after the fifteenth instrument of ratification) EX.CL/846(XXV) <https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf> accessed 18 November 2025.

⁴² African Union, *African Union Convention on Cyber Security and Personal Data Protection* (adopted 27 June 2014, EX.CL/846(XXV)) <https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf> accessed 18 November 2025.

⁴³ IBM, 'What Is Cybersecurity?' (IBM Think, n.d.) <https://www.ibm.com/think/topics/cybersecurity> accessed 18 November 2025.

⁴⁴ Bowmans, "Zambia: New Laws to Strengthen Cybersecurity and Cybercrime Capacities" (Bowmans, 7 October 2025) <https://bowmanslaw.com/insights/zambia-new-laws-to-strengthen-cybersecurity-and-cybercrime-capacities/> accessed 18 November 2025.

2.2 THE RATIONALE BEHIND CYBER-CRIME AND CYBER SECURITY

Increasing threat landscape. Zambia's increasing internet usage has made cybercrime a major cause for concern. Zambia had over 12.6 million internet users (~64% penetration) by 2023, with mobile devices being the most popular.⁴⁵ Increased connection implies greater chances for fraudsters and hackers. Cyberattacks have increased significantly, with one study estimating 10 million attacks in Zambia in 2021, leading to over 50,000 investigations. By 2022, investigations had nearly doubled.⁴⁶ High-profile incidents emphasize the threat. In 2023-24, Zambian authorities uncovered a large-scale scam operation ("Golden Top") organized by foreign nationals who generated thousands of false online identities and fraudulent investment schemes. *Twenty foreign suspects (mainly Chinese) were later convicted of crimes under the Cyber Crimes Act (2021) and the ICT Act (2009).*⁴⁷ Similarly, the National Pensions Scheme Authority (NAPSA) reportedly lost months of data in a hack, while the Bank of Zambia's social media accounts were compromised in 2023.⁴⁸ These cases demonstrate how cybercrime may endanger both private citizens and essential institutions.

Motivations for cybercrime. Criminals engage in cybercrime primarily for financial gain (online fraud, theft, extortion/ransomware), but also for political or ideological reasons (disinformation, hacktivism, or covert surveillance). Cyber tools facilitate classic crimes (e.g., phishing may capture identities inexpensively) while also enabling new crimes such as malware attacks or spreading misleading information. Resourceful criminals can operate internationally with relative anonymity. In Africa, insufficient cyber legislation and enforcement capacity can attract transnational cybercriminal organizations. According to the Zambian government, the Golden Top scammers exploited SIM-boxes to circumvent

⁴⁵ Freedom House, *Freedom on the Net 2024: Zambia* (Freedom House, 2024)

<https://freedomhouse.org/country/zambia/freedom-net/2024> accessed 18 November 2025

⁴⁶ Africa Defense Forum, 'Chinese Cyber Scam Bust Reveals Zambia's Efforts to Disrupt Online Fraudsters' (ADF, 7 May 2024) <https://adf-magazine.com/2024/05/chinese-cyber-scam-bust-reveals-zambias-efforts-to-disrupt-online-fraudsters/> accessed 18 November 2025.

⁴⁷ National Prosecution Authority, '20 Chinese Nationals and One Cameroonian Convicted in Major Cyber Crime Case' (NPA, 13 June 2024) <https://www.npa.gov.zm/index.php/2024/06/13/20-chinese-nationals-and-one-cameroonian-convicted-in-major-cyber-crime-case/> accessed 18 November 2025.

⁴⁸ Diggers Editor, 'The Hacking at NAPSA, BoZ Pose a National Security Risk' (News Diggers, 27 July 2023) <https://diggers.news/opinion/2023/07/27/the-hacking-at-napsa-boz-pose-a-national-security-risk/> accessed 18 November 2025

telecom billing and acquire victims' data under false pretenses⁴⁹, demonstrating a sophisticated use of technology for economic crime.

Implications and harms. Cybercrime destroys trust in the digital economy and can result in significant losses for businesses and individuals. Loss of personal information or money can have disastrous human effects. Attacks on banks, government databases, or infrastructure might jeopardize national security and public services (as demonstrated by the NAPSA and BoZ hacks).⁵⁰ Cybercrime also impedes international investment, since investors and partners may be hesitant to cooperate without adequate cyber protections. Pervasive fraud (for example, mobile money frauds and social media con artists) can erode public trust in technology.

Need for regulation and cybersecurity. Because cybercrime easily crosses boundaries, Zambia, like other African countries, has strengthened its laws and agencies. The Cyber Security and Cyber Crimes Act of 2021 was Zambia's first comprehensive law, criminalizing a variety of ICT offenses and establishing a cybersecurity agency. It established a Cyber Security Advisory Committee and a Cyber Council to coordinate national cybersecurity policies. Specialized units of the police and anti-corruption authorities have been established to investigate cybercrimes.⁵¹ At the same time, individuals and enterprises must increase their own defenses (antivirus, backups, user education). The premise is that robust cybersecurity and deterrent sanctions will reduce crime and create a more secure digital economy.

Regional and international obligations. International agreements also influence Zambian legislation. Zambia, an African Union member, has signed the Malabo Convention on Cybersecurity and Personal Data Protection of 2014. That Convention clearly urges nations to enact cybercrime legislation and protect personal data while

⁴⁹ National Prosecution Authority, '20 Chinese Nationals and One Cameroonian Convicted in Major Cyber Crime Case' (NPA, 13 June 2024) <https://www.npa.gov.zm/index.php/2024/06/13/20-chinese-nationals-and-one-cameroonian-convicted-in-major-cyber-crime-case/> accessed 18 November 2025.

⁵⁰ Diggers Editor, 'The Hacking at NAPSA, BoZ Pose a National Security Risk' (News Diggers, 27 July 2023) <https://diggers.news/opinion/2023/07/27/the-hacking-at-napsa-boz-pose-a-national-security-risk/> accessed 18 November 2025.

⁵¹ Africa Defense Forum, 'Chinese Cyber Scam Bust Reveals Zambia's Efforts to Disrupt Online Fraudsters' (ADF, 7 May 2024) <https://adf-magazine.com/2024/05/chinese-cyber-scam-bust-reveals-zambias-efforts-to-disrupt-online-fraudsters/> accessed 18 November 2025.

upholding human rights.⁵² In other words, Malabo commits Zambia to both harsh cybercrime repression and respect for fundamental liberties. (Free expression and journalism are guaranteed by Article 20 of Zambia's Constitution, for example, therefore any cyber law must not unreasonably restrict these rights.)⁵³ Zambia has also been affected by the Council of Europe's Cybercrime Convention (Budapest, 2001) and UN resolutions against cybercrime.

Local cyber trends. Zambia's recent data and cases demonstrate the rationale. In April 2024, anti-fraud efforts busted the Golden Top scam, seizing 11 SIM boxes, 37,000 SIM cards, hundreds of devices, and enormous sums of money.⁵⁴ According to Zambian security experts, Internet fraud schemes are on the rise throughout Africa, and the Zambian government has responded by hosting yearly Cyber Security Summits and joining INTERPOL cyber networks. However, observers point out gaps: a 2023 study by Lusaka researchers warned that finance and coordination (between ZICTA, police cyber-units, and the new Cyber Agency) was insufficient.⁵⁵ Rising attacks, multinational frauds, and legislative catch-up highlight the importance of strong cybercrime legislation and cybersecurity regulations in Zambia.

2.3 CONSTITUTIONAL RIGHTS ON CYBER-CRIME AND CYBER SECURITY

Zambia's Bill of Rights (Part III of the 2016 Constitution)⁵⁶ enshrines several key liberties that bear on cyber issues: notably privacy, free expression, and due process. Any cybercrime or cybersecurity law must be interpreted consistently with these constitutional guarantees. In practice, Zambia's courts and civil society have begun to grapple with how digital surveillance, censorship and data collection intersect with the Constitution.

⁵² African Union, *African Union Convention on Cyber Security and Personal Data Protection* (adopted 27 June 2014, EX.CL/846(XXV)) Preamble ("Reaffirming the commitment ... protected by international human rights Conventions") <https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf> accessed 18 November 2025.

⁵³ *Zambia, Constitution* (amended 2016) art 1(1), Constitute Project https://www.constituteproject.org/constitution/Zambia_2016 accessed 18 November 2025.

⁵⁴ *Zambia, Constitution* (1991, rev. 2016), Preamble, Constitute Project https://www.constituteproject.org/constitution/Zambia_2016 accessed 18 November 2025.

⁵⁵ Africa Defense Forum, 'Chinese Cyber Scam Bust Reveals Zambia's Efforts to Disrupt Online Fraudsters' (ADF, 7 May 2024) <https://adf-magazine.com/2024/05/chinese-cyber-scam-bust-reveals-zambias-efforts-to-disrupt-online-fraudsters/> accessed 18 November 2025.

⁵⁶ The Constitution of Zambia, Act No. 2 of 2016 (Amendment Act)

Privacy and data protection. Article 17 of the Constitution⁵⁷ prohibits unnecessary searches: "Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises". This high privacy protection means that government personnel cannot lawfully inspect personal devices, offices, or premises without judicial authorization. To reflect this, Zambia's Cyber Security Act 2025⁵⁸ requires cyber inspectors to get a warrant before conducting any search or inspection.⁵⁹ (According to LexAfrica's interpretation, the Act "protects the right to privacy; a cyber inspector must have or be in possession of a warrant prior to exercising [search] powers.") Civil society has also raised concerns about invasions of privacy. Bloggers of Zambia and the Chapter One Foundation sued the ICT Authority (ZICTA) in Lusaka High Court in 2023, claiming that a regulation requiring SIM card users to provide live facial images was unlawful.⁶⁰ The case (which prompted ZICTA to suspend the rule) demonstrates that forced biometric collecting is closely scrutinized under Article 17's privacy guarantee.

Freedom of expression and press. Article 20 of the Constitution⁶¹ ensures freedom of expression and a free press: "No person shall be hindered in the enjoyment of his freedom of expression or freedom from interference with his correspondence except with his own consent." These precautions apply both online and offline. The Constitutional Court and other authorities recognize "freedom of expression" as include the receipt and dissemination of information via any means, and private correspondence is expressly protected. As a result, any cybercrime regulation must not unreasonably restrict lawful expression.⁶²

⁵⁷ *ibid*

⁵⁸ Section 56 of Cyber Security Act No. 3 of 2025

⁵⁹ Jackie Jhala and Rabeca Banda (Corpus Legal Practitioners), "*Zambia: Cyber Security and Cyber Crimes Act*" (Lex Africa, 29 April 2021) <https://lexafrica.com/2021/04/zambia-cyber-security-and-cyber-crimes-act/> accessed 18 November 2025.

⁶⁰ Freedom House, *Freedom on the Net 2024: Zambia* (Freedom House, 2024) <https://freedomhouse.org/country/zambia/freedom-net/2024> accessed 18 November 2025, "Key Developments, June 1, 2023–May 31, 2024", C6.

⁶¹ The Constitution of Zambia, Act No. 2 of 2016 (Amendment Act)

⁶² Edrine Wanyama, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 18 November 2025.

Critics say that Zambia's cybercrime laws are overly broad and imprecise, thereby chilling free speech. For example, the Cyber Crimes Act 2025 include charges such as "harassment" or "humiliation" on digital platforms, as well as revived defamation laws. Civil society (CIPESA, bloggers, and media attorneys) has argued that phrases like "harassment" are so broad that they could be used to punish valid criticism of politicians. The Cybersecurity Act also authorizes authorities to intercept and monitor communications (Sections 21, 39) with little oversight.⁶³

The Law Association of Zambia (LAZ) expressed concern that the Act's wide definitions of "critical information" and surveillance powers may render it illegal to acquire, hold, or impart information without State consent ⁶⁴. Indeed, Section 20(2) of the Constitution expressly prohibits any law "derogating from the freedom of the press". As a result, judges evaluating any cyber-related issue must strike a balance between enforcement needs and constitutionally protected liberties. (against date, judicial challenges against the 2025 regulations are pending; nonetheless, the concept remains that censorship or prior restraints in cyberspace violate the Constitution's strict right of expression.)⁶⁵

Due process and fair trial. Article 18⁶⁶ ensures a fair hearing and related procedural rights in criminal matters. In the context of cybercrime, this means that suspects have the right to court authorization before any intrusive measures (arrest, search, or wiretap), to be informed of charges, to counsel, and to a timely trial. For example, while the Cyber Security Agency may monitor networks, any interception of private data without authorization must be allowed by a court order (in accordance with Article 18's provision that legal power not be arbitrary)⁶⁷. Evidence collected illegally (without a warrant) may be considered inadmissible for violating constitutional rights. In principle, the

⁶³ Global Partners Digital, *How to Respect Privacy and Free Expression as a Tech SME in Zambia* (2018) 9, Global Partners Digital https://www.gp-digital.org/wp-content/uploads/2018/12/ZAMBIA_web.pdf accessed 18 November 2025.

⁶⁴ Ay-Lyne Wolfenden, 'LAZ Opposes Zambia's New Cyber Laws Over Rights Infringement' (TechAfrica News, 23 April 2025) <https://techafricanews.com/2025/04/23/laz-opposes-zambias-new-cyber-laws-over-rights-infringement/> accessed 18 November 2025.

⁶⁵ *ibid*

⁶⁶ The Constitution of Zambia, Act No. 2 of 2016 (Amendment Act)

⁶⁷ Ay-Lyne Wolfenden, 'LAZ Opposes Zambia's New Cyber Laws Over Rights Infringement' (TechAfrica News, 23 April 2025) <https://techafricanews.com/2025/04/23/laz-opposes-zambias-new-cyber-laws-over-rights-infringement/> accessed 18 November 2025.

Constitution's due process articles require that cybercrime investigations follow the same safeguards as other crimes: the accused must examine and challenge the evidence, obtain a defence lawyer, and be presumed innocent.⁶⁸

Cases and controversies. While particular constitutional court opinions on cyber laws are still being issued, there have been significant challenges. NGOs allege that current cyber legislation infringe rights. They filed petitions claiming that clauses permitting broad surveillance "without meaningful judicial oversight" violate Articles 17 and 20.⁶⁹ International observers, including the US Embassy and GNI, have warned that the 2025 Acts allow for "real-time surveillance and interception...without sufficient procedural checks." These criticisms parallel a broader African Commission recommendation that defamation (libel) laws be decriminalized in order to protect free expression. Zambia has foreshadowed defamation reform in 2022, and critics point out that new cyber laws essentially penalize false online claims.⁷⁰

Balancing security and rights. Zambia's Constitution safeguards fundamental digital rights. Law enforcement is authorized to combat cybercrime, but only within constitutional boundaries. Proper balance necessitates public oversight (e.g., judicial warrants for surveillance), precise legal definitions (so that ordinary speech is not criminalized), and accountability. Section 4 of the Cyber Security work, for example, places the Cyber Agency under the office of the President, raising issues about separation of powers; strong courts and legislatures are required to ensure that such agencies work legitimately. Practical initiatives, such as the establishment of a Data Protection Commission (June 2023)⁷¹, demonstrate an understanding that citizens' privacy must be protected even as cyberthreats are addressed. In the end, public confidence in cybersecurity efforts and

⁶⁸ Ibid

⁶⁹ *Zambia, Constitution* (1991, rev. 2016) art 1(1), Constitute Project https://www.constituteproject.org/constitution/Zambia_2016 accessed 18 November 2025.

⁷⁰ Edrine Wanyama, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 18 November 2025, s 39, s 22.

⁷¹ Freedom House, *Freedom on the Net 2024: Zambia* (Freedom House, 2024) <https://freedomhouse.org/country/zambia/freedom-net/2024> accessed 18 November 2025, Key Developments ("Zambia established a Data Protection Commission in June 2023") C6

Zambia's democracy will be maintained by respecting due process (Article 18), privacy (Article 17), and free expression (Article 20) in the digital realm.

Cybersecurity and cybercrime control are critical to Zambia's progress, but they must be properly balanced with constitutional freedoms. On the one hand, escalating cyberattacks and fraud (ranging from individual scams to network hijackings) necessitate strong legislation and technology safeguards, as demonstrated by the 2021 Cyber Act and succeeding 2025 laws. Zambia's Constitution, on the other hand, has provisions for privacy, free speech, and a fair trial, which limit how such powers can be exercised. In reality, this balance includes proper legal definitions (to avoid unclear offenses)⁷², warrants or judicial orders for searches and interceptions⁷³, and control procedures for any surveillance. International frameworks such as the AU Malabo Convention specifically require both security and rights protection.

The main lessons for Zambia are that legitimacy and openness are crucial. Citizens must understand that cyber laws are designed to combat crime rather than silence critics, such as by explicitly distinguishing between illicit online conduct and authorized political expression. Second, judicial safeguards should be in place. Warrants, independent audits of law enforcement, and remedies for rights abuses all contribute to conformity with Articles 17-20 of the Constitution. Public awareness and education are required: individuals should learn both how to protect themselves (changing passwords, identifying frauds) and their rights (e.g., not having personal data confiscated without justification).

2.4 CONCLUSION

This chapter explored the concepts of cyber-crime, cyber security and constitutional rights. The Chapter begun by providing a brief background of the doctrine, followed by a clear definition and explanation of what cyber-crime and cyber security entails. The research proceeded to chapter to look at the rationale behind cyber-crime and cyber

⁷² Edrine Wanyama, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 18 November 2025, s 39, s 22.

⁷³ Jackie Jhala and Rabeca Banda, 'Zambia: Cyber Security and Cyber Crimes Act' (Lex Africa, 29 April 2021) <https://lexafrica.com/2021/04/zambia-cyber-security-and-cyber-crimes-act/> accessed 18 November 2025, para on cyber inspectors.

security. The research further explored the concepts of cyber-crime, cyber security and constitutional rights.

CHAPTER THREE

EXPLORING THE LEGAL FRAMEWORK GOVERNING CYBER-CRIME, CYBER SECURITY AND CONSTITUTIONAL RIGHTS IN ZAMBIA

3.0 INTRODUCTION

This chapter explores the legal framework governing cyber-crime, cyber security and constitutional rights in Zambia. The Chapter begins looking at key relevant legal provisions from other Zambian statutes that look at cyber-crimes. The chapter will then extensively discuss the cyber security and cyber-crimes Act, 2025 in relation to cyber - crimes. Finally, a conclusion will be drawn

3.1 VARIOUS GOVERNING ACTS

Historically, Zambia relied on traditional regulations like the Penal Code Act⁷⁴, the Forfeiture of Proceeds of Crime Act⁷⁵, and the Electronic Communications and Transactions Act⁷⁶ to combat technologically enabled crimes. However, the increasing prevalence of digital fraud, identity theft, ransomware, cyber extortion, and attacks on essential information infrastructure needed a more specialised and modern legal framework. In 2025, the government enacted the Cyber Security Act, No. 3 of 2025 (CSA) and the Cyber Crimes Act, No. 4 of 2025 (CCA), which serve as the foundation for Zambia's modern cyber-governance system. These two Acts amended and expanded previous legislation, including updated definitions, institutional organizations, regulatory processes, cyber-incident protocols, and investigation authorities in accordance with international standards.

The Constitution is the supreme law in Zambia under which all legislation is issued and which guarantees individual inalienable right and freedoms. The currently valid republican constitution is the 1991 which has undergone multiple amendments including the last amendment in 2016.

⁷⁴ The Penal Code Act Chapter 87 of the laws of Zambia

⁷⁵ Forfeiture of Proceeds of Crime Act No 19 of 2010

⁷⁶ The Electronic Communications and Transactions Act No 4 of 2021

3.1.1 THE CONSTITUTION

The Republican constitution currently in force in Zambia is the 1991 Constitution which has undergone a series of amendments including the most recent in 2016.

Article 1 of the Constitution projects its supremacy stating:

- (1) “This Constitution is the supreme law of the Republic of Zambia and any other written law, customary law and customary practice that is inconsistent with its provisions is void to the extent of the inconsistency.
- (2) An act or omission that contravenes this Constitution is illegal.
- (3) This Constitution shall bind all persons in Zambia, State organs and State institutions.
- (4) The validity or legality of this Constitution is not subject to challenge by or before a State organ or other forum.
- (5) A matter relating to this Constitution shall be heard by the Constitutional Court.”

Part III of the Constitution contains the Bill of Rights laying out fundamental rights and freedoms of all individuals. Among the rights in the Bill of Rights are the following:

The Republican Constitution in Article 11 provides that all individuals shall have inalienable rights including:

- a. Right to life, liberty, security of the person and the protection of the law;
- b. Freedom of conscience, expression, assembly, movement and association;
- c. Protection of young persons from exploitation; and
- d. Protection for the privacy of his home and other property and from deprivation of property without compensation.

The Constitution of Zambia⁷⁷ thus remains the supreme law, defining the framework within which cyber security and cybercrime control must operate. Constitutional rights are

⁷⁷ The Constitution of Zambia 1991

increasingly important in the digital context due to the intrusive nature of technological surveillance, the sensitivity of personal data, and the growing reliance on digital platforms for communication and business. Cyber governance directly implicates several constitutional rights, including right to privacy, freedom of expression, and right to a fair trial.

The right to privacy is guaranteed under Article 17 of the Constitution⁷⁸. This includes protection from unauthorized searches of one's person, property, or premises, as well as interference with correspondence or communication. In today's digital age, this right applies to emails, metadata, mobile phone communications, cloud-based data, personal identity information, and digital records. Cybercrime legislation must consequently ensure that any monitoring, data access, or communication interception is carried out precisely within constitutional boundaries. The Cyber Security Act⁷⁹ is expected to meet this criterion by establishing judicial authorization for interception, guaranteeing that state intrusions into private communication are subject to external supervision. The Cyber Crimes Act⁸⁰ allows authorized officers to intercept communications where they have reasonable suspicion of a crime.

Another fundamental right touched by cyber regulation is the right to free expression, which is guaranteed by Article 20 of the Constitution⁸¹. Civic involvement, political conversation, journalistic expression, and social commentary now take place primarily on digital media. As a result, cyber legislation must distinguish between lawful expression, even if it is critical or controversial and kinds of communication that justify criminalization, such as hate speech, cyber harassment, or the sharing of illegal content. The Constitution recognizes justified restrictions on expression, but they must meet the requirements of necessity and proportionality. If cybercrime regulations are read too broadly, they risk suppressing legitimate expression, particularly political discourse on social media.

⁷⁸ Ibid

⁷⁹ No. 3 of 2025

⁸⁰ No. 4 of 2025

⁸¹ ibid

Article 16 of the Constitution⁸², which guarantees the right to property, has important implications for cyber legislation. Financial data, electronic records, cryptocurrencies, intellectual property, and corporate information are examples of digital assets that must be protected by the Constitution. Cybercrime offenses such as unauthorized access, data interception, and malware distribution jeopardize the integrity, security, and ownership of these digital assets. The Cyber Crimes Act⁸³ strengthens Article 16 by criminalising the manipulation or destruction of electronic data, acknowledging the modern reality that property exists not just in physical form but also in digital versions.

Cyber-crime investigations often involve forensic imaging, device seizure, password disclosure, and communication interception, which can violate constitutional protections if not properly supervised. The Constitution also protects fair trial rights, such as the presumption of innocence and the right to legal representation. A matter of discussion is how to treat unlawfully obtained evidence. The Cyber Security Act⁸⁴ and the Electronic Communications and Transactions Act⁸⁵ state that evidence collected through unauthorized interception is inadmissible except by leave of the Court. Judicial oversight over inspection is necessary to ensure electronic evidence is obtained following due process in accordance with the law.

The Constitution⁸⁶ thus establishes the normative context within which cyber legislation must be read. Any uncertainties in the Cyber Crimes Act⁸⁷ or Cyber Security Act⁸⁸ must be addressed in a way that upholds constitutional primacy. Individual rights can be maintained while allowing for efficient cyber governance via judicial interpretation and procedural safeguards.

It is imperative to take note that the rights guaranteed by the Constitution may be derogated from as provided by the Constitution itself. Such derogation requires to be necessary, provided for in a written piece of legislation which should have adequate

⁸² *ibid*

⁸³ No. 4 of 2025

⁸⁴ No. 3 of 2025

⁸⁵ The Electronic Communications and Transactions Act No 4 of 2021

⁸⁶ The Constitution of Zambia (Amendment) Act 2016

⁸⁷ No. 4 of 2025

⁸⁸ No. 3 of 2025

safeguards against unnecessary and over derogation. The question that will be asked and answered in subsequent chapters is whether the legal framework under discussion provides such safeguards.

3.1.2 CYBER SECURITY ACT, NO. 3 OF 2025

The Cyber Security Act⁸⁹ is the regulatory foundation of Zambia's national cyber governance architecture. Its goals are to improve cyber resilience, protect vital information infrastructure, regulate cyber-security service providers, and create methods for detecting, preventing, and responding to cyber threats. The Act is institutional rather than punitive in nature, complementing the Cyber Crimes Act⁹⁰ by emphasizing systemic control over the tabulation of specific offenses.

The Zambia Cyber Security Agency (ZCSA) is the central institution responsible for enforcing the Act and coordinating national cyber-security measures. The Agency, which reports to the President, is responsible for developing national cyber-security strategy, conducting risk assessments, providing technical guidance, and coordinating with law enforcement authorities⁹¹. The institutional placement underscores the strategic relevance of cyber security and recognizes that attacks to digital infrastructure can jeopardize national security, economic stability, and public safety. Recognizing the global nature of cyber threats, the Agency also enables collaboration with international cyber-security authorities.⁹²

One of the most important aspects of the Act is its control of critical information infrastructure (CII). Digital infrastructure is critical to many industries, including finance, electricity, telecommunications, mobile money, aviation, immigration, and national identity. A successful cyber-attack on these systems could cause financial turmoil, data leaks, or the disruption of critical services. Sections 14 – 17 of the Act⁹³ require controllers of CII to install security controls, conduct periodic audits, and report cyber incidents to the Agency. The implementation of obligatory reporting is especially important since early

⁸⁹ *ibid*

⁹⁰ No. 4 of 2025

⁹¹ Catherine Pule, 'Zambia Cyber Security Agency Coming' (Kalemba News, 30 April 2025) <https://kalemba.news/local/zambia-cyber-security-agency-coming/> accessed 18 November 2025.

⁹² *ibid*

⁹³ Cyber Security Act No. 3 of 2025

discovery increases the possibility of confining an attack and minimizing systemic damage. The Act takes cyber governance obligations very seriously, as evidenced by the fact that failing to report such incidents is criminalized.

The Act also empowers the Agency to appoint cyber inspectors which the Act equips with broad investigation – related powers. Inspectors are empowered to, when armed with a warrant, access premises, demand for documentation and access electronic communication equipment and computer systems. They can search, seize equipment, or extract digital records.⁹⁴ These powers allow the Agency to respond quickly to cyber threats, but they also raise worries about possible abuse. Judicial monitoring is a crucial protection for the maintenance of proportionality and prevention of abuse of power.⁹⁵

Another major legislative aspect is the necessity that all cyber-security service providers obtain a license. Section 42⁹⁶ gives the Agency the authority to regulate cyber security service providers through licensing, guaranteeing conformity with professional standards and preventing unqualified enterprises from delivering crucial cyber-security services. This regulatory framework improves accountability and safeguards both public and commercial entities from ineffective or fraudulent cyber-security practices.

The Act also sets tools for national cyber security readiness, such as a Cyber-Security Risk Register and national cyber drills.⁹⁷ These procedures enable the government to regularly assess threats, improve incident response capabilities, and guarantee that institutions take a proactive approach to cybersecurity governance.

The Act in section 22, prohibits interception of communication but authorizes it as an exception in Sections 29 when facilitated by law enforcement officers with reasonable cause to believe that an offence has been committed, is likely to be committed, or is being committed. The section requires such law enforcement officer to, first, apply ex-parte to a judge for an interception of communication order.

⁹⁴ Section 18(4) Cyber Security Act No. 3 of 2025

⁹⁵ 'Handling of Digital Evidence' (UNODC Education for Justice (E4J), Cybercrime Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics) <https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html> accessed 18 November 2025.

⁹⁶ Cyber Security Act No. 3 of 2025

⁹⁷ Section 19 and 20 Cyber Security Act No. 3 of 2025.

Section 30 authorizes law enforcement officers to facilitate interception of communication without a Court order where there is reasonable cause to believe that such interception may avert bodily harm, death, damage to property or loss of finances by banks, financial institutions, account holders or beneficiaries of funds and that applying for the Court order was, in the circumstances, not practicable.

The law enforcement officer is, in the above situation, required to swear and submit to a judge an affidavit outlining the circumstances and other facts of the interception.

The Cyber Security Act⁹⁸ establishes a strong institutional and regulatory framework, considerably improving Zambia's ability to prevent and manage cyber threats. Its performance will depend on adequacy of relevant finances, inter-agency cooperation, technical expertise, and ongoing assessment to accommodate emerging technology.

3.1.3 CYBER CRIMES ACT, NO. 4 OF 2025

The Cyber Crimes Act⁹⁹ complements the Cyber Security Act by criminalising conduct that threatens the integrity, confidentiality and availability of computer systems and data. It modernises Zambia's criminal law by defining cyber-crime offences in forms that reflect global developments in digital criminal behaviour.

Unauthorized access is one of the most serious violations of the Act. Section 3 of the Act¹⁰⁰ criminalizes unauthorized access to computer systems. This offence extends to infringing security measures and accessing or monitoring a computer or computer system.

Section 4¹⁰¹ includes the charge of illegal data interference, which complements unauthorised access. This rule makes it illegal to change, delete, deteriorate, or suppress computer data without authorization. Data interference is a prevalent characteristic of white-collar cybercrime, especially in internal corporate fraud, in which staff manipulate financial records to conceal embezzlement. It is also fundamental to ransomware

⁹⁸ Ibid

⁹⁹ No. 4 of 2025

¹⁰⁰ Ibid

¹⁰¹ Cyber Crimes Act, No. 4 of 2025

assaults, which encrypt or destroy data. By criminalizing such behaviour, the Act acknowledges the economic and institutional harm caused by data manipulation in digital contexts.

A significant crime is computer-related fraud - specified in Section 12 of the Act.¹⁰² This rule applies to those who intentionally input, edit, or manipulate electronic data so as to cause the manipulated and now inauthentic data to be considered or acted on by another person as if it were authentic. The crime specifically covers digital fraud schemes such as accounting data or software manipulation, fraudulent electronic invoice fabrication, and digital financial record tampering. This is a substantial improvement over previous legal systems, particularly the Penal Code,¹⁰³ which lumped all fraud – digital and otherwise together attracting the same sanction.

The Act¹⁰⁴ also criminalizes cyber extortion in Section 13, identity theft in Section 14 and child pornography in Section 15. Identity theft is becoming more common in mobile money fraud and SIM-card-related frauds. Cyber extortion, which may involve threats to reveal or destroy information until a demand is satisfied, illustrates the increasing usage of ransomware and blackmail in digital environments.

Section 8 criminalizes the introduction of malware into a computer because of its destructive potential and regularity of usage in facilitating financial and other crimes or disrupting systems.

Section 10 of the Act under discussion¹⁰⁵ prohibits recording of a private conversation without the consent of parties to such conversation. The section, however, authorizes law enforcement officers to record such a conversation apparently without judicial authority where there is reasonable suspicion of a threat to life, an imminent threat of serious violence to a person, a threat of substantial damage to property or that an offence under any written law may be committed.

¹⁰² Ibid

¹⁰³ Chapter 87 of the Laws of Zambia

¹⁰⁴ Cyber Crimes Act, No. 4 of 2025

¹⁰⁵ ibid

According to Section 27(1), a law enforcement officer may, with a warrant, enter any premises to search and seize a computer or computer system, where a computer or computer system contains material -

- (a) or evidence necessary in proving an offence; or
- (b) that has been acquired by a person as a result of an offence.

According to Section 27(2,) a law enforcement officer who is undertaking a search under this Act may, where the law enforcement officer has reasonable grounds to believe that the data sought is stored in another device, computer or computer system or part of it, and such data is lawfully accessible from another device, computer or computer system, extend the search or access to the other device, computer or computer system.

While these powers are critical for conducting effective cybercrime investigations, they require to be critically analysed for purposes of ascertaining whether they fall foul of the constitution by not being accompanied by adequate safeguards against overreach and undue derogation of constitutionally guaranteed rights. Courts will consequently play an important role in articulating procedural safeguards, establishing admissibility rules, and enforcing conformity with constitutional rights.

The Cyber Crimes Act operates within a larger statutory framework. For example, offenses under the Penal Code¹⁰⁶, such as obtaining money under false pretenses or conspiring to defraud, nevertheless apply to digital fraud schemes. The Forfeiture of Proceeds of Crime Act¹⁰⁷ allows courts to confiscate digital assets earned through cybercrime. The Prohibition and Prevention of Money Laundering Act¹⁰⁸ strengthens the prosecution of cyber-enabled financial crimes by criminalizing the conversion or transfer of unlawful digital gains.

¹⁰⁶ The Penal Code Act, Cap 87 of the Laws of Zambia

¹⁰⁷ Forfeiture of Proceeds of Crime Act No 19 of 2010

¹⁰⁸ The Anti-Money Laundering Act No 14 of 2001

The Cyber Crimes Act¹⁰⁹ was meant to establish a modern, comprehensive, and technologically responsive framework for criminalizing computer wrongdoing. It criminalizes a whole host of activities in its quest to combat cyber-crime.

The Constitution¹¹⁰ provides an overarching normative foundation for the interpretation and application of cyber legislation, particularly in terms of privacy, expression, property, and fair trial rights. The Cyber Security Act,¹¹¹ seeks to create an institutional and regulatory framework for national cyber governance by strengthening critical information infrastructure protection, regulating cyber-security service providers, and improving national preparedness. Its institutional approach represents a change toward proactive cyber governance in response to the nation's increasingly sophisticated digital challenges.

The Cyber Crimes Act¹¹², broadens Zambia's criminal code to encompass modern cyber-enabled crimes like hacking, data interference, digital fraud, identity theft, and virus distribution. Its implementation greatly enhances Zambia's ability to pursue technologically advanced offenses.

Together, the two Acts seek to provide a robust and modern legal foundation for combating cybercrime, and fostering cyber security and need arises to critically analyse their adequacy, effectiveness and appropriateness. As cyber risks evolve, Zambia's legal system must remain responsive, balanced, and firmly based on constitutional values.

3.2 CONCLUSION

This chapter explored the legal framework governing cyber-crime, cyber security and constitutional rights in Zambia. The Chapter begun looking at key and relevant legal provisions from the Republican Constitution and how they find relevance in cyber security and combatting of cyber-crime. The chapter then extensively discussed the Cyber Security Act before turning to the consideration of the Cyber Crimes Act.

¹⁰⁹ No. 4 of 2025

¹¹⁰ The Constitution of Zambia (Amendment) Act 2016

¹¹¹ No. 3 of 2025

¹¹² No. 4 of 2025

The chapter, thus, provide an overview of and run – through the legal framework governing cyber security, cyber-crime and constitutional rights. This prepares the reader for the critical analysis of the above framework in the following chapter.

CHAPTER FOUR

CRITICAL ANALYSIS OF THE APPROPRIATENESS OF THE CYBER SECURITY ACT AND CYBER CRIMES ACT IN UPHOLDING CONSTITUTIONAL RIGHTS: LESSONS FROM INTERNATIONAL BEST PRACTICE

4.0 INTRODUCTION

This chapter critically analyses the appropriateness of the Cyber Security Act and the Cyber Crimes Act in achieving their intended goals while safeguarding constitutional rights, drawing on lessons from international best practice. It begins by examining the objectives of the Cyber Security Act 2025 and the Cyber Crimes Act 2025, followed by an assessment of provisions that are inappropriate in meeting the goals of the legal framework or that may jeopardize constitutional rights – considering whether the Acts have adequate safeguards against such jeopardy.

The above will extend to an evaluation of the institutional design and autonomy of Cyber Security Agency as well as how appropriately couched provisions in the two pieces of legislation are. The chapter will draw best practice from regional and international instruments before concluding.

4.1 GENERAL OVERVIEW OF GOALS OF THE CYBER SECURITY ACT 2025 AND CYBER CRIMES ACT 2025 AND GENERAL SHORTCOMINGS RAISED BY CRITICS.

4.1.1 The Cyber Crimes Act

The Cyber Crimes Act, in its preamble, indicates that it was enacted to provide for offences relating to computers and computer systems; provide for the protection of persons against cyber-crimes; provide for child online protection; and provide for matters connected with, or incidental to, the foregoing. It was, thus, enacted to protect computers, cyberspace and persons using computers – including children – against cyber-crimes.

The Cyber Crimes Act, as one observer points out, "introduces provisions against emerging cyber offences including identity-related fraud, cyber terrorism, attacks on CII [critical information infrastructure], and non-consensual sharing of intimate content¹¹³."

Critics, however, indicate that some provisions outlining crimes under the Cyber Crimes Act are vaguely worded which unduly expands the scope of the offences. Criticism has also been raised relating to the alleged lack of adequate safeguards in the face of wide powers accorded to law enforcement officers.

4.1.2 Cyber Security Act

The Cyber Security Act on the other hand was enacted to provide for cyber security in the Republic; establish the Zambia Cyber Security Agency and provide for its functions; provide for the regulation of cyber security service providers; provide for the constitution of the Zambia Cyber Incident Response Team and provide for its functions; provide for the constitution of sectoral cyber incident response teams; continue the existence of the Central Monitoring and Coordination Centre; provide for the designation, protection and registration of critical information and critical information infrastructure; repeal and replace the Cyber Security and Cyber Crimes Act, 2021; and provide for matters connected with, or incidental to, the foregoing.¹¹⁴

¹¹³ Global Network Initiative. GNI Statement on Zambia's New Cyber Laws: A Blow to Freedom of Expression and Privacy, <https://globalnetworkinitiative.org/gni-statement-on-zambias-new-cyber-laws-a-blow-to-freedom-of-expression-and-privacy/> Accessed 21/11/2025

¹¹⁴ Preamble of the Cyber Security Act No. 3 of 2025

The Cyber Security Act may be commended for creating a separate national cyber agency and incident response teams which can help to centralize expertise and better foster cyber security and combat cyber-crime. The Act's provisions for licensing cyber-security service providers and implementing security audits have the potential to elevate the industry. Requiring financial institutions and telecoms to retain call data (section 40) and cooperate with investigations can help solve crimes. If implemented with care, the Acts could enhance Zambia's cyber preparedness, child protection online, and prosecution of digital offences (such as fraud and extortion). These measures are arguably *"aligned with efforts to improve digital resilience"*.¹¹⁵

Critics may, however, point to the fact that powers accorded to cyber inspectors may be too broad and safeguards against over derogation from constitutional rights are grossly inadequate.

4.2 KEY SPECIFIC CONSTITUTIONAL RISKS AND CRITIQUE

Despite the objectives, both statutes present significant constitutional issues, particularly with relation to oversight, vagueness, and overbreadth. Strong liberties are guaranteed by the Zambian Constitution: Article 17¹¹⁶ safeguards privacy (no search of person or property without consent or law) and Article 20(1)¹¹⁷ enshrines freedom of expression (including the right to receive and impart information). Any statutory restriction must not be excessively ambiguous and must be "reasonably required" in the interests of defense, public safety, order, morality, or the rights of others. Numerous clauses in this case go against those ideals.

First, both the Cyber Crimes Act¹¹⁸ and the Cyber Security Act¹¹⁹ employ broad terminology that undermines legal clarity. For example, "critical information" refers to nearly any data relevant to public safety, public health, economic stability, or even "critical cyberspace sustainability." Critics argue that this expansion provides the state "carte

¹¹⁵ *ibid*

¹¹⁶ *Constitution of Zambia (Amendment) Act, 2016* (Act No 2 of 2016), read together with the *Bill of Rights* contained in the *Constitution of Zambia (1991, as amended)*.

¹¹⁷ *Ibid*

¹¹⁸ Act No. 4 of 2025

¹¹⁹ Act No. 3 of 2025

blanche to regulate practically all information." Similarly, the term "law enforcement officer¹²⁰" has, in both Acts, been enlarged to encompass people appointed by the President, presenting accountability difficulties.¹²¹

Section 22 of the Cyber Crimes Act prohibits the use of a computer or computer system to disseminate data that subjects another to embarrassment, knowing the same to be false. It is unclear why the above should be a crime when there is adequate remedy under civil law. It, of course may be argued that such action is a crime offline as well but the same question is raised with the relevant provisions.

According to GNI, the combination of undefined terminology such as "false information" and "public embarrassment" can lead to arbitrary enforcement.¹²² Such vagueness breaches the idea of legality. According to Zambia's Constitution¹²³, "no person shall be convicted of a criminal offence unless that offence is defined and the penalty is prescribed in a written law." Overbroad statutes allow for the de facto formation of new offenses by governmental fiat, which violates the rule of law.

Second, both Acts consolidate vast surveillance powers with few safeguards. For example, Section 39 of the Cyber Security Act¹²⁴ compels all internet and telecom companies to establish full-time monitoring and interception systems. While it may be necessary for instances when lawful interception is required to be effected, the above does not come with adequate safeguards. Opponents fear that "these provisions can enable real-time surveillance of private communication" as well as "a grave threat to

¹²⁰ Section 2 in both the Cyber Security Act as well as the Cyber Crimes Act.

¹²¹ Edrine Wanyama, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 19 November 2025.

¹²² Global Network Initiative, 'GNI Statement on Zambia's New Cyber Laws: A Blow to Freedom of Expression and Privacy' (2021) <https://globalnetworkinitiative.org/gni-statement-on-zambias-new-cyber-laws-a-blow-to-freedom-of-expression-and-privacy/> accessed 19 November 2025.

¹²³ *Constitution of Zambia (Amendment) Act, 2016* (Act No 2 of 2016), read together with the *Bill of Rights* contained in the *Constitution of Zambia (1991, as amended)*.

¹²⁴ Act No. 3 of 2025

citizens' privacy.¹²⁵ The absence of adequate judicial and other oversight may violate constitutional values of privacy, proportionality, and accountability.

The above is stated considering that requiring service providers to have interception – ready systems potentially effectively channels all private conversations into the government's hands where the procedure of acquiring lawful authority to intercept is not rigorous with judicial and other safeguards as is the case in Zambia as may be observed below.

Section 21¹²⁶ designates the "Central Monitoring and Co-ordination Centre" as "the sole facility" for lawful interception. However, the public is not aware of the location of this facility and neither are employees or at least positions there known. A rogue government may pack the centre with party cadres to illegally monitor and intercept communication and no one will have any suspicion because they do not know where the centre is or who is the head and who are employees there.

Section 29 of the Cyber Security Act¹²⁷, requires law enforcement personnel to seek a judge's warrant before intercepting communications. On its face, judicial authorization appears to be consistent with Article 17 of the Constitution,¹²⁸ which protects the privacy of correspondence and prohibits unreasonable searches. However, Section 29¹²⁹ drops the requirement for Attorney General's consent prior to obtaining an interception order from a High Court Judge which was provided for in the Cyber Security Act's 2021 predecessor. The earlier approach required the Attorney General to assess interception applications for legality and need before they reached the judiciary, resulting in a dual layer of protection against abuse. Removing this precaution leaves judges as the sole gatekeepers, increasing the likelihood of "rubber-stamping" interception requests, especially given the broad and weakly defined grounds for interception.

¹²⁵ Wiriranai Brilliant Masara, 'How Zambia's Cyber Laws Rebrand Repression' (Journal of Democracy, August 2025) <https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-laws-rebrand-repression/> accessed 19 November 2025.

¹²⁶ Ibid

¹²⁷ Ibid

¹²⁸ *Constitution of Zambia (Amendment) Act, 2016* (Act No 2 of 2016), read together with the *Bill of Rights* contained in the *Constitution of Zambia (1991, as amended)*.

¹²⁹ Act No. 3 of 2025

Academic work on surveillance governance emphasizes the importance of multi-institutional monitoring and independent review systems to prevent politically motivated or disproportionate intrusions into private communications. Restoring the Attorney General's oversight would thus strengthen constitutional compliance by ensuring that interception powers are used only when strictly necessary, legally justified, and proportionate - key requirements under Zambian constitutional law and international human-rights standards.

The Zambian Supreme Law (Article 17)¹³⁰ prohibits searches without a clear justification, adequate oversight, robust safeguards and absolute necessity. However, the Cyber Security Act in Section 30 and the Cyber Crimes Act in Section 10 grant interception powers where there is reasonable belief that property may be damaged. The problem is that the Acts do not place a threshold of the kind, nature or quantum of property meaning any property and undergoing or potentially undergoing any quantum of damage - whether minor or not can trigger authority to legally intercept communication.¹³¹

Section 22 of the Cyber Crimes Act¹³² criminalizes using a computer system to publish or transmit electronic data that is obscene, vulgar, lewd, lascivious or indecent with intent to humiliate, harass or cause substantial emotional distress to another person.

The clause is written in broad and subjective language, with the potential to criminalize lawful public conversation, political criticism, satire, and journalistic commentary. Article 20 of the Constitution¹³³ states that any restriction on freedom of expression in a democratic society must be reasonable, explicitly defined, and proportionate. Section 22¹³⁴ fails this test because phrases like "vulgar" may totally be subjective and do not establish an objective basis for law enforcement. Academic commentary on digital speech regulation demonstrates that criminalizing mere insult or cause of emotional distress

¹³⁰ *Constitution of Zambia (Amendment) Act, 2016* (Act No 2 of 2016), read together with the *Bill of Rights* contained in the *Constitution of Zambia (1991, as amended)*.

¹³¹ Thomas Katuma Malama (IT Law Lecturer University of Lusaka) 4th year Information Technology Law Lecture Notes 2025.

¹³² Act No. 4 of 2025

¹³³ *Constitution of Zambia (Amendment) Act, 2016* (Act No 2 of 2016), read together with the *Bill of Rights* contained in the *Constitution of Zambia (1991, as amended)*.

¹³⁴ Act No. 4 of 2025

violates democratic free-speech principles, and the African Court on Human and Peoples' Rights has similarly noted that criminal defamation or insult – related charges - especially against political leaders impose an undue burden on expression.¹³⁵ Thus, Section 22 creates a direct constitutional risk – authorizing criminal sanctions for conduct that should only be subject to civil remedies, thereby discouraging public debate, investigative reporting, and civil-society activism.

4.3 SPECIFIC CRITIQUE OF FREEDOM OF EXPRESSION – RELATED PROVISIONS

The **Cyber Crimes Act** includes several clauses that, as written, significantly limit free expression. Most significantly, Section 22 criminalizes seemingly innocent expressions. It prohibits using a computer to publish anything "obscene, vulgar, or lewd" with the goal to "humiliate or harass another person".¹³⁶ Sending a "false statement...which causes damage to reputation" or exposing a person to "public ridicule, hatred, or contempt" is an offense. The phrases "humiliate," "harass," and "false information" are not defined in the Act and are fundamentally subjective. In practice, journalists, activists, and regular residents might face prosecution for lawfully criticizing public authorities or exposing humiliating information. According to one study, the vagueness in this case allows authorities to "target dissenting journalists, opposition members, and civil society activists," suppressing online conversation.¹³⁷

Equally concerning is the Act's restoration of criminal defamation in cyberspace. President Hichilema's administration had previously eliminated the colonial-era criminal defamation of the President, promoting free expression.¹³⁸ However, the new Act criminalizes any false statement that harms reputation. In essence, slander has become a cybercrime once again. This violates regional norms, as the African Commission has frequently called on states to remove criminal defamation laws, calling them as "a serious

¹³⁵ African Court on Human and Peoples' Rights <https://share.google/Oaf2uaEJ1LjHy1s8Z> Accessed 21/11/2025

¹³⁶ Wiriranai Brilliant Masara, 'How Zambia's Cyber Laws Rebrand Repression' (Journal of Democracy, August 2025) <https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-laws-rebrand-repression/> accessed 19 November 2025.

¹³⁷ *ibid*

¹³⁸ *ibid*

interference with freedom of expression".¹³⁹ Zambia runs the risk of arbitrary prosecutions if it reverses this change. Indeed, section 22's prison penalties for "false information" mean that any activist who spreads an unpleasant rumor may face criminal charges, even if there is no malice involved. Such content-based offenses are precisely the types that Article 20 of the Constitution¹⁴⁰ requires to be "reasonably justifiable in a democratic society". The justifications are vague, and the prohibitions are not tightly tailored to legitimate goals such as national security or public order.

Other speech-related provisions also cause worry. Section 23 of the Cyber Crimes Act¹⁴¹ prohibits sending communications that encourage violence or hatred against a tribe (a type of cyber-terrorism). While limiting hate speech is a worthy goal, the language is broad and covers "reawakening tribal or racial divisions". Without precise criteria, this could lead to political discourse on ethnicity or history. Furthermore, Section 24 of the same Act¹⁴² criminalizes any internet statement that is likely to cause another person "emotional distress". This introduces a broad harassing charge that might be used to muzzle critics. Zambia's constitutional heritage protects even controversial speech: "opinions" and the freedom to receive information are explicitly protected, with the exception of certain constraints (national security, for example). The Cyber Crimes Act's FOE provisions go far beyond constitutionally permissible limitations, ultimately replacing free discourse with an environment of terror. In short, the Acts prohibit a wide range of expression on unclear grounds. They convert civil wrongs (defamation, harassment) into broad criminal offenses with prison sentences, undermining Zambia's own Bill of Rights and contradicting the spirit of reform.¹⁴³

¹³⁹ African Commission on Human and Peoples' Rights (ACHPR), '*Resolution on Repealing Criminal Defamation Laws in Africa (ACHPR/Res.169(XLVII))*' <https://achpr.au.int/en/adopted-resolutions/169-resolution-repealing-criminal-defamation-laws-africa-achpres169xlvii> accessed 19 November 2025.

¹⁴⁰ Constitution of Zambia (Amendment) Act, 2016 (Act No 2 of 2016), read together with the *Bill of Rights* contained in the *Constitution of Zambia (1991, as amended)*.

¹⁴¹ Act No. 4 of 2025

¹⁴² *ibid*

¹⁴³ Wiriranai Brilliant Masara, '*How Zambia's Cyber Laws Rebrand Repression*' (Journal of Democracy, August 2025) <https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-laws-rebrand-repression/> accessed 19 November 2025.

4.4 INSTITUTIONAL DESIGN: INDEPENDENCE OF THE CYBER SECURITY AGENCY

Section 3 of the Cyber Security Act¹⁴⁴ establishes the Zambia Cyber Security Agency "in the Office of the President" with "general direction" from him. This design is constitutionally and normatively problematic. The Agency has significant regulatory and surveillance powers, but it reports directly to the head of the executive. Section 5 of the same Act¹⁴⁵ empowers the President to appoint the Director-General. The Agency's responsibilities include evaluating security measures surrounding Critical Information and Critical Infrastructure, co - ordinating national cyber security responses and licensing Cyber Security Service Providers. This concentration of authority undermines the fundamental principles of separation of powers and independent oversight. In contrast, other Zambian monitoring authorities such as the Information and Communication Technology Authority and Independent Broadcasting Authority have statutory independence though reporting to the Minister and Parliament through submission of Annual Reports. Here, political influence is built in with the Agency even directly "advising the President on matters relating to cyber security," thereby blurring the lines between policymaking and enforcement.¹⁴⁶

Legal experts have expressed concern that this arrangement "undermine[s] the agency's independence and increases the risk of political interference in its operations."¹⁴⁷ Without parliamentary oversight, the Agency's scope of power and influence is virtually unmonitored. In essence, the President's office determines who is monitored or prosecuted under these laws. This is contrary to constitutional values: the President has no particular authority to overturn legislative safeguards, and the Constitution requires that any restriction on rights be implemented in accordance with transparent legislation rather than arbitrarily. Indeed, the GNI has advised that Zambia "establish an

¹⁴⁴ Act No. 3 of 2025

¹⁴⁵ *ibid*

¹⁴⁶ Edrine Wanyama, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 19 November 2025.

¹⁴⁷ *ibid*

independent, autonomous Cyber Security Agency, free from executive control"¹⁴⁸, noting that present legislation reduces the Agency to a mere arm of the presidency.

The problem goes beyond nominal independence. The Agency's enabling Act lacks effective oversight measures. It establishes no compulsion for accountability to the legislature through submission of reports as is ordinarily the case. In contrast, strong governance models (and Zambia's constitutional spirit of accountability) would necessitate at least multi-stakeholder scrutiny. Placing this powerful body under direct presidential control violates the implicit balance of power. For example, if an opposition leader suspects improper surveillance, under current law, the President effectively polices himself. This is against the spirit of Article 18(1) of the Constitution¹⁴⁹, which requires impartial adjudication by an independent body. In conclusion, Section 3's institutional architecture is flawed. In order to prevent the executive from abusing its substantial powers, the Agency should be reorganized with statutory independence while being subject to Parliament for accountability's sake.

The Cyber Crimes Act in Section 10 authorizes a law enforcement officer to record a private conversation where such officer has reasonable belief that there is -

- (i) a threat to life or an imminent threat of serious violence to a person;
- (ii) a threat of substantial damage to property; or
- (iii) an offence under any written law that may be committed.

The above provision is, however, in direct contradiction to Section 29 of the Cyber Security Act which necessitates a Court Order to be obtained prior to such recording which, by definition, qualifies to be designated as "interception."

¹⁴⁸ Global Network Initiative, 'GNI Statement on Zambia's New Cyber Laws: A Blow to Freedom of Expression and Privacy' (2021) <https://globalnetworkinitiative.org/gni-statement-on-zambias-new-cyber-laws-a-blow-to-freedom-of-expression-and-privacy/> accessed 19 November 2025

¹⁴⁹ *Constitution of Zambia (Amendment) Act, 2016* (Act No 2 of 2016), read together with the *Bill of Rights* contained in the *Constitution of Zambia (1991, as amended)*.

The above provision in the Cyber Crimes Act goes against the Constitution in that it does not provide adequate safeguards against undue derogation from rights guaranteed by under the Constitution.

4.5 INTERNATIONAL AND REGIONAL BEST PRACTICE LESSONS

Zambia's cyber laws should ideally comply with regional and international human rights standards. The African Charter on Human and Peoples' Rights (ACHPR) protects free expression (Article 9) and international bodies have consistently pushed states to decriminalise defamation. As other states, Zambia is obliged by these instruments which requires them to ensure their legislation is in accord with them and declarations of international bodies which specifically state that criminal defamation "constitutes a serious interference with freedom of expression". Similarly, the African Declaration of Principles on Freedom of Expression and Access to Information (2002) seeks to foster freedom of expression which loosely worded provisions in legislation infringes. Zambia risks breaking away from the regional norm by providing for content-based speech charges.¹⁵⁰

Best practice in cybersecurity law (based on African Union and UN recommendations) emphasizes clear definitions, necessity, and oversight. For example, the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) asks states to strike a balance between security and rights. Article 25(3) of the Convention provides:

"In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others."

¹⁵⁰ African Commission on Human and Peoples' Rights, 'Resolution on Repealing Criminal Defamation Laws in Africa (ACHPR/Res.169(XLVII))' <https://achpr.au.int/en/adopted-resolutions/169-resolution-repealing-criminal-defamation-laws-africa-achpres169xlvii> accessed 19 November 2025.

According to CIPESA, Zambia should align its laws with "regional and international human rights standards, including the African Charter" and the AU Convention on Cybercrime.¹⁵¹

According to the UN Special Rapporteur on Freedom of Expression, states should repeal any law that criminalizes or unduly restricts expression, avoid heavy-handed viewpoint-based regulation or that impose disproportionate sanctions but should ensure transparency, accountability and adequate oversight of interception of communication and other acts that have potential of limiting constitutional rights including detailed reports to an independent body.¹⁵²

Security laws must be as limited as possible in accordance with constitutional and human rights standards. Governments throughout the world are under increasing pressure to develop multi-stakeholder cyber-defence measures that preserve citizens' rights. In contrast, Zambia's approach, which combines broad definitions with little control, violates these principles. Regional entities (for example, the SADC Parliamentary Forum) have campaigned for cybersecurity rules that include adequate judicial authority for interceptions and exemptions for journalists. Zambia's laws currently do the reverse.¹⁵³

While Zambia's new cyber laws address legitimate digital security issues, their current form poses significant dangers to constitutional liberties, particularly the right to expression and privacy.

4.6 CONCLUSION

In this chapter, a critical analysis was undertaken to assess the appropriateness of the Cyber Security Act and the Cyber Crimes Act in achieving their intended goals while safeguarding constitutional rights, drawing on lessons from international best practice.

¹⁵¹ Edrine Wanyama, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 19 November 2025.

¹⁵² United Nations, A/HRC/38/35: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression <https://www.ohchr.org/en/documents/thematic-reports/ahrc3835-report-special-rapporteur-promotion-and-protection-right-freedom> Accessed 21 November 2025

¹⁵³ Global Network Initiative, 'GNI Statement on Zambia's New Cyber Laws: A Blow to Freedom of Expression and Privacy' (2021) <https://globalnetworkinitiative.org/gni-statement-on-zambias-new-cyber-laws-a-blow-to-freedom-of-expression-and-privacy/> accessed 19 November 2025.

The chapter began by examining the objectives of the Cyber Security Act 2025 and the Cyber Crimes Act 2025. It then assessed key provisions in the two pieces of legislation and whether they align with requirements of the Republican Constitution and international best practice.

The chapter noted that the two pieces of legislation do not achieve the goals for which they were enacted which include fostering a balance between combatting cyber-crime and fostering cyber security while upholding constitutionally guaranteed rights.

The following chapter will summarize this study, provide recommendations and provide the conclusion of this study.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.0 INTRODUCTION

This chapter's objective is summarising the contents and findings of the chapters of this study, provide recommendations and bring the study to its conclusion.

5.1 SUMMARY OF CHAPTERS

The purpose of this research was to critically analyse the Cyber Security and Cyber Crimes Acts in Zambia: examining the legal and institutional gaps in upholding constitutional rights while addressing emerging digital threats. The research, in chapter one, provided the introduction to the study, projected the problem statement, laid out the significance and scope of the study before delving into literature review. The chapter thereafter indicated the research methodology the study was going to adopt before winding up by conveying ethical considerations.

The research in Chapter Two examined the concepts, rationale, and constitutional implications of cybercrime and cybersecurity in Zambia within the context of the country's evolving digital landscape. The research began by defining cybercrime drawing from both Zambian legislation and international instruments such as the AU Malabo Convention. Noted was the fact that Cyber Crime was defined in the Cyber Crimes Act as crime committed in, by or with the assistance of, a simulated environment or state of connection

or association with electronic communications or networks including the internet.

The chapter also noted that cybersecurity may be defined as the technical, organisational, and legal and other measures employed to safeguard digital systems, emphasising its role in building trust, ensuring data protection, and supporting digital transformation. These definitions established the foundation for understanding the dual nature of cyberspace as both a catalyst for development and a source of new criminal vulnerabilities.

The chapter proceeded to explore the rationale behind Zambia's cybercrime and cybersecurity framework. It demonstrated that rising internet penetration, the proliferation of mobile devices, and the increasing sophistication of cyberattacks have collectively intensified the threat environment. The analysis highlighted incidents such as the Golden Top scam, the NAPSA data breach, and the compromise of the Bank of Zambia's social media accounts as evidence of the growing scale and complexity of cyber risks. The research also noted that cybercrime was driven by financial, ideological, and opportunistic motivations, and that Zambia's digital ecosystem is particularly attractive to transnational cybercriminals due to enforcement gaps and regional interconnectedness.

The chapter further examined the implications of cybercrime, showing that it threatens individuals, institutions, and the economy at large. It explained that financial losses, identity theft, and disruptions to critical infrastructure undermine public trust and hinder economic growth. The chapter also underscored Zambia's efforts to respond to these risks through regulatory reforms, institutional strengthening, participation in regional conventions, and public-private collaboration in cybersecurity initiatives.

The chapter later discussed the constitutional rights that frame Zambia's response to cybercrime and cybersecurity. It analyzed the right to due process of the law, right to privacy and freedom of expression under Articles 17, 18 and 20 of the Constitution, respectively, examining their relevance to digital regulation. The research showed that although cyber laws aim to enhance security, they must operate within constitutional safeguards, particularly regarding search warrants and data interception. Ongoing legal challenges by civil society and scrutiny from international observers were presented as indicators of the need for clearer legal definitions, stronger oversight mechanisms, and safeguards against excessive surveillance.

Through these discussions, Chapter Two illustrated that Zambia's approach to cybercrime and cybersecurity was shaped by both escalating digital threats and the imperative to uphold constitutional liberties. The analysis emphasized that while robust cyber governance is essential for national security and economic resilience, it can only be effective and legitimate when balanced with transparency, adequate judicial oversight, and respect for fundamental rights in the digital age.

In chapter three, the research explored the legal framework governing cyber-crime, cyber security and constitutional rights in Zambia. The chapter began by outlining the foundational role of the Constitution and demonstrating how its guarantees, particularly the rights to privacy, freedom of expression, property, and fair trial, shaping the limits within which cyber legislation must operate. This constitutional context established the normative baseline for assessing the legality, legitimacy, and scope of State action in the digital sphere.

The chapter then explored the Cyber Security Act, No. 3 of 2025, highlighting its institutional and regulatory focus. It demonstrated that the Act sought to strengthen national cyber governance by introducing measures for the protection of critical information infrastructure, establishing a licensing regime for cyber-security service providers, and empowering the Zambia Cyber Security Agency with oversight and investigative authority. The discussion underscored that while these mechanisms were designed to enhance cyber resilience, their implementation required close attention to judicial supervision and procedural safeguards to avoid disproportionate intrusions into constitutionally protected rights.

The analysis subsequently turned to the Cyber Crimes Act, No. 4 of 2025, which, it was observed, criminalized a wide spectrum of technologically enabled activities including unauthorized access, data interference, digital fraud, identity theft, and the dissemination of malware. The research showed that the Act modernized Zambia's criminal law by aligning domestic offences with international cybercrime trends. The chapter illustrated that Zambia's legal framework had undergone significant reform to address the rising complexity and sophistication of cyber threats. The chapter, at the same time, demonstrated that effective cyber governance depended not merely on the existence of

legislation but on its constitutional conformity, clarity, procedural safeguards, and practical enforceability.

Overall, the discussions in this chapter provided a structured overview of the statutory and constitutional architecture underpinning cybersecurity and cybercrime regulation in Zambia. This analysis set the stage for the critical assessment that followed in the next chapter, which evaluated the adequacy, effectiveness, and appropriateness of the 2025 Acts in light of evolving cyber risks and constitutional imperatives.

Chapter Four critically examined the extent to which the Cyber Security Act and the Cyber Crimes Act of 2025 achieved their intended objectives while upholding Zambia's constitutional guarantees. It demonstrated that although the Acts sought to modernize the country's digital governance framework, by addressing emerging cyber offences, enhancing institutional coordination, and improving investigative capacities, they simultaneously introduced significant constitutional, structural, and rights-based concerns. The chapter began by outlining the Acts' stated goals taking note that measures such as licensing regimes, incident-response structures, and obligations imposed on service providers could, if carefully implemented, strengthen national cyber preparedness and digital security.

The analysis then exposed substantial constitutional risks arising from vague definitions, expansive offence categories, and broadly framed surveillance powers. Provisions with widely worded vague terms including "critical information," and "public embarrassment" were shown to undermine the principle of legality and create opportunities for arbitrary enforcement. The chapter further highlighted weaknesses in the interception regime, noting that the broad emergency interception of communication – related powers, and the removal of multi-layered oversight, particularly the former role of the Attorney-General, diminished essential safeguards guaranteed under the Constitution. These shortcomings were shown to heighten the likelihood of disproportionate intrusions into private communications and weaken judicial scrutiny.

A specific critique was that provisions that criminalized insult-based offences, had vague terminologies and broad prohibitions jeopardized the freedom of expression. The chapter demonstrated that these clauses risked suppressing legitimate public debate, investigative journalism, and civic engagement, and diverged sharply from regional and

international human-rights standards.

The chapter further evaluated the institutional design of the Zambia Cyber Security Agency, showing that its placement within the Office of the President and the presidential appointment of its Director-General compromised its independence and created a high potential for political influence. The absence of parliamentary, adequate judicial, or multi-stakeholder oversight mechanisms compounded these concerns, placing the Agency at odds with established principles of accountability and good governance.

Chapter Four demonstrated that Zambia's challenge lay not in the absence of a cyber legislative framework but in the constitutional, institutional, and rights-related weaknesses embedded within it. Noted was the fact that ensuring that the Acts fulfilled their intended purpose required clearer definitions, restoration of independent oversight, stronger institutional safeguards, and alignment with regional and international human-rights standards.

5.2 RECOMMENDATIONS

It can be noted that while Zambia has enacted comprehensive cyber legislation to regulate digital conduct and enhance national security, the effectiveness and constitutional soundness of the Cyber Security Act and the Cyber Crimes Act remain undermined by vague offence definitions, weak oversight mechanisms, expansive surveillance powers, and institutional vulnerabilities. The challenges identified in Chapter Four, particularly the overreach of speech – related provisions, the concentration of executive power, ambiguous definitions, and inadequate safeguards for privacy and due process, demonstrate the urgent need for targeted legislative and institutional reforms. It is therefore recommended that specific amendments be undertaken to align Zambia's cyber laws with constitutional guarantees and international best practice.

Free Speech – Related Provisions

It is recommended that vague and overly broad speech-related offences be repealed to comply with the constitutional right to freedom of expression under Article 20.

Vague Definitions

Provisions that criminalize actions that lead to “public humiliation,” should be repealed and instead be relegated to civil law. In particular, the criminal defamation provision under section 22 of the Cyber Crimes Act should be eliminated, and the offence should be limited strictly to genuine threats of violence or intimidation. This approach would reflect authoritative guidance from the African Commission on Human and Peoples’ Rights, which calls for the decriminalisation of defamation and the substitution of civil remedies.

Independence of the Cyber Security Agency

Furthermore, it is recommended that the independence and oversight of the Zambia Cyber Security Agency be strengthened. Section 3 of the Cyber Security Act should be amended to remove the Agency from the Office of the President, as this arrangement compromises institutional autonomy and heightens the risk of politically influenced surveillance. The Agency should report to a Minister. In addition, the Agency should be mandated to publish regular transparency reports to Parliament detailing interception requests, incident-response activities, and compliance measures. All interception orders should be subject to prior judicial and Attorney General approval and persons whose communication was intercepted in vain receiving post-facto notification once investigations conclude. Such reforms are consistent with international recommendations emphasizing the need for accountability and transparency.

Judicial Oversight

In order to safeguard privacy rights under Article 17, it is recommended that judicial and legislative checks on surveillance be strengthened. All searches, seizures, and interceptions of communication should require prior warrant authorization, save for narrowly defined emergencies subject to immediate thorough judicial review. The law should expressly facilitate the knowledge by individuals of infringement of their constitutionally guaranteed rights and challenge of unlawful surveillance, while also ensuring that data collected through interception is not retained beyond what is strictly necessary and is destroyed upon the conclusion of criminal proceedings. These

safeguards would bring Zambia into compliance with regional standards calling for proportionate, accountable, and rights-respecting surveillance regimes.

Public Interest Exemptions

It is also recommended that the Acts should incorporate express public-interest exemptions for journalism, whistleblowing, and civic reporting to ensure that legitimate democratic discourse is not chilled. This will ensure that restrictions on expression satisfy the “reasonably required” test under Article 20 of the Constitution.

Procedural Safeguards

It is, furthermore, recommended that procedural safeguards be enhanced to prevent misuse of punitive cyber powers. Wiretap orders should be valid only for a month renewable only where absolutely necessary subject to strict judicial scrutiny. An independent parliamentary or multi-stakeholder oversight committee should be established to review interception logs, authorizations, and compliance records. Provisions should also require that individuals who are acquitted of cyber offences have their digital data restored and that all institutions handling personal data adhere to lawful collection, storage, and disposal standards. Such safeguards reflect international best practice, which stipulates that cybersecurity enforcement must respect privacy, freedom of expression, and due process.

Public Participation in Legislative Process

It is, finally, recommended that legislative amendments be developed through broad-based stakeholder consultation. Parliament should convene public hearings that involve civil society organizations, the media, ICT industry actors, digital rights advocates, and legal experts. At the same time, capacity-building programs should be institutionalized to ensure that judges, prosecutors, and law-enforcement officers understand constitutional rights and the principles of necessity and proportionality. Training officials to apply cyber laws within human-rights-compliant standards will ensure more consistent and constitutionally sound enforcement.

Implementing these recommendations has the potential of creating a clearer, more accountable, and constitutionally compliant cyber governance framework. By refining definitions, strengthening institutional independence, enhancing oversight, and promoting participatory law-making, Zambia will be better positioned to balance national security imperatives with the protection of fundamental rights in the digital age.

BIBLIOGRAPHY

STATUTES

The Constitution of Zambia, (Amendment) Act No. 2 of 2016

Cyber Security Act, No. 3 of 2025 (Zambia).

Cyber Crimes Act, No. 4 of 2025 (Zambia).

Zambia Information and Communications Technologies Act No. 15 of 2009

Forfeiture of Proceeds of Crime Act No 19 of 2010

The Anti-Money Laundering Act No 14 of 2001

The Electronic Communications and Transactions Act No 4 of 2021

The Penal Code Act Chapter 87 of the laws of Zambia

INTERNATIONAL AND REGIONAL CONVENTIONS

Council of Europe Convention on Cybercrime (Budapest Convention), 2001.

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014.

OTHER PUBLICATIONS

African Union, *African Union Convention on Cyber Security and Personal Data Protection* (adopted 27 June 2014, EX.CL/846(XXV)) <https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf> accessed 18 November 2025

Africa Defense Forum, '*Chinese Cyber Scam Bust Reveals Zambia's Efforts to Disrupt Online Fraudsters*' (ADF, 7 May 2024) <https://adf-magazine.com/2024/05/chinese-cyber-scam-bust-reveals-zambias-efforts-to-disrupt-online-fraudsters/> accessed 18 November 2025

Bowmans, '*Zambia: New Laws to Strengthen Cybersecurity and Cybercrime Capacities*' (Bowmans, 7 October 2025) <https://bowmanslaw.com/insights/zambia-new-laws-to-strengthen-cybersecurity-and-cybercrime-capacities/> accessed 18 November 2025

Digger Editor, '*The Hacking at NAPSA, BoZ Pose a National Security Risk*' (News Diggers, 27 July 2023) <https://diggers.news/opinion/2023/07/27/the-hacking-at-napsa-boz-pose-a-national-security-risk/> accessed 18 November 2025

Edrine Wanyama, '*Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights*' (CIPESA, 19 May 2025) <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/> accessed 18 November 2025

Freedom House, *Freedom on the Net 2024: Zambia* (Freedom House, 2024) <https://freedomhouse.org/country/zambia/freedom-net/2024> accessed 18 November 2025

Global Partners Digital, *How to Respect Privacy and Free Expression as a Tech SME in Zambia* (2018) 9 https://www.gp-digital.org/wp-content/uploads/2018/12/ZAMBIA_web.pdf accessed 18 November 2025

IBM, 'What Is Cybersecurity?' (IBM Think, n.d.) <https://www.ibm.com/think/topics/cybersecurity> accessed 18 November 2025

Jackie Jhala and Rabecca Banda, '*Zambia: Cyber Security and Cyber Crimes Act*' (Lex Africa, 29 April 2021) <https://lexafrica.com/2021/04/zambia-cyber-security-and-cyber-crimes-act/> accessed 18 November 2025

Kay-Lyne Wolfenden, 'LAZ Opposes Zambia's New Cyber Laws Over Rights Infringement' (TechAfrica News, 23 April 2025) <https://techafricanews.com/2025/04/23/laz-opposes-zambias-new-cyber-laws-over-rights-infringement/> accessed 18 November 2025

Michael Aaron Dennis, 'Cybercrime' (Encyclopaedia Britannica, updated 11 October 2025) <https://www.britannica.com/topic/cybercrime> accessed 18 November 2025

National Prosecution Authority, '20 Chinese Nationals and One Cameroonian Convicted in Major Cyber Crime Case' (NPA, 13 June 2024) <https://www.npa.gov.zm/index.php/2024/06/13/20-chinese-nationals-and-one-cameroonian-convicted-in-major-cyber-crime-case/> accessed 18 November 2025

Zambia, *Constitution* (1991, rev. 2016), art 1(1), Constitute Project https://www.constituteproject.org/constitution/Zambia_2016 accessed 18 November 2025

Bowmans, "Zambia: New Laws to Strengthen Cybersecurity and Cybercrime Capacities" (Bowmans, 7 October 2025) <https://bowmanslaw.com/insights/zambia-new-laws-to-strengthen-cybersecurity-and-cybercrime-capacities/> accessed 18 November 2025

CIPEsa, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPEsa, 19 May 2025) <<https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/>> accessed 13 November 2025.

Edrine Wanyama, 'Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights' (CIPEsa, 2025) <<https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/>> accessed 13 November 2025.

Emmanuel Kunda, 'Effectiveness of the Cyber Security Act in Combating Emerging Cyber Threats in Zambia' (ResearchGate, 2023).

G M Siampondo, M Sumbwanyambe and B Chansa, 'A Study on the Existing Cybersecurity Policies and Strategies in Combating Increased Cybercrime in Zambia'

(2023) 14 *Journal of Information Security* 294 <<https://doi.org/10.4236/jis.2023.144017>> accessed 13 November 2025.

G Sarkar and S K Shukla, 'Behavioral analysis of cybercrime: Paving the way for effective policing strategies' (2023) *Journal of Economic Criminology* <<https://www.sciencedirect.com/science/article/pii/S2949791423000349>> accessed 13 November 2025.

Global Network Initiative, 'Five Things to Know: Zambia's Cyber Crimes Act and Cyber Security Act' (ICNL, 2025) <<https://www.icnl.org/post/tools/five-things-to-know-zambias-cyber-crimes-act-and-cyber-security-act>> accessed 13 November 2025.

ICNL (International Center for Not-for-Profit Law), 'Five Things to Know: Zambia's Cyber Security Act 2025' (ICNL, April 2025) <<https://www.icnl.org/wp-content/uploads/Zambia-Five-Things-Cyber-Security-Act-2025-final.pdf>> accessed 13 November 2025.

INTERPOL, *Africa Cyberthreat Assessment Report 2025* (4th edn, June 2025) <https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf> accessed 13 November 2025.

INTERPOL, 'New INTERPOL report warns of sharp rise in cybercrime in Africa' (23 June 2025) <<https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-African-cybercrime>> accessed 13 November 2025.

Kay Lyne Wolfenden, 'LAZ Opposes Zambia's New Cyber Laws Over Rights Infringement' (TechAfrica News, 23 April 2025) <<https://techafricanews.com/2025/04/23/laz-opposes-zambias-cy-laws-over-rights-infringement/>> accessed 13 November 2025.

M&J Consultants, 'Zambia's New Cybercrime Law: Essential Knowledge for Entrepreneurs' (M&J Consultants, 2025) <<https://mjconsultants.co.zm/zambias-new-cybercrime-law-essential-knowledge-for-entrepreneurs/>> accessed 13 November 2025.

Michalsons, 'AU Convention on Cyber Security and Personal Data Protection | Malabo Convention' (Michalsons, 24 April 2023) <<https://www.michalsons.com/blog/au->

[convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281\>](#)
accessed 13 November 2025.

Patricia Nachilima, 'Challenges of Cybercrime Enforcement in Africa: The Case of Zambia' (Dissertation, University of Lusaka, 2024).

Wiriranai Brilliant Masara, 'How Zambia's Cyber Laws Rebrand Repression' (Journal of Democracy Online Exclusive, 2025) <<https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-laws-rebrand-repression/>> accessed 13 November 2025.

Appendix 1

CLEARANCE FORM



UNIVERSITY
of **LUSAKA**
Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

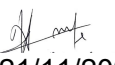
L400B / Dissertation II – DIRECTED RESEARCH (OBLIGATORY ESSAY)

RESEARCH CLEARANCE FORM

NAME: NTAZANA YAMBALA KANCHULE. STUDENT NUMBER: LLB20120299

**SUPERVISOR: Mr. THOMAS MALAMA TOPIC: A CRITICAL ANALYSIS OF THE CYBER
SECURITY ACT AND THE CYBER CRIMES ACT OF ZAMBIA: EXAMINING THEIR
APPROPRITENESS IN UPHOLDING CONSTITUTIONAL RIGHTS.**

Stage	Supervisor's Comments	Supervisor's Signature & Date	Student's Signature & Date
Research Proposal	The research proposal was reviewed and approved.	<i>TKmalama</i> 10/11/2025	<i>NTAZANA</i> 10/11/2025
Chapter 1 – Introduction	Approved following effecting of corrections including in literature in review and Research Methodology	<i>TKmalama</i> 12/11/2025	<i>NTAZANA</i> 12/11/2025
Chapter 2 –	Reviewed and approved after effecting corrections in numbering, logical flow of content and footnotes.	<i>TKmalama</i> 13/11/2025	<i>NTAZANA</i> 13/11/2025

Chapter 3 –	Reviewed and approved after corrections relating to the following were effected: Typos, wrong references to sections, and footnotes	<i>TKmalama</i> 15/11/2025	 15/11/2025
Chapter 4 –	Chapter was reviewed and approved following corrections including mis citation of legislation	<i>TKmalama</i> 21/11/2025	 21/11/2025
Chapter 5 – Conclusions & Recommendations	Reviewed and approved.	<i>TKmalama</i> 21/11/2025	 21/11/2025
Abstract, Table of Contents and Bibliography	Ran out of time to review	<i>TKmalama</i> 21/11/2025	 21/11/2025
First Draft			
Second Draft			
Final Draft	Reviewed and Approved minus Abstract, Table of Contents and Bibliography due to running out of time for submission	<i>TKmalama</i> 21/11/2025	 21/11/2025

****Please attach this form to the back of your dissertation at the end of the research, before submission via the Moodle e-learning platform***

Appendix 2

Plagiarism Report

