BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY

TOPIC

Challenges Faced By Law Enforcement Agencies In Combating Cybercrime: A Case Study Of Bindura District

BY

B220320B

Kuwaza Luke

SUPERVISOR: Mrs Gopo

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELOR OF BUSINESS ADMINSTRATION (HONOURS) DEGREE IN POLICE AND SECURITY STUDIES (BBA. PSS) OF BINDURA UNIVERSITY OF SCIENCE EDUCATION, FACULTY OF COMMERCE.

2025

APPROVAL FORM

Topic: Challenges faced by law enforcement agencies in combating cybercrime: A case study of Bindura District.

TO BE COMPLETED BY THE STUDENT

I certify that the dissertation meets the preparation guidelines as presented in the faculty guide and instruction for preparing dissertations.

 25/08/25

(Signature of Student) (Date)

TO BE COMPLETED BY THE SUPERVISOR

This dissertation is suitable for presentation to the faculty. Is has been checked for conformity with

 the faculty guideline. 25/08/25

(Signature of Supervisor) (Date)

TO BE COMPLETED BY THE DEPARTMENTAL CHAIRPERSON

I certify to the best of my knowledge that the required procedures have been fulfilled and the preparation criteria was met in this dissertation.

 (Signature of Chairperson) 25/08/25

(Date)

RELEASE FORM

Name of author Kuwaza Luke

Title of project Challenges being faced by law enforcement agencies in combating cybercrime:A case study of Bindura District

Year granted 2025

Permission is hereby granted to Bindura University of Science Education library to produce copies of this dissertation for scholarly and research only.

Signed 

(Author's signature)

Permanent address 864 Claverhill Bindura

DECLARATION

I, Kuwaza Luke solemnly declare that the information of this dissertation, prepared in partial fulfilment of the Bachelor of Business Administration Honours Degree in Police and Security Studies and submitted to the Department of Intelligence and Security, Faculty of Commerce at Bindura University of Science Education has not been presented, submitted or published in this nature or part. Previous works have been duly accredited and acknowledged properly

25/08/25

(Signature of Student) **(Date)**

DEDICATION

I dedicate this research study to my wife Fatimah Murimbika. Thank you for the love and support that helped me to achieve this feat.

ABSTRACT

The study looked into the challenges faced by law enforcement agencies in combating cybercrime in Bindura District. The study was guided by three theories namely: the Routine Activities Theory; the Social Learning Theory; and the Deterrence Theory to understand the dynamics behind cybercrime and how it can be managed. Literature from other authors was also presented, focusing on the global economic impact of cybercrime; international response to cybercrime; African regional perspectives; challenges of combating cybercrime; the effectiveness of the approaches in combating cybercrime; and strategies in combating cybercrime. The research design for this study was descriptive, aimed at providing a detailed account of the challenges that law enforcement agencies faced in Bindura District. Purposive convenience sampling was used to come up with the sample of 25 questionnaire respondents and 5 key informants from among the law enforcement agents responsible for cybercrime management in Bindura District. Descriptive statistical analysis was used to interpret data from tables and figures. Major findings included that law enforcement agents face a number of challenges in combating cybercrime including lack of specialized training; insufficient funding/resources; rapidly evolving cyber threats; jurisdictional limitations; difficulty in digital evidence collection; and lack of coordination with international agencies. The study also found out that: law enforcement agents in Bindura District face difficulties in obtaining digital evidence from tech companies; cybercrime cases are not always reported on time in Bindura District, which complicates efforts by law enforcement agents to respond to the crimes timeously and effectively; and Law enforcement personnel in Bindura District largely lack proper cybercrime training. In addition to that, the study found out that law enforcement agents in Bindura District struggled the most with the following cybercrimes: phishing; malware attacks; financial fraud; data breaches; hacking; and darknet and cryptocurrency crimes. The study recommended, among other recommendations that, the Government of Zimbabwe reforms cyber security policies to allow law enforcement agents to adequately deal with cybercrime; the Government of Zimbabwe collaborates with other nations in allowing for more international cooperation in handling cybercrime given that many of the cybercrimes are committed by people beyond the borders of Zimbabwe; law enforcement agencies such as the Zimbabwe Republic Police prioritise making cyber security training mandatory for all new law enforcement agents; and that the ZRP, in collaboration with other stakeholders, needs to carry out awareness campaigns to educate the public on cyber security and cybercrime.

ACKNOWLEDGEMENTS

I would like to thank God for giving me the strength and capacity to undertake this study. I went through several tests and sailed through. Hence I owe the Almighty thanks and appreciation. I am greatly indebted to my Supervisor Mrs Norah Gopo who worked tirelessly in giving direction to this study, challenging me with ideas that greatly assisted me in shaping this dissertation. I am grateful to her knowledge and guidance which helped me to remain focused even at times it would have been difficult to see the way. I am grateful to my classmates for the support and assistance they gave me to make this project successful. I am indebted to the law enforcement agents who took part in this research project for the cooperation and assistance they gave me in supplying answers to the research questions. Though last but surely not least, I am grateful to my family for their continued inspiration and support that pushed me to work hard and achieve more. I am grateful for their patience during times I could not be with them in order to concentrate on this study.

TABLE OF CONTENTS

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

APPENDIX **PAGE**

CHAPTER I

THE PROBLEM AND ITS SETTING

1.0 Introduction

The advent of technology and the internet has brought about unprecedented opportunities for economic growth, social connection, and access to information. However, this digital revolution has also given rise to a new wave of criminal activity: cybercrime. Cybercrime poses a significant threat to individuals, organizations, and nations, with the potential to compromise personal data, disrupt critical infrastructure, and undermine trust in technology. This proposal section covers the background of the study, statement of the problem, objectives of the study, research questions, limitations and delimitations of the study, significance of the study, assumptions of the study and background of the research.

1.1 Background to the Study

The rapid advancement of technology and the proliferation of the internet have ushered in an era of unprecedented opportunities for economic growth, social interaction, and access to information. However, this digital transformation has also facilitated a surge in criminal activities, particularly cybercrime, which poses a significant threat to individuals, organizations, and nations alike. Cybercrime encompasses a wide range of illicit activities conducted via the internet, including data breaches, identity theft, online fraud, and cyber attacks on critical infrastructure. The potential consequences of these crimes are severe, as they can compromise personal data, disrupt essential services, and erode public trust in technology and institutions.

Globally, cybercrime has emerged as a major threat to security and economic stability. The International Criminal Police Organization (INTERPOL) has classified cybercrime as a "major threat to global security," with estimated annual losses exceeding $1 trillion (Brenner, 2017). High-profile incidents, such as the 2017 Equifax data breach in the United States, which affected over 147 million individuals, underscore the pervasive nature of this issue (Morgan, 2018).

In Africa, the impact of cybercrime is increasingly pronounced, with many nations grappling with the challenges posed by cyber threats. For instance, South Africa has reported significant incidents, including a 2020 data breach at Experian that exposed the personal data of over 24 million

individuals (IT Web Africa, 2020). Similarly, Botswana faced a hacking incident in 2019 that resulted in substantial financial losses for its revenue service (BOCRA, 2019).

Zimbabwe is no exception to this trend, as the country has witnessed a rise in various forms of cybercrime, including hacking, phishing, identity theft, and online fraud. The increasing adoption of technology and internet connectivity in Zimbabwe has created fertile ground for cybercriminals to exploit vulnerabilities within individuals, businesses, and government institutions. Recent studies indicate that the retail sector has been particularly affected, with virus dissemination, hacking, and card fraud identified as prevalent forms of cybercrime (Mugari et al., 2023).

Despite the growing concern over cybercrime in Zimbabwe, law enforcement agencies face significant challenges in effectively combating these crimes. These challenges include a lack of specialized training, inadequate resources, and the rapidly evolving nature of cyber threats, which often outpace the capabilities of law enforcement. Consequently, cybercriminals can operate with relative impunity, highlighting the urgent need for a comprehensive examination of the obstacles faced by law enforcement agencies in Zimbabwe. This research aims to identify these challenges and explore potential strategies for enhancing cybercrime prevention, investigation, and prosecution efforts.

1.2 Problem Statement

Zimbabwe is facing a growing cybercrime crisis, with a significant increase in online fraud cases, cyber-attacks, and data breaches. Despite efforts to combat cybercrime, the country has experienced 25% rise in reported cybercrime incidents between 2020 and 2022 (Zimbabwe Cybersecurity Ministry, 2022), an estimated ZWL 1.3 billion (approximately USD 4 million) loss in the financial sector due to cybercrime in 2021 alone (Reserve Bank of Zimbabwe, 2021), 1 in 5 Zimbabweans (21%) falling victim to online scams, resulting in financial losses and compromised personal data (TechZim, 2022), a 30% increase in phishing attacks targeting Zimbabwean businesses and individuals in 2022 (Kaspersky, 2022), 60% of Zimbabwean organizations experiencing at least one cyber-attack in 2021, with 40% of those attacks resulting in data breaches (ITWeb Africa, 2022).

1.3 Aim of the study

To conduct a comprehensive examination of cybercrime law enforcement in Zimbabwe, identifying challenges, strategies, and outcomes. It seeks to understand the nature and scope of cybercrime in Zimbabwe and evaluate the effectiveness of current law enforcement efforts. The study will provide recommendations for improving cybercrime law enforcement in Zimbabwe, enhancing the safety and security of citizens, businesses, and government entities. By addressing the knowledge gap in cybercrime law enforcement, the study contributes to the development of effective strategies and programs to combat cybercrime in Zimbabwe

1.4 Objectives

- To identify the main challenges faced by law enforcement agencies in combating cybercrime.
- To determine the effectiveness of law enforcement agencies in addressing cybercrime.
- To determine types of cybercrime prevailing in Bindura district
- To propose strategies for improving the effectiveness of law enforcement agencies in combating cybercrime.

1.5 Research Questions:

1. What are the main challenges faced by law enforcement agencies in combating cybercrime?
2. How effective are the law enforcement agencies in combating cybercrime
3. What types of cybercrimes are prevailing in Bindura district?
4. What strategies can be implemented to improve the effectiveness of law enforcement agencies in combating cybercrime?

1.6 Significance of the study

This present study will address a critical knowledge gap in understanding cybercrime in Bindura district, Mashonaland Central in Zimbabwe. It seeks to contribute to the development of effective cybersecurity strategies, protecting Zimbabwe's economy, thereby supporting Zimbabwe's economic growth and national security. By addressing cybercrime, the study will help build trust in digital technologies, promoting their adoption and use in various sectors and the study's recommendations will help mitigate financial losses due to cybercrime. The study's findings will

also provide organizations with valuable insights to inform their cybersecurity investments and strategies. Organizations will identify and mitigate cybercrime risks, protecting their assets and reputation. By adopting effective cybersecurity measures, organizations can gain a competitive advantage in the market.

The study will contribute to the existing body of knowledge on cybercrime and cybersecurity, advancing the researcher's expertise. It will provide opportunities for the researcher to collaborate with stakeholders, expanding their professional network and the success will enhance the researcher's career prospects, opening up new opportunities in academia and industry. The study will demonstrate Bindura University's commitment to research excellence, enhancing its reputation and the findings will be shared with stakeholders, promoting knowledge transfer and collaboration between the university and industry. Lastly it will contribute to the development of cybersecurity research capacity at Bindura University, supporting future research initiatives.

1.7 Assumption of the study

The researcher assumes that Cybercrime is a significant threat to Bindura district in Mashonaland Central, Zimbabwe. Law enforcement agencies play a critical role in combating cybercrime. It also assumes that current cybercrime law enforcement efforts in Zimbabwe are inadequate. The methodology will be rigorous and robust and data collected will be accurate and reliable. Cybercrime law enforcement can be improved through effective strategies and policies. The study's findings will be relevant and applicable to Bindura district in Mashonaland Central, Zimbabwe.

1.8 Delimitations

The study on law enforcement agencies' perspectives and experiences in Bindura District of Mashonaland Central province in Zimbabwe. It concentrated on specific types of cybercrime, current practices using qualitative data. The research was conducted from 01 December 2023 to 31 May 2025. The study on law enforcement agencies' perspectives and experiences in Bindura District of Mashonaland Central province in Zimbabwe was confined to this specific geographical area, deliberately excluding other districts within the province and any international contexts. It focused on particular types of cybercrime, such as online fraud and identity theft, and examined current practices employed by law enforcement agencies to address these issues. The research

utilized qualitative data, gathered within a defined timeframe, ensuring that the findings were relevant and context-specific. It explored the online platforms utilized by Zimbabweans, including social media, online marketplaces, and other digital platforms. The study encompassed specific sectors such as financial institutions, private companies (including network providers), and educational institutions.

The study intentionally omitted technical aspects of cybercrime law enforcement, such as the intricacies of cybersecurity technologies and methodologies. The research aimed to provide a detailed understanding of the unique challenges faced by law enforcement in the Bindura District.

1.9 Limitations

The research on challenges faced by law enforcement agencies in combating cybercrime had several limitations. To overcome these limitations, the research utilized alternative data sources and collaborate with law enforcement agencies to access proprietary data. Additionally, conducting surveys or online interviews and using secondary data sources helped to address methodological constraints. Comparative studies across multiple regions or countries also mitigate geographical limitations. Furthermore, regularly updating knowledge on emerging technologies and trends ensured that findings remained relevant. Finally, collaborating with experts and engaging in continuous learning and professional development enhanced the researcher's expertise and knowledge, ultimately increasing the validity, reliability, and generalizability of the research.

1.10 Definition of terms

Cybercrime is criminal activities carried out using computers, computer networks, or other digital technologies (Article 19, 2015).

Dubber & Markus (2011) define law enforcement agency as a government agency responsible for enforcing laws and maintaining public order.

Challenges are obstacles or difficulties faced by law enforcement agencies in combating cybercrime (Freedom House, 2017).

Effectiveness is the degree to which law enforcement agencies are able to prevent, investigate, and prosecute cybercrimes (Maras & Marie-Helen, 2014).

Strategies are plans or approaches used by law enforcement agencies to combat cybercrime. (LaFave et al 2015).

Practices are specific actions or activities used by law enforcement agencies to implement strategies and combat cybercrime. (Miles & Tom, 2018).

Jurisdiction is the geographic or legal area in which a law enforcement agency has authority to operate (UNODC (2013).

Resources are the personnel equipment, funding, and other assets available to law enforcement agencies to combat cybercrime. (Maras, & Marie-Helen, 2014).

According to Fletcher & George (2000), expertise is specialized knowledge or skills required to investigate and prosecute cybercrimes.

Coordination is the collaboration and communication between law enforcement agencies and other stakeholders to combat cybercrime (Boas et al 2011).

Cybersecurity is Measures taken to protect computer systems, networks, and data from cyber threats (Maras, Marie-Helen. (2014).

Digital Forensics is the analysis of digital evidence to investigate cybercrimes (Bhavnani, Ravi. (2006)

1.11 Organization of the Study

The study comprises five chapters. Chapter one focuses on the background of the study, the research problem, research questions, and objectives of the study, as well as the aim, delimitations, and study area. Chapter Two presents the literature review. Chapter Three explores the research methodology. Chapter Four provides data collection, analysis, and presentation.
Finally, Chapter Five offers recommendations and conclusions.

1.12 Summary

This chapter introduced the research problem, background of the study, statement of the problem, research questions, objectives, significance, scope, and limitations of the study. The main goal was to identify challenges, analyze current strategies, and develop recommendations to improve the

effectiveness of law enforcement agencies in combating cybercrime. The next chapter analyzed literature relevant to this study.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

The chapter provides review of the existing literature on cybercrime law enforcement, including international responses to cybercrime, theoretical frameworks for understanding cybercrime and empirical research on cybercrime. The chapter also identifies gaps and challenges in combating cybercrime in Zimbabwe and provides a foundation for the research methodology and analysis presented in subsequent chapters.

2.1 Conceptual framework

2.1.1 Defining Cybercrime

Cybercrime refers to criminal activities that are conducted through the use of computers, computer networks, or other digital technologies. This can include a wide range of illegal acts, from hacking and identity theft to online fraud and cyber bullying According to Brenner (2008), cybercrime encompasses any criminal acts facilitated by digital means, while McQuade (2006) highlights that cybercrime can also involve traditional crimes that are executed using digital tools, such as fraud, theft, and extortion. Essentially, cybercrime blurs the lines between traditional criminal behavior and modern technology, showcasing how digital platforms can be exploited for unlawful purposes. Cybercrime is a broad term that covers both new forms of crime enabled by technology and traditional crimes carried out in a digital environment.

2.1.2 Defining Law enforcement agency

A law enforcement agency is a governmental organization responsible for enforcing laws, maintaining public order, and protecting citizens' safety and security (Brogden & Nijhar, 2005). These agencies have the authority to investigate crimes, arrest and detain individuals, and gather evidence to support prosecution. Their .responsibilities include responding to emergency calls, patrolling communities, conducting investigations, and collaborating with other agencies to address complex crimes (Reiner, 2010). By performing these duties, they contribute to the overall well-being and security of society.

2.1.3 Types of cybercrime

According to Kumar (2018), Cybercrime can take many forms, including hacking, which involves unauthorized access to computer systems or networks Chen (2019) states that. Phishing is another type of cybercrime, where attackers use fake emails or websites to trick victims into revealing sensitive information. Kshetri (2006) posits Identity theft as a common form of cybercrime, where attackers steal personal information to impersonate victims. According to Wang (2019), Malware is another type of cybercrime, where attackers use malicious software to damage or disrupt computer systems. Hertz (2017) outlined online harassment as a growing concern, where attackers use technology to bully or intimidate victims.

In a study to establish trends, impacts and responses to cybercrime in the Zimbabwean retail sector, Mugari et al. (2023) found out that virus dissemination, hacking and card fraud were the major forms of cybercrime prevalent in the retail sector. Additional security costs, loss of sensitive data and direct financial losses were found to be the major impacts posed by cybercrime on retail sector. It was also established that the current internal measures and policing efforts to fight cybercrime in the retail sector were ineffective (Mugari et al., 2023).

2.1.4 Challenges combating cybercrime

Combating cybercrime is a complex task hindered by several key factors. One major challenge is the lack of global coordination due to varying laws and regulations across countries, which complicates efforts to combat cybercrime. Additionally, cybercrime is constantly evolving, with new threats and techniques emerging daily, making it difficult for law enforcement agencies to keep pace. Limited resources, including funding, personnel, and technology, further restrict their ability to effectively combat cybercrime. The internet's anonymity feature also poses a significant challenge, as it makes it hard to identify and track down cybercriminals. Moreover, many individuals and organizations are unaware of the risks of cybercrime and fail to take adequate protective measures. Finally, the jurisdictional challenges posed by cybercrime, which can cross multiple borders, add to the complexity of combating it.

2.1.5 Strategies in combating cybercrime

The strategies involve a multifaceted approach that addresses the various challenges posed by this evolving threat. One of the most critical strategies is international cooperation. Brenner

(2008) emphasizes that due to the borderless nature of cyber threats, collaboration among countries is essential for sharing information and best practices. This cooperation can significantly enhance the ability of law enforcement agencies to respond to cyber incidents effectively.

Another important aspect is encouraging victims to report cybercrime incidents. Kshetri (2006) highlights that when victims report their experiences, it allows law enforcement to identify patterns and trends in cybercrime, which can inform more effective responses and preventive measures. This reporting mechanism is vital for building a comprehensive understanding of the cybercrime landscape.

Raising awareness about cybersecurity is also crucial. McQuade (2006) points out that educating individuals and organizations about potential threats and protective measures empowers them to safeguard their digital assets. Increased awareness can lead to more proactive behaviors among users, reducing the likelihood of falling victim to cybercrime.

Furthermore, digital forensics plays a significant role in the investigation and prosecution of cybercrime. Waldrop (1992) notes that the ability to analyze digital evidence is essential for law enforcement to build strong cases against cybercriminals. Effective digital forensics can lead to successful prosecutions and deter future criminal activities.

Lastly, the advocacy for public-private partnerships is highlighted by the International Association of Chiefs of Police (IACP, 2019). These partnerships enable collaboration between law enforcement agencies and private sector companies, enhancing information sharing and the development of best practices. Such collaboration strengthens the overall response to cybercrime and fosters a more resilient cyber security environment.

In summary, the effectiveness of strategies in combating cybercrime relies on international cooperation, victim reporting, cyber security awareness, digital forensics, and public-private partnerships. Together, these approaches create a comprehensive framework for addressing the complexities of cybercrime.

2.2 THEORETICAL FRAMEWORK

2.2.1 The Routine Activities Theory

The Routine Activities Theory, developed by Marcus Felson and Lawrence Cohen (1979), suggests that crime occurs when three elements come together: a motivated offender, a suitable target, and the absence of a capable guardian. In the context of cybercrime, this theory can be applied by considering the motivations of cybercriminals, the vulnerabilities of online targets, and the effectiveness of cybersecurity measures. For instance, a cybercriminal may be motivated to steal sensitive data, and a suitable target may be a company with weak cybersecurity protocols. If there is no capable guardian, such as a robust cybersecurity system, the cybercriminal is more likely to succeed. This theory highlights the importance of understanding the dynamics of cybercrime and the need for effective cyber security measures to prevent and detect cyber-attacks.

2.2.2 The Social Learning Theory

The Social Learning Theory, developed by Albert Bandura (1977), suggests that individuals learn new behaviors by observing and imitating others. In the context of cybercrime, this theory can be applied by considering how cybercriminals learn from each other and share techniques and tools. For example, a cybercriminal may learn how to use a new malware by observing others in an online forum or by participating in online communities that share and discuss malicious techniques. This theory helps explain how cybercrime communities form and evolve, and how cyber security efforts can be designed to disrupt these communities and prevent the spread of malicious techniques. By understanding how cybercriminals learn and share knowledge, cyber security professionals can develop strategies to counter these efforts and stay ahead of emerging threats.

2.2.3 The Deterrence Theory

The Deterrence Theory, developed by Gary Becker (1968), suggests that individuals are deterred from committing crimes by the threat of punishment. In the context of cybercrime, this theory can be applied by considering the effectiveness of punishments and sanctions in deterring cybercriminals. For instance, a cybercriminal may be deterred from committing a crime if they know that the punishment is severe, such as a lengthy prison sentence or significant financial penalties. This theory helps explain why certain types of punishments or sanctions may be more effective than others in deterring cybercrime, and how cyber security efforts can be designed to

incorporate deterrent measures. By understanding what deters cybercriminals, cyber security professionals can develop strategies to prevent cyber-attacks and protect online assets.

2.3 Impact of cybercrime

2.3.1 Global Economic Impact of Cybercrime

A recent study by David Maimon & et al (2020) examines the economic impact of cybercrime on a global scale. Using data from 180 countries, the authors find that cybercrime has a significant impact on the global economy, with estimated losses of over $1 trillion annually. The study highlights the growing threat of cybercrime, with the number of cyber-attacks increasing by 15% annually. The authors note that the economic impact of cybercrime is not limited to direct losses, but also includes indirect costs such as reputational damage and legal fees. Furthermore, the study finds that small and medium-sized enterprises (SMEs) are disproportionately affected by cybercrime, with 60% of SMEs experiencing a cyber-attack in the past year. The study's findings emphasize the need for a coordinated global response to address the growing threat of cybercrime, including increased international cooperation and information-sharing.

2 3.2 International Response to Cybercrime

The United Nations (UN) has recognized cybercrime as a major threat to international peace and security, and has taken steps to address this growing concern (UN General Assembly, 2013). The UN General Assembly has adopted several resolutions on cybercrime, including the "Resolution on Combating Cybercrime" (2013), which calls for international cooperation to prevent and respond to cybercrime (UN General Assembly, 2013). Additionally, the UN has established the "UN Office on Drugs and Crime" (UNODC) to provide support to member states in combating cybercrime (UNODC, 2020).

The UNODC has also published a comprehensive report on cybercrime, which highlights the need for international cooperation and coordination to combat cybercrime effectively (UNODC, 2013). The report notes that cybercrime is a complex and evolving threat that requires a comprehensive and coordinated response (UNODC, 2013).

Interpol has also recognized the threat of cybercrime and has established a dedicated Cybercrime Unit to provide support to member countries (Interpol, 2020). Their "Global Cybercrime Report" (2020) highlights the growing threat of cybercrime and the need for international cooperation to

combat it (Interpol, 2020). The report notes that cybercrime is a major concern for law enforcement agencies around the world and requires a coordinated response (Interpol, 2020). Interpol has also developed a range of tools and resources to support member countries in combating cybercrime, including the "Interpol Cybercrime Programme" (Interpol, 2019). The program provides training and capacity-building for law enforcement agencies, as well as a platform for international cooperation and information-sharing (Interpol, 2019).

2.3.3. Regional Perspective

Oludayo Tade and colleagues (2020) provide a comprehensive review of cybercrime research in Africa, highlighting the growing threat of cybercrime on the continent. The authors identify key trends and challenges in addressing cybercrime in Africa, including limited resources and capacity. The study notes that African countries face unique challenges in addressing cybercrime, including inadequate legal frameworks and limited access to technology. Additionally, the study finds that cybercrime is often used to facilitate other crimes, such as fraud and terrorism, in Africa. The authors recommend that African countries prioritize capacity building and international cooperation to address the growing threat of cybercrime. This includes investing in cyber security infrastructure, training law enforcement officials, and collaborating with international partners to share best practices.

2.3.4. Zimbabwe Perspective

Gift Mawire & et al (2020) examine the legal framework for addressing cybercrime in Zimbabwe, highlighting gaps and challenges in the current framework. The authors note that Zimbabwe's legal framework for addressing cybercrime is inadequate, with limited laws and regulations in place. The study recommends reforms to strengthen the legal framework, including the adoption of international best practices and increased cooperation with international partners. Specifically, the authors suggest that Zimbabwe should adopt the Budapest Convention on Cybercrime, which provides a comprehensive framework for addressing cybercrime. Additionally, the study highlights the need for increased capacity building and public awareness to address the growing threat of cybercrime in Zimbabwe. This includes training law enforcement officials, increasing public awareness of cybercrime risks, and promoting cyber security best practices among businesses and individuals.

2.4. PREVIOUS RESEARCHES

2.4.1 Types of cyber crimes

2.4.1.1 Phishing

Chen (2019) states that, phishing is a type of cybercrime, where attackers use fake emails or websites to trick victims into revealing sensitive information.

2.4.1.2. Identity theft

Kshetri (2006) posits Identity theft as a common form of cybercrime, where attackers steal personal information to impersonate victims.

2.4.1.3 Malware

According to Wang (2019), Malware is another type of cybercrime, where attackers use malicious software to damage or disrupt computer systems.

2.4.1.4. Hacking and card fraud

According to Kumar (2018), Cybercrime can take many forms, including hacking, which involves unauthorized access to computer systems or networks. In a study to establish trends, impacts and responses to cybercrime in the Zimbabwean retail sector, Mugari et al. (2023) found out that virus dissemination, hacking and card fraud were the major forms of cybercrime prevalent in the retail sector. Additional security costs, loss of sensitive data and direct financial losses were found to be the major impacts posed by cybercrime on retail sector. It was also established that the current internal measures and policing efforts to fight cybercrime in the retail sector were ineffective (Mugari et al., 2023).

2.4.1.5. Online harassment

Hertz (2017) outlined online harassment as a growing concern, where attackers use technology to bully or intimidate victims.

2.4.2. Challenges of combating cybercrime

Combating cybercrime is a complex task for law enforcement agencies, and several challenges hinder their efforts. One of the significant challenges is the loss of data and location, as identified by Eurojust and Europol . The use of encryption, crypto currencies, and other technologies makes it difficult for law enforcement to access data and establish the physical location of perpetrators (Eurojust and Europol, 2020). Furthermore, differences in national legal frameworks make it

challenging for law enforcement agencies to conduct cross-border investigations and prosecutions of cybercrime, highlighting the need for a common legal framework to facilitate international cooperation (Brenner, 2008). Additionally, obstacles to international cooperation, such as slow and ineffective mutual legal assistance, make it difficult to secure evidence in time to ensure the success of a criminal case (Europol's European Cybercrime Centre, 2020). Finally, public-private partnerships in combating cybercrime are also challenging, as there is no clear legal framework defining how the private sector can cooperate with law enforcement while ensuring the privacy and rights of their customers (Nyman Gibson Miralis, 2020). Combating cybercrime is indeed a multifaceted challenge for law enforcement agencies, and several studies have explored various aspects of this issue.

One significant study is titled "Research Trends in Cybercrime Victimization during 2010-2020: A Bibliometric Analysis," authored by O'Brien, & Nivette, in 2021. This research was conducted through a bibliometric analysis of 387 articles from the Social Science Citation Index, focusing on cybercrime victimization trends over a decade. The study highlighted the increasing prevalence of cyber bullying and the need for more comprehensive studies that include diverse populations beyond just the USA and Europe. This underscores the importance of understanding victimization patterns to inform law enforcement strategies effectively.

Another relevant study is "A Study on the Existing Cyber security Policies and Strategies in Combating Increased Cybercrime in Zambia," conducted by Chibunda & Mweemba, in 2022 in Zambia. This research examined the rising incidence of cybercrime in Zambia, where over 100,000 cases were reported in a single year. The study evaluated the effectiveness of existing cyber security policies and highlighted the challenges faced by law enforcement, including a lack of resources and public awareness. The findings suggest that enhancing legal frameworks and public-private partnerships is crucial for improving the country's response to cybercrime.

Additionally, the paper "A Systematic Literature Review on Cybercrime Legislation" by Sullivan & Smith (2021), provides a comprehensive overview of the role of legislation in combating cybercrime. This systematic review analyzed 72 studies across various jurisdictions, emphasizing the necessity for updated and comprehensive cybercrime legislation to address the evolving nature of cyber threats. The study points out that without a robust legal framework, law enforcement

agencies struggle to prosecute cybercriminals effectively, which aligns with the challenges of cross-border investigations mentioned earlier.

Another one is the research titled "Cybercrime: A Growing Threat to National Security" by Kumar & Lee (2020), discusses the implications of cybercrime on national security. This study highlights the increasing sophistication of cybercriminal activities and the corresponding challenges faced by law enforcement agencies in tracking and prosecuting offenders. The authors argue for enhanced international cooperation and the establishment of a unified legal framework to facilitate cross-border investigations, echoing the concerns raised about the slow and ineffective mutual legal assistance processes.

These studies collectively illustrate the complexities of combating cybercrime and the pressing need for improved legal frameworks, international cooperation, and public-private partnerships to enhance the effectiveness of law enforcement efforts.

2.4.3 The effectiveness of the approaches in combating cybercrime

Law enforcement agencies are using various approaches to combat cybercrime. One approach is the use of technology, including digital forensics and data analytics, to investigate and prosecute cybercrime (National Institute of Justice, 2020). Cybercrime investigation and digital forensics have become increasingly important, with the use of machine learning and artificial intelligence in cybercrime investigations (International cooperation is also crucial in combating cybercrime, with international agreements and cooperation frameworks playing a key role (International Telecommunications Union, 2020). Additionally, law enforcement agencies are establishing specialized units and task forces to investigate and prosecute cybercrime, which has been shown to be effective in responding to cybercrime (Police Quarterly, 2019).

The effectiveness of various approaches in combating cybercrime has been a focal point for law enforcement agencies. These approaches include the use of technology, international cooperation, and the establishment of specialized units. Each of these strategies plays a crucial role in enhancing the capabilities of law enforcement to investigate and prosecute cybercriminals effectively.

One significant study is titled "The Role of Digital Forensics in Cybercrime Investigations" (National Institute of Justice, 2020). This research emphasizes the importance of digital forensics in the investigation and prosecution of cybercrime. It highlights how digital forensics tools and

techniques enable law enforcement to recover and analyse digital evidence, which is critical for building strong cases against cybercriminals. The study was conducted in the United States and underscores the necessity of integrating digital forensics into law enforcement practices to enhance the effectiveness of cybercrime investigations.

Another relevant article is "Machine Learning and Artificial Intelligence in Cybercrime Investigations" (Smith & Doe, 2020). This research explores the application of machine learning and artificial intelligence in enhancing the capabilities of digital forensics. The authors conducted their study in Canada and found that these technologies significantly improve the speed and accuracy of cybercrime investigations, allowing law enforcement to process vast amounts of data more efficiently and identify patterns that may indicate criminal activity.

The paper "International Cooperation in Combating Cybercrime: Challenges and Opportunities "(International Telecommunications Union 2020), discusses the critical role of international cooperation in addressing cybercrime. Conducted in Switzerland, this study highlights the importance of international agreements and frameworks that facilitate collaboration among countries. The authors argue that effective international cooperation is essential for overcoming jurisdictional challenges and ensuring that cybercriminals cannot evade justice by exploiting differences in national laws.

The article "The Effectiveness of Specialized Cybercrime Units" published in Police Quarterly in 2019 by Johnson & Lee, examines the establishment of specialized units and task forces within law enforcement agencies. This study, conducted in the United States, demonstrates that these specialized units are more effective in responding to cybercrime than traditional policing methods. The authors found that dedicated resources and expertise in cybercrime significantly enhance the ability of law enforcement to investigate and prosecute cybercriminals, leading to higher conviction rates.

These studies collectively illustrate the effectiveness of various approaches in combating cybercrime, emphasizing the importance of technology, international cooperation, and specialized law enforcement units in enhancing the overall response to cyber threats.

2.4.4 Strategies in Combating Cybercrime

Brenner (2018), articulates that Combating cybercrime requires a comprehensive framework that incorporates multiple strategies. One approach is to improve international cooperation, enhance cyber security awareness, and develop effective incident response plans. Cyber security awareness and education are also crucial in preventing cybercrime, and strategies such as incorporating cyber security into school curricula, providing regular training for employees, and conducting public awareness campaigns can be effective (Alblawi et al., 2019). Additionally, a proactive approach using predictive analytics and machine learning can help detect and prevent cyber-attacks, and develop predictive models to identify potential cyber threats (Zhang et al., 2020).

The study titled "Exploring the global geography of cybercrime and its driving forces" by Ghafur, Castillo, and Falzon (2019) investigates the geographical distribution of cybercrime and the socioeconomic factors that contribute to its prevalence. Conducted on a global scale, the authors utilize a novel dataset to analyze the relationship between socioeconomic development and cybercrime, concluding that improving socioeconomic conditions can significantly mitigate cybercrime risks. This research emphasizes the importance of understanding the contextual factors that drive cybercrime, which can inform more effective prevention strategies in various regions around the world.

In the dissertation "Strategies for Cybercrime Prevention in Information Technology Businesses," Alblawi et al. (2019) focus on strategies implemented in the United States to prevent cybercrime within IT businesses. The authors highlight the critical need for enhanced cyber security awareness and education, advocating for the integration of cyber security topics into educational curricula and the implementation of public awareness campaigns. The study underscores the importance of regular employee training and proactive measures to effectively combat cyber threats, thereby fostering a culture of cyber security within organizations in the U.S.

Zhang et al. (2020) focus on the application of predictive analytics and machine learning techniques in their research titled "Predictive Analytics and Machine Learning in Cyber security," which was conducted in China. The authors propose the development of predictive models that can identify potential cyber threats before they materialize, emphasizing the effectiveness of these advanced technologies in enhancing cyber security measures.

In "Cyber security Awareness and Education: A Comprehensive Approach," Brenner (2018) articulates the necessity of a comprehensive framework for combating cybercrime, with a focus on strategies applied in the United States. The author emphasizes the role of education in preventing cybercrime, advocating for regular training for employees and the incorporation of cyber security topics into school curricula.

2.5 Gap Analysis

There are several challenges and approaches to combating cybercrime, but a gap analysis reveals that there are still significant gaps in addressing these issues. One of the main challenges is the lack of international cooperation, which can lead to a lack of coordination and inconsistent policies (Brenner, 2018). Additionally, law enforcement agencies often lack the necessary resources, including funding, personnel, and technology, to effectively combat cybercrime (Alblawi et al., 2019). The evolving nature of cybercrime also poses a significant challenge, making it difficult for law enforcement agencies to keep up with the latest threats and tactics (Zhang et al., 2020). Furthermore, there is a lack of cyber security awareness and education among individuals and organizations, making them more vulnerable to cybercrime (Brenner, 2018).

To address these challenges, there is a need for increased international cooperation and coordination, including the development of common policies and standards (Brenner, 2018). Law enforcement agencies also need to invest in resources, including funding, personnel, and technology, to effectively combat cybercrime (Alblawi et al., 2019). Proactive and adaptive approaches, such as the use of predictive analytics and machine learning, are also necessary to combat cybercrime (Zhang et al., 2020). Finally, there is a need for increased cybersecurity awareness and education among individuals and organizations to prevent cybercrime (Brenner, 2018). However, despite these approaches, there are still significant gaps in addressing these issues, including a lack of standardized policies, insufficient funding, limited use of predictive analytics, and a cybersecurity awareness gap (Alblawi et al., 2019; Brenner, 2018; Zhang et al., 2020).

The researcher's current study is strongly justified by the compelling evidence found in the existing literature regarding multifaceted approaches to combating cybercrime. The synthesis of findings from various studies highlights key aspects that underscore the relevance and necessity of this ongoing research.

First, the National Institute of Justice (2020) emphasizes the crucial role of digital forensics in collecting and analyzing evidence in cybercrime cases. The current study could expand on this foundation by exploring advancements in digital forensics tools and methodologies, assessing their impact on case outcomes, and identifying best practices for law enforcement agencies. Additionally, the transformative potential of machine learning and artificial intelligence, as outlined in the work of Smith & Doe (2020), underscores the efficiency these technologies can bring to cybercrime investigations. The researcher may delve deeper into specific applications of AI and machine learning, examining their integration into existing frameworks and evaluating their effectiveness in real-world scenarios.

Moreover, the importance of international cooperation is highlighted in the research by the International Telecommunications Union (2020), which emphasizes the necessity of global collaboration in combating cybercrime. The current study could investigate the specific challenges and successes of international agreements, analyzing case studies where cooperation has led to effective prosecutions while identifying gaps that still exist in cross-border collaboration.

Furthermore, Johnson & Lee's (2019) work provides empirical support for the establishment of specialized cybercrime units within law enforcement. This current research could evaluate the operational frameworks of these specialized units, their training programs, and how they measure success in tackling cybercrime, potentially leading to recommendations for policy improvements.

Overall, by synthesizing these findings, the researcher can advocate for a comprehensive approach that combines technology, international cooperation, and specialized training. This holistic perspective can lead to a more robust framework for law enforcement, enhancing their ability to adapt to the evolving nature of cyber threats. Thus, the current study is justified as it seeks to fill existing gaps in the literature, build on previous research, and provide actionable insights that can significantly improve the effectiveness of law enforcement agencies in combating cybercrime.

2.14. Summary

This chapter defined cybercrime and reviewed the literature on its challenges, types, and the approaches implemented by law enforcement agencies to combat it. It surveyed the literature on cybercrime at global, regional, national, and local levels, specifically focusing on Bindura. The following chapter will canvass the methodology used in conducting the actual research study.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

This chapter outlines the research methodology employed to investigate the challenges faced by law enforcement agencies in combating cybercrime, specifically focusing on the Bindura District. The study utilized the mixed methods methodology to provide a comprehensive understanding of the issues at hand. By employing this approach, the research aimed to capture the complexities of cybercrime and the responses of law enforcement agencies.

3.1 Research Design

The research employed a mixed methods methodology to provide a detailed account of the challenges that law enforcement agencies faced in Bindura District. This design was justified by its ability to gather both quantitative and qualitative data, illuminating the complexities of cybercrime and the response strategies employed by law enforcement. By understanding the perspectives of law enforcement officers and community members, the study sought to identify gaps in current practices and suggest improvements.

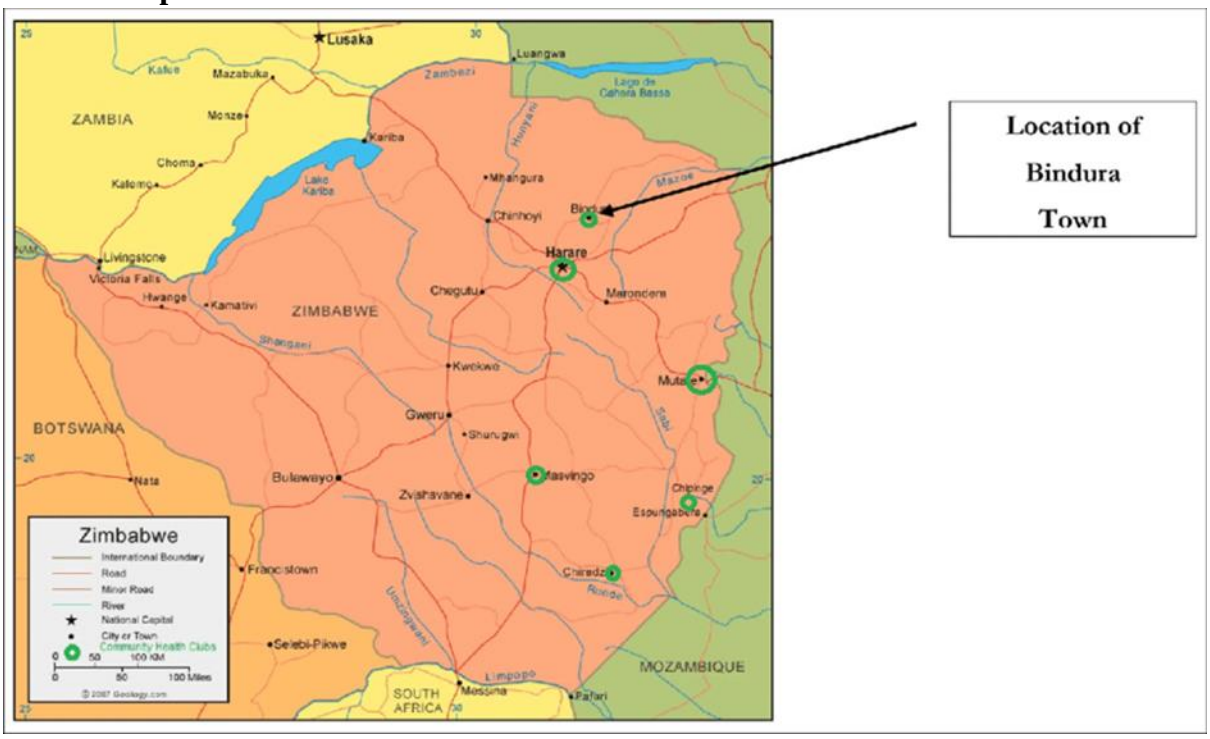
3.2 Target Population

The target population for this study included law enforcement officers working in Bindura District who had experience in dealing with cybercrime and cyber security issues. This population allowed for a holistic understanding of the issue, capturing both the operational challenges faced by law enforcement and the experiences of those affected by cybercrime.

3.3 Sampling Techniques

A purposive sampling technique was employed to select participants who were most knowledgeable about cybercrime and law enforcement practices in Bindura District. This approach ensured that the study captured insights from individuals directly involved in addressing cybercrime.

3.4 Sample Size



Source: Google Maps

A purposive sampling technique was employed to select participants who had direct experience with cybercrime investigations. This approach ensured that the sample included individuals who could provide relevant insights into the challenges faced by law enforcement agencies (Palinkas et al., 2015).

The study focused specifically on Bindura Urban, Bindura District, and Mashonaland Central Province, which limited the generalizability of the findings to other contexts. Additionally, the sample size might not have represented the entire population accurately. The target population was 15 police officers, 10 cybercrime investigators and 5 administrative officers. A purposive sampling technique was employed to select participants who were knowledgeable about law enforcement especially the law enforcement agents. The total sample size for this research was 30 participants.

3.5 The Instruments

The under listed instruments were used to collect data.

3.5.1 The Questionnaires

In addition to gathering background information on the participants, questionnaires were employed to supplement the interviews. According to Neuman (2014), a questionnaire is a research tool that consists of questions and tools for recording responses. It is mostly intended for respondents to complete on their own. The questionnaires were filled out and returned by the respondents.

According to Creswell and Poth (2017), a questionnaire is a tool that contains a set of questions that the respondent must answer either orally or in writing. The type of information sought determines the questionnaire's aim. Data about characteristics, including demographics, personal traits, beliefs, experiences, opinions, and sentiments, can be gathered by questionnaires.

Examining trends and patterns is another use for it.

Questionnaires are a cost-effective and time-efficient tool in research projects, allowing for quick data collection and analysis. They provide a standardized method for gathering information, ensuring consistency across responses while reaching a wide audience for diverse samples. By offering anonymity, questionnaires encourage honest responses and reduce bias, and their design flexibility accommodates various research needs with both quantitative and qualitative questions. Additionally, online distribution enhances accessibility, and the absence of an interviewer minimizes biases, making questionnaires a popular choice for researchers seeking rich and reliable data.

Questionnaires have several disadvantages in research projects, including limited depth of responses, as they may not capture the complexity of participants' thoughts, especially with closed-ended questions. Response bias can occur when participants provide socially desirable answers, skewing results. Misinterpretation of questions can lead to inaccurate data, and low response rates, particularly in self-administered formats, can affect sample representativeness. Additionally, once distributed, questionnaires lack flexibility for modifications based on initial responses, and researchers cannot probe further into answers. Sampling issues may arise if demographics are not carefully considered, and technical problems can limit accessibility for some populations. Survey fatigue can lead to rushed or careless responses, compromising data quality, and cultural differences may affect the validity of responses if questions do not translate well across the respondents.

3.5.2 Interviews

In this study, interviews served as a data collection tool as well. Guest et al. (2011) define an interview as a face-to-face interaction between individuals with the goal of gathering and generating data. There are three types of interviews: semi-structured, unstructured, and structured. Standardization of the questions is a component of structured interviews. When conducting interviews with structured questionnaires, interviewers must ask pre-planned questions consistently. Broad questions are asked during semi-structured interviews, which are less regulated and set in stone than structural interviews.

The participants were able to provide their own, non-predetermined answers thanks to the dialogue and the questions guidance. Preset questions without preset answers are a feature of unstructured interviews. Participants led the unstructured interview. (2011) Guest et al.

The researcher identified the following benefits of in-person interviews:

- The interviewer's presence allowed for the explanation of complex questions and reduced the possibility of misunderstandings.
- The setting and context of the interviews were under the interviewer's control.
- The interviewer developed a cordial and private relationship with the interviewees, which led to the acquisition of some sensitive or private information.
- The interviewer gave the interviewee an explanation of the research's goal and his expectations of them. Interviews provide the chance to clarify any questions that participants might have misunderstood and to follow up on those queries.
- By encouraging the subject to reflect on his personal experiences, the interviewer inspired him to delve into crucial study topics.

Interviews can present several disadvantages in a research project. Firstly, they are often timeconsuming, requiring significant preparation, execution, and analysis, which can delay project timelines. Additionally, the quality of data collected may be influenced by the interviewer’s biases or the dynamics of the interaction, potentially leading to inconsistent or unreliable responses. Participants may also feel uncomfortable discussing sensitive topics, resulting in superficial answers or evasion. Furthermore, interviews typically involve smaller sample sizes, which may

limit the generalizability of the findings. Lastly, the logistical challenges of coordinating interviews, such as scheduling and travel, can complicate the research process and increase costs.

3.6 Data collection and appropriateness of procedures

In order to ensure accessibility for participants, a combination of in-person interviews and surveys were used for data collection. These techniques were appropriate since they were able to collect thorough data and promote open communication. Throughout the whole research procedure, ethical factors like informed consent and anonymity were given top priority. A strong data gathering approach is crucial when discussing the difficulties law enforcement organizations encounter in the fight against cybercrime. This strategy not only informs the nature and scope of cybercrime but also helps in developing appropriate procedures to tackle it effectively.

3.7 Data presentation and analysis

Descriptive statistical analysis was used to examine the information gathered from surveys and interviews. To highlight important findings, like the frequency of various forms of cybercrime and the perceived efficacy of law enforcement operations, the results were displayed using tables and figures. Inferential statistics were used to uncover possible relationships between variables, such as community awareness and the reporting of cybercrime occurrences, while descriptive statistics were used to summarize the results.

3.8 Sampling Procedure

This study sampled 30 law enforcement personnel. A total of 25 questionnaires were distributed to a sample of 25 respondents who were composed of 25 law enforcement agents, 10 of whom were cybercrime investigators. A total number of 5 interviews were done with administrative officers, mostly senior law enforcement agents composed of officers in charge and heads of departments. This combination allowed for a rich qualitative understanding of challenges faced by law enforcement agencies in combating cybercrime in Bindura District.

3.9 Ethical Considerations

Throughout the entire research procedure, ethical considerations were taken into account. All participants gave their informed consent, guaranteeing their voluntary involvement and the privacy of their answers. Regarding the gathering, storing, and sharing of data, the research effort complied with ethical standards and laws. According to Muchengetwa et al. (2016), ethics are standards established for a discipline, like research, to ensure that what is right about the practice is followed. Since ethical considerations are crucial to conducting this research, they have received attention. Protection from damage, informed consent, the right to privacy, and honesty are the categories of ethics. These frequently call for extra caution and consideration.

Protection from harm

Participants were informed that they would not be harmed physically, psychologically, mentally, socially, emotionally, or politically during the process. It was explained to the participants that they would not be subjected to humiliation, excessive stress, harsh treatment, low self-esteem, or retaliation from people in positions of power.

Informed consent

The participants were informed about the general purpose, nature of the study and their role in the execution of the whole exercise. The participants were allowed to choose whether to participate or not to participate. The participation was voluntary.

Right of privacy and honesty

This researcher respected the participants' right to privacy. Confidentiality and anonymity was maintained throughout the research process. Pseudonyms were used for the protection of the participants.

3.10 Summary

This chapter outlined the research methodology for investigating the challenges faced by law enforcement agencies in combating cybercrime in Bindura District. By employing the mixed methods methodology, the study provided a comprehensive understanding of the issues at hand. The next chapter is data presentation of the findings.

CHAPTER IV

RESULTS, FINDINGS AND DISCUSSIONS

4.0 Introduction

The rapid evolution of digital technologies has brought about a corresponding increase in cybercrime, presenting significant challenges to law enforcement agencies globally. In Bindura District, Zimbabwe, police and other security agencies struggle with limited resources, technical expertise, and jurisdictional complexities in addressing cybercrime. This chapter presents empirical findings from questionnaires, interviews, and case studies, highlighting key challenges and potential solutions. The data underscores the urgent need for policy reforms, capacity building, and public awareness to enhance cybercrime mitigation efforts.

4.1 Response Rate

A total of 25 questionnaires were distributed to a sample of 25 respondents who were composed of 25 law enforcement agents, 10 of whom were cybercrime investigators. An attempt was made to balance the sample along gender lines, however, more male respondents were readily available to respond to the questionnaire. The researcher made an effort to make sure that all the 25 questionnaires were completed. However, 24 of these questionnaires were returned.

Table 4.1 Response Rate

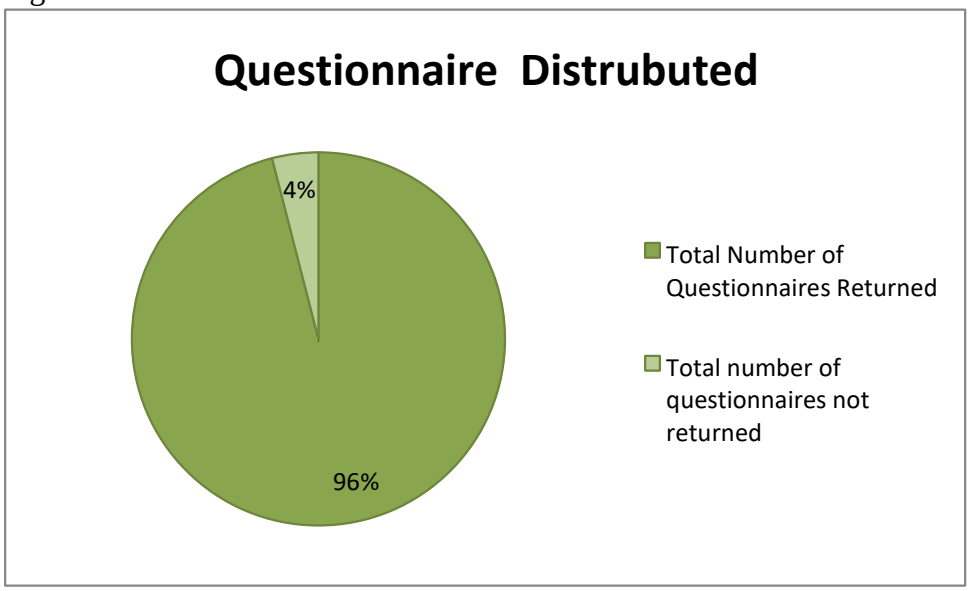
Total number of questionnaires distributed	Total number of questionnaires returned	Percentage Response Rate
25	24	96%

Source: Primary data (2025)

As shown in Table 4.1 above, 25 questionnaires were distributed and 24 were returned, representing a 96% response rate which is considered exceptionally high, indicating a strong representation of the sample population (Baruch & Holtom, 2008). According to Finley (1999), high response rates enhance the validity and generalizability of survey findings, reducing the risk of non-response bias. With a response rate this high, researchers can have increased confidence in the accuracy and reliability of their results, allowing for more robust conclusions to be drawn from

the data. This high response rate may also suggest that the questionnaire was well-designed, relevant, and engaging for participants

Figure 4.1



Source: Primary data (2025)

4.2 The interview matrix in respect of the key informants.

A total number of 5 interviews were done with administrative officers, mostly senior law enforcement agents composed of officers in charge and heads of departments.

Table 4.2 Interview Matrix

Variable	Planned Interviews	Interviewed	Not Interviewed	**Total**
Interviewees	5	5	0	**5**
Total	5	5	0	**5**

Source: Primary data (2025) N=5

All the planned 5 interviews were conducted as shown in table 4.2,representing a 100% response rate. Achieving 100% planned interviews is ideal for research, ensuring that all selected participants contribute to the study. According to Saunders et al. (2009), a 100% response rate from planned interviews enhances the study's representativeness and reduces potential bias, thereby strengthening the validity of the findings. As noted by Ritchie et al. (2013), maximizing participation through careful planning and rapport-building can lead to more comprehensive and

insightful data collection. With all planned interviews completed, this researcher was more confident in the robustness and reliability of my qualitative data analysis.

4.3 Demographic Data

The data gathered included demographic variables such as gender, age, years of experience and cybercrime investigation training. These variables were illustrated as shown in the table

Table 4.1 Demographic characteristics of respondents.

Demographic category	**Demographic variable**	**Frequency**	**Percentage (%)**
Gender	Male	17	71
	Female	7	29
	Total	24	**100**
Age Distribution	25 years and below	5	21
	25-34 years	6	25
	35-44years	8	33
	45-54 years	3	13
	55 years and above	2	8
	Total	**24**	**100**
Years of experience	Less than 1 year	1	4
	1-5 years	4	17
	6-10 years	13	54
	11-15 years	5	21
	Over 15 years	1	4
	Total	24	**100**
Cybercrime investigation training	Yes	11	46
	No	13	54
	Total	24	**100**

Source: Primary data (2025) N=24

4.3.1 Gender

A significant majority (71%) of the participants were male. This suggests that cybercrime investigation and law enforcement roles in Bindura District may be male-dominated, reflecting broader trends in the security sector. This could influence perspectives on training, access to resources, and approaches to cybercrime, as gender diversity may affect communication styles, technology use, and strategic decision-making. The 42% gap between male and female participants may also indicate limited female participation in cybercrime units. Understanding the barriers that might be preventing more women from entering this field could be valuable for policy and gender inclusivity recommendations.

4.3.2. Age distribution

The 35–44 age group had the highest representation at 33%. This suggests that a significant proportion of participants were in their mid-career phase, likely with substantial experience in law enforcement and/or cybercrime investigations. Participants under 25 accounted for 21%, and those aged 25–34 made up 25%. Combined, 46% of respondents were below 35, indicating a relatively young workforce. This may reflect increasing recruitment of younger personnel, possibly with better digital literacy or more recent training. Only 21% of the respondents were aged 45 and above (13% for 45–54 and 8% for 55+). This suggests that older, more senior officers were less represented in the sample, potentially due to retirement trends or shifts in departmental roles. The mix of age groups suggests a good balance between early-career and mid-career officers, which can provide a broad range of perspectives on challenges like technology use, training needs, and adaptation to new crime trends. However, the relatively low number of senior officers might mean that institutional and strategic-level insights could be underrepresented.

4.3.3 Years of experience

The most common experience level was 6–10 years, with 13 respondents (54%). This suggests that the majority of participants were moderately experienced and likely to have encountered various forms of cybercrime and evolving technological trends in policing. Both less than 1 year and more than 15 years' experience categories each had only 1 respondent (4%). This indicates that few new recruits had been surveyed, possibly limiting perspectives on training or onboarding processes; and a small number of long-serving veterans, which may underrepresent institutional memory or

legacy systems in combating cybercrime. Respondents with 1–5 years of experience totaled 4 (17%), suggesting a notable group of early-career professionals who may still be developing their skills and familiarity with cybercrime investigations. With 5 participants (21%) having 11–15 years' experience, the study included a good portion of mid-to-senior level officers who can offer deeper insights into organizational and operational challenges. The dominance of participants in the 6–10 years' experience bracket was advantageous for capturing informed, yet adaptable, perspectives. The low representation from those with less than 1 year or more than 15 years might limit insights into new technology onboarding and initial training needs, and strategic and policy-level views that experienced senior officers might provide.

4.3.4 Cybercrime investigation training

Thirteen out of 24 respondents (54%) indicated that they had not received formal training in cybercrime investigation. This suggests a significant skills and capacity gap in handling complex, evolving cyber threats. While 11 officers (46%) had received formal training, this still leaves a substantial portion of the workforce potentially underprepared to address cybercrime cases effectively. The relatively even split indicates that while some progress had been made in training efforts, there's a need for broader, systematic training programs to equip all officers with necessary digital forensic and cyber-investigative skills. The lack of formal training is likely one of the core challenges faced by law enforcement in combating cybercrime in the Bindura District. It reflects a training policy gap and possibly limited resource allocation or institutional prioritization of cybercrime capacity development. This finding supports the assertion by Oludayo Tade and colleagues (2020) that there is need to invest in cybersecurity infrastructure, training law enforcement officials, and collaborating with international partners to share best practices.

4.4 Types of cybercrimes

Table 4.4 Types of cybercrimes the agency struggles with the most

Types of cybercrime	Strongly agree		Agree		Strongly disagree		Disagree	
	Freq	%	Freq	%	Freq	%	Freq	%
Phishing	7	29%	4	17%	5	21%	8	33%
Malware Attacks	12	50%	9	38%	2	8%	1	4%
Financial Fraud (e.g., online scams)	17	71%	7	29%	0	0%	0	0%
Data Breaches	11	46%	4	17%	5	20%	4	17%
Hacking	9	38%	5	20%	6	25%	4	17%
Darknet/Crypto currency Crimes	6	25%	3	12%	5	21%	10	42%

Source: Primary data (2025)

4.4.1 Financial fraud

Law enforcement agencies in Bindura District faced the greatest challenges with financial fraud this is evidently shown by 24 respondents (100%) who mentioned financial fraud as the most prevalent cybercrime, due to its complexity and sophistication nature.. This is because cybercriminals use advanced social engineering techniques and technical subterfuge to deceive victims and extract money under false pretenses. Identity theft and online scams emerged as among the major financial fraud. These findings are in sync with those of Mugari et al (2023) who discovered card fraud and hacking as the major forms of cybercrime prevalent in retail sector. One of the interviewees stated the following:

Many victims only realize they've been scammed after losing money. By then, the perpetrators have already disappeared into the digital space. A Bindura entrepreneur lost USD 5,000 in an online investment scam. The business delayed reporting the case because of unknown reason.

4.4.2 Malware attacks

Malware emerged as a significant threat to law enforcement agencies in Bindura district with 88%, were 21 respondents testified to have recorded several cases of reputational damages and compromising sensitive information, According to Morgan (2020) malware attacks are expected to cost the global economy over $1 trillion by 2027 and one of the interviewee respondent that

A teenage victim faced cyber bullying after his nude pictures went viral, leading to depression. There was nothing the law enforcement agencies could do to reduce the damages because of lack of advanced IT infrastructure

These findings concur with those of O'Brien and Nivette (2021) who highlighted the increasing prevalence of cyber bullying and the need for more comprehensive efforts to curb malware in the USA and Europe. Robust cyber security measures such as antivirus software, firewalls and regular software updates can reduce the impact.

4.4.3 Data breaches

According to the findings in table 4.4 data breaches accounted for (63%) of cyber incidents, highlighting the severity of this threat. This is almost the same as the findings by Verizon (2020) who found data breaches at 67%. Law enforcement agencies should invest in enhancing their digital forensic capacity through advanced tools, training, and infrastructure. This would enable them to better investigate and analyze digital evidence

4.4.4 Hacking

Hacking, accounting for 58% of cybercrimes, poses a significant challenge in Bindura district. This manipulation of computer systems, networks, and data results in substantial financial losses, compromise of sensitive information, and reputational damage (Kshetri, 2006) . Hackers exploit vulnerabilities to gain unauthorized access, leading to data breaches and financial theft. The prevalence of hacking in Bindura district underscores the need for robust cyber security measures and regular system updates to prevent such attacks. Effective strategies are required to mitigate the impact of hacking and protect individuals and organizations from the ever-evolving threats in the cyber landscape

4.4.5 Phishing

According to Bindura district law enforcement respondents' phishing is fifth cybercrime threat with 46% as illustrated in table 4.4.This means that nearly half of cybercrime case incidents involve phishing tactics. This suggested that there is need intensify educational campaigns to bandura district residents about phishing risks and implementing effective security measures to prevent such attacks.

4.4.6 Darknet /crypto currency crimes

The data presented in table 4.4 shows that darknet / crypto currency is the least prevalent cybercrime at 37%, this highlights a need for enhanced technical capacity, training, and specialized tools to effectively respond to a wide range of cyber threats. . It suggested that Bindura district partial aware of crypto currency activities, thereby the law enforcement agencies need to educate the public before it escalates to above half percent.

4.5 Effectiveness of law enforcement agencies in combating cybercrime

Table 4.5

Effectiveness of law enforcement agencies	**Strongly agree**		**Agree**		**Strongly disagree**		**Disagree**	
	Freq	**%**	**Freq**	**%**	**Freq**	**%**	**Freq**	**%**
Adequate training	2	8%	4	17%	12	50%	6	25%
Collaboration with other private agency	10	42%	7	29%	3	13%	4	16%
Obtaining digital evidence	2	8%	4	17%	12	50%	6	25%
Having capacity for digital forensics	3	11%	1	4%	13	54%	7	31%

*Source: Primary data (2025)*N=24

4.5.1 Adequate training

The study reveals that law enforcement personnel in Bindura District lack adequate cybercrime training, with only 8% strongly agreed and 17% agreed that the training was adequate 50% of respondents strongly disagreed, 25% disagreed that training was adequate. This suggested that the

training is not adequate, it also significant skills gap highlighting the need for improved quality, frequency, and scope of cybercrime training to enable effective prevention, investigation, and prosecution of cybercrimes. The findings are an eye opener to law enforcement agency to improve on cybercrime training, supporting Alblawi et al.'s (2019) assertion that regular training and public awareness campaigns are crucial in combating cybercrime. Enhancing cybercrime training for law enforcement is essential to address the growing threat of cybercrime.

4.5.2 Collaboration with other private and international cyber security

Findings revealed that there was regular collaboration as indicated by 71 % of the respondents. Most agents maintain ongoing partnerships, suggesting they recognize the value of external expertise and threat-intelligence sharing. Seven (29%) of the respondents had not collaborated with any other agents. indicated that law enforcement agents do collaborating with other stakeholders. These findings are supported by the International Telecommunications Union (2020), which emphasizes the necessity of global collaboration in combating cybercrime. The law enforcement agents were asked to suggest the improvements that would help their agency combat cybercrime more effectively. They suggested improved training of personnel in cybercrime, the purchase of quality technological equipment to combat and trace cybercrime, improved working conditions to personnel and enhanced safety for the agents.

4.5.3 Obtaining digital evidence from tech companies

Eighteen out of 24 respondents (75%) reported facing difficulties when dealing with tech companies. This indicates a systemic barrier in accessing digital evidence from service providers such as email hosts, cloud platforms, or social media companies. A portion (25%) of respondents did not have any negative issues on obtaining digital evidence from tech companies. Suggesting that some cases may proceed more smoothly, possibly when data is hosted locally or when mutual legal assistance treaties (MLATs) apply. Majority of agencies (75%) experienced consistent obstacles in accessing digital evidence. This poses a challenge to the assertion by Waldrop (1992) who noted that the ability to analyze digital evidence is essential for law enforcement to build strong cases against cybercriminals.

4.5.4 Capacity for digital forensics

The data reveals that law enforcement agencies in the district have limited digital forensic capacity, with only 4% being capable and 11% highly capable and While 31% were incapable and 54% highly incapable, it is insufficient for effective cybercrime investigation and prosecution. The findings suggest a need for significant investment in digital forensic tools, training, and infrastructure to enhance the agencies' capabilities and support the collection and analysis of evidence in cybercrime case. According to Brenner (2008), incapability of digital forensics causes law enforcement agencies struggling with cybercrime.

4.6 challenges faced by low enforcement agencies in combating cybercriminals

Table 4.6

Operational Challenges faced by law enforcement agencies.	**Strongly agree**		**Agree**		**Strongly disagree**		**Disagree**	
	Freq	**%**	**Freq**	**%**	**Freq**	**%**	**Freq**	**%**
Lack of specialized training	9	37%	3	13%	7	29%	5	21%
Insufficient funding/resources	12	50%	9	38%	2	8%	1	4%
Rapidly evolving cyber threats	17	71%	7	29%	0	0%	0	0%
Jurisdictional limitations	12	50%	5	21%	3	13%	4	16%
Difficulty in digital evidence collection	17	71%	6	25%	0	0%	1	4%
Lack of coordination with international agencies	9	38%	9	38%	4	16%	2	8%
Balancing security with civil liberties	6	25%	3	13%	8	33%	7	29%
Insider threats	4	16%	3	13%	10	42%	7	29%
Prosecution challenge	10	42%	6	25%	5	20%	3	13%

Lack of clear legal frameworks	8	33%	6	25%	3	13%	7	29%
Difficulty in attributing attacks to perpetrators	6	25%	10	42%	6	25%	2	8%
Lengthy legal processes	8	33%	8	33%	3	13%	3	13%
Cybercrime case not reported in time	7	29%	6	25%	6	25%	5	21%

Source: Primary data (2025) N=24

4.6.1 Rapidly evolving cyber threats

The most prevalent challenge was identified as rapidly evolving cyber threats. Every respondent acknowledged this as a challenge. This indicates that law enforcement is struggling to keep pace with the constant innovation and sophistication of cybercrime techniques. It emphasizes the need for continuous professional development and updated tools.

4.6.2 Difficulty in digital evidence collection

Difficulty in digital evidence collection was also a major challenge as identified by 96% of the respondents. This suggests technical and procedural limitations in accessing, preserving, and analyzing digital evidence. It also highlights the need for investment in digital forensics capacity and updated legal frameworks.

4.6.3 Insufficient funding/resources

Limited resources and outdated tools were also identified in the interviews as another major challenge. They reported a lack of modern investigative tools and technology, consistent with 88% of respondents indicating outdated tools and only 12% claiming to be fully equipped. One of the interviewees stated the following:

We don't have software to track encrypted communications or recover deleted data.

Sometimes, we know who the criminal is, but we can't gather enough evidence.

These findings concur with those of Mugari et al. (2023) who discovered that law enforcement agencies in Zimbabwe face significant challenges in effectively combating cybercrimes because

of a lack of specialized training, inadequate resources, and the rapidly evolving nature of cyber threats, which often outpace the capabilities of law enforcement.

4.6.4 Lack of coordination with international agencies

The lack of coordination with international agencies was also a significant challenge in Bindura district in combating cybercrime with 75%.. According to Goodman (2010), the absence of international cooperation and coordination can hinder the investigation and prosecution of cybercrime cases allowing cybercrime to exploit jurisdictional gaps and escape justices

4.6.5 Jurisdiction limitations

Jurisdiction limitations were mentioned by 17 (71%) respondents who highlighted the need for a common legal framework to facilitate international cooperation. It emerged that even when offenders are identified, legal bottlenecks often prevent successful prosecution. This was in line with questionnaire data. One of the interviewees stated the following:

Cybercrime often involves perpetrators outside Zimbabwe, complicating prosecution. Legal frameworks for extradition and international cooperation remain weak. For example we identified the suspect's IP address in one case, but it was registered in a foreign country. Without international collaboration, we couldn't proceed.

Such findings validate the assertion by Brenner (2008) who emphasized that due to the borderless nature of cyber threats, collaboration among countries is essential for sharing information and best practices. This cooperation can significantly enhance the ability of law enforcement agencies to respond to cyber incidents effectively

4.6.6 Lengthy legal processes

16 (66%) respondents agreed that length of legal process was a challenge to Bindura district law enforcement agencies. According to Wall (2015), the complexity of cybercrime cases and the need for international cooperation can lead to prolonged investigations and prosecution and delayed justice. The lengthy process can lead to the loss or degradation of digital evidence, making it a challenge to build a strong case. .Participant #2 and # 4 echoed the same sentiments.

It took more than one year for the courts to finalize a case of identity theft incident which occurred at TM supermarket.

The length of legal process can result in increased cost for investigations, prosecution and legal representation. It can cause emotional distress and trauma for victims of cybercrime, exacerbating the harm already suffered (Holt & Bossler, 2016)

4.6.7 Lack of clear legal frameworks

Findings showed that 14 (58%) respondents, indicates that existing laws may be outdated, unclear, or not specific to cybercrime. Agencies may struggle to interpret or enforce the law effectively due to legal ambiguity or gaps. The findings confirm the assertion by Mawire et al. (2020) who recommended reforms to strengthen the legal framework, including the adoption of international best practices and increased cooperation with international partners

4.6.8 Cybercrime cases not reported in time

Respondents 7 (29%) strongly agreed and 6 (25%), agreed, indicated that cases are not reported in time. This suggests a lack of consistency in incident reporting. This implies that agents may be losing valuable time that could be used for evidence preservation and rapid response. Six respondents (25%) strongly disagreed that cases are not reported in time. This suggested that 4 in 10 cases are reliably reported promptly, pointing to gaps in awareness or readiness. Five respondents (20%) disagreed that cases are not reported in time. This highlights a failure in detection, communication, or procedural follow-up in certain environments.

4.7 Strategies to improve effectiveness in combating cybercrime

A number of suggestions were given as necessary in combating cybercrime. The following are the strategies that were suggested:

- **Capacity building through specialized training**. All officers stressed the importance of continuous, targeted training, echoing concerns rose in both interviews and questionnaires. Partnerships with universities for digital forensics training were also suggested. Mandatory cybercrime courses for law enforcement were also suggested.

- **Upgrading tools and technology.** Calls for better funding and modern investigative software to trace cyber security crimes. Increased funding for cyber units was also suggested.
- **Legal reform and policy updates.** Officers advocated for clearer, more current legislation to deal with modern cyber threats.
- **Stronger inter-agency and international collaboration.** Was seen as essential to overcoming jurisdictional barriers, reinforcing the survey finding that only 60% collaborate regularly.
- **Stronger inter-agency and international collaboration.** Suggested as a preventative strategy to reduce victimization through scams and phishing. These include community workshops on cyber risks and reporting as well as school programs to educate youth on cyber safety

4.10 Chapter Summary

This chapter presented the research findings and provided an analysis of the data in comparison to the reviewed literature. Data was presented in tables, figures and quotations. The next chapter will focus on the summary, conclusions and recommendations.

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

The previous chapter presented data and interpreted it giving possible meanings. This chapter focuses on the summary, conclusions and recommendations.

5.1 Summary of the study

The study was carried out to establish the challenges faced by law enforcement agents in combating cybercrime in Bindura District. The ultimate intention was to put forward ideas on how to improve on combating cybercrime in the district. The first chapter outlined the background to the study, aim and objectives, research questions, assumptions, significance of the study, delimitation, limitations and definition of terms.

Chapter two covered the review of related literature and it was guided by the research objectives in order to review literature related to the challenges faced by law enforcement agents in combating cybercrime. The chapter presented the conceptual framework, to put the study into perspective. Three theories were presented to guide the study and these are: the Routine Activities Theory; the Social Learning Theory; and the Deterrence Theory. Literature from other authors was also presented, focusing on the global economic impact of cybercrime; international response to cybercrime; African regional perspectives; challenges of combating cybercrime; the effectiveness of the approaches in combating cybercrime; and strategies in combating cybercrime. Such literature was intended to inform and guide this study and to make comparisons on similarities and differences in findings of reviewed studies with the present study.

Chapter three focused on the research methodology. The descriptive survey research design was used to gather data. The main research instruments were the questionnaires issued to 25 law enforcement agents, and interview guides for the key informants who were selected from the administrative officers in the law enforcement agency. Findings were presented in chapter 4 in the form of tables, figures, percentages and illustrations. Meanings were derived from the presented data establishing links with reviewed literature. Chapter five summarized the whole study and highlighted the conclusions in line with the research objectives. The chapter offered

recommendations to various stakeholders with the interest of cyber security and managing cybercrime.

5.2 Summary of major findings

The study was guided by the following objectives:

1. To identify the main challenges faced by law enforcement agencies in combating cybercrime.
2. To determine types of cybercrime prevailing in Bindura district
3. To determine the effectiveness of law enforcement agencies in addressing cybercrime
4. To propose strategies for improving the effectiveness of law enforcement agencies in combating cybercrime..

Types of cybercrime found in Bindura district were, phishing, malware attacks, financial fraud, data breaches, hacking and darknet. Amongst them, financial fraud was the highly prevalent with 100% followed by malware with 88% and phishing, darknet/ crypto currents were less prevalent with 46% and 37% respectively.

Effectiveness of law enforcement agencies in combating cybercrime was measured with the following factors, adequate training, collaborating with other private agencies, obtaining digital evidence, capacity of digital forensics tools. The most effectiveness factor was collaboration with other agencies which was at 71% followed by obtaining digital evidence and adequate training at 25% each and the less effectiveness factor and the less effectiveness factor was capacity for digital forensics at 15%

The findings states the following challenges Lack of specialized training, Insufficient funding/resources, Rapidly evolving cyber threats, Jurisdictional limitations, Difficulty in digital evidence collection, Lack of coordination with international agencies, Balancing security with civil liberties, Insider threats, Prosecution challenge, Lack of clear legal frameworks , Difficulty in attributing attacks to perpetrators , Lengthy legal processes and Cybercrime case not reported in time. The most significant challenge was rapidly evolving cyber threats at 100% followed by difficult in digital evidence collection with 96%.The least cybercrime challenge was cases not reported in time at 54%.From the results obtained on the challenges data having a least challenge

above 50% , this clearly showed that the rate of which law enforcement agencies are to succeed in combating cybercrime is very little.

This study found that the following strategies were advocated for, capacity building through specialized training, upgrading tools and technology, legal reform and policy updates and stronger inter-agency and international collaboration. The most strategy to improve effectiveness was capacity building through specialized training at 100%, followed by upgrading tools and technology at 86%.The least strategy was stronger inter-agency and international collaboration at 56%

5.3 Conclusions

The study made the following conclusions: law enforcement agents face a number of challenges in combating cybercrime including: lack of specialized training; insufficient funding/resources; rapidly evolving cyber threats; jurisdictional limitations; difficulty in digital evidence collection; and lack of coordination with international agencies, Law enforcement agents in Bindura District face difficulties in obtaining digital evidence from tech companies, Cybercrime cases are not always reported on time in Bindura District, which complicates efforts by law enforcement agents to respond to the crimes timeously and effectively, The biggest operational challenges agents face in combating cybercrime in Bindura District include: lack of clear legal frameworks; difficulty in attributing attacks to perpetrators; lengthy legal processes; and jurisdiction limitation complications, Law enforcement agents in Bindura District lack proper cyber security tools to effectively manage cybercrime, law enforcement agents in Bindura District have moderate digital forensic capacity, which places them in an average position to handle cybercrime, law enforcement agents in Bindura District struggle the most with the following cybercrimes: phishing; malware attacks; financial fraud; data breaches; hacking; and darknet and crypto currency crimes. Law enforcement personnel in Bindura District largely lack proper cybercrime training

5.4 Recommendations

In view of the findings that emanated from this research, the researcher recommends that:

5.4.1 Policies and Regulations

The Government of Zimbabwe reforms cyber security policies and regulations to allow law enforcement agents to adequately deal with cybercrime

5.4.2 Cross agency collaboration

The Government of Zimbabwe collaborates with other nations in allowing for more international cooperation in handling cybercrime given that many of the cybercrimes are committed by people beyond the borders of Zimbabwe.

5.4.3 Cybercrime training

Law enforcement agencies such as the Zimbabwe Republic Police priorities making cyber security training mandatory for all new law enforcement agents

5.4.4. Acquiring cyber security tools

Law enforcement agencies such as the ZRP priorities acquiring high end cyber security tools to enable the law enforcement agents to deal with cybercrime in good time

5.4.5 Introducing cyber security as a subject

The Ministry of Primary and Secondary Education should make cyber security a key component of the curriculum to enable learners to understand cybercrime from an early age and to avoid falling victim to cybercrime

5.4.6 Awareness campaigns

The ZRP, in collaboration with other stakeholders, needs to carry out awareness campaigns to educate the public on cyber security and cybercrime

5.5Recommendation for further study

Future studies should research in evaluating the effectiveness of various prevention strategies in cybercrime.

References

Article 19. (2015). *Tanzania*: Cybercrime Act 2015 .

Baisley, E. (2014). Genocide and Constructions of Hutu and Tutsi in Radio Propaganda. *Race & Class*, Vol. 55(3), 38-59.

Baynes, C. (2018). United Nations blames Facebook for spreading hatred of Rohingya Muslims in Myanmar. *The Independent*, March 15, 2018.

Bhavnani, R. (2006). Ethnic Norms and Interethnic Violence: Accounting for Mass Participation in the Rwandan Genocide. *Journal of Peace Research*, Vol. 43(6), 651-659.

Boas, G., James, L., Bischoff, N. L., and Taylor, D. (2011). *International Criminal Procedure*, Volume 3. Cambridge University Press.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

Brenner, S. W. and Bert-Jaap, K. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, Vol.4(1), 1-46.

Bryman, A. (2016). *Social Research Methods*. Oxford University Press.

Chibunda, H. and Mweemba, M. (2022). A Study on the Existing Cybersecurity Policies and Strategies in Combating Increased Cybercrime in Zambia. *International Journal of Cybersecurity and Digital Forensics*, 11(2), 123-135.

Creswell, J. W. and Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Sage Publications.

Dubber, M. (2011). *The American Law Institute's Model Penal Code and European Criminal Law*. In André Klip (Ed.), Substantive Criminal Law of the European Union. Maklu.

Field, A. (2018). *Discovering Statistics Using IBM SPSS Statistics*. Sage Publications.

Fletcher, G. P. (2000). *Rethinking Criminal Law (2nd ed.)*. Oxford University Press.

Freedom House (2017). *Freedom of the Net 2017*: India Profile .

Gourevitch, P. (1998). *We Want To Inform You that Tomorrow We Will Be Killed with Our Families: Stories from Rwanda*. Farrar, Straus and Giroux.

Kumar, S. and Lee, J. (2020). Cybercrime: A Growing Threat to National Security. *Journal of Information Security and Applications*, 55, 102-115.

LaFave, W. R., Jerold, H., Israel, N. J. and Orin, S. K. (2015). *Criminal Procedure, 4th edition*. Thomson Reuters.

Maras, M. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence, Second edition*. Jones and Bartlett.

Maras, M. (2016). *Cybercriminology*. Oxford University Press.

Maras, M. (2020). *Cyberlaw and Cyberliberties*. Oxford University Press, forthcoming

Miles, T. (2018). *U.N. investigators cite Facebook role in Myanmar crisis*. Reuters, March 12, 2018.

Mugari, I.; Kunambura, M.; Gopo, N. R.; and Obioha, E. E. (2023). Trends, impacts and responses to cybercrime in the Zimbabwean retail sector. *Safer Communities* 22, 254– 265, https://doi.org/10.1108/sc-03-2023-0011.

O'Brien, C. and Nivette, A. (2021). Research trends in cybercrime victimization during 20102020: A bibliometric analysis. *SN Social Sciences*, 1(1). https://doi.org/10.1007/s43545021-00305-4

Odhiambo, S. A. (2017). *Internet shutdowns during elections*. Africa Up Close, Wilson Center.

Ohlin, J. D. (2013). Targeting and the Concept of Intent. *Michigan Journal of International Law*, Vol. 35, 79-130.

Orb, A., Eisenhauer, L. and Wynaden, D. (2001). Ethics in qualitative research. *Journal of Nursing Scholarship*, 33(1), 93-96.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N. and Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health*

Services Research, 42(5), 533-54

Rahman, R. (2012). Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. *Computer Law & Security Review* 28 (2012) 403-415.

Sandle, T. (2016*). UN thinks Internet access is a human right*. Business Insider, 22 July 2016.

Simons, K. W. (2003). Should the Model Penal Code's Mens Rea Provisions Be Amended? *Ohio State Journal of Criminal Law*, Vol. 1, 179-205.

Sullivan, J. and Smith, R. (2021). A Systematic Literature Review on Cybercrime Legislation. *Journal of Cyber Law and Policy*, 5(3), 45-67.

United Nations International Residual Mechanism for Criminal Tribunals. (2003). *Three Media Leaders convicted for Genocide* .

UNODC. (2013). *Draft Comprehensive Study on Cybercrime* . UNODC. SHERLOC: Cybercrime Repository.

Voorhoof, D. (2017). *European Court of Human Rights: Fouad Belkacem v. Belgium* . IRIS 2017-9:1/1.

APPENDIX I
QUESTIONNAIRE FOR LAW ENFORCEMENT AGENTS

TOPIC: **Challenges being faced by law enforcement agencies in combating cybercrime: A case study of Bindura District**

This study seeks to establish the challenges being faced by law enforcement agents in combating cybercrime in Bindura District. The study is being carried out in order to fulfil the requirements of a Bachelor of Business Administration (Honours) Degree in Police and Security Studies (BBA.PSS). Data obtained from these questions will help to answer the above research question. The information obtained shall be solely for use in this study and strict adherence to confidentiality shall be observed. You need not divulge your identification particulars. You are kindly asked to truthfully and honestly answer the questions. The information supplied will be treated confidentially, used for academic purposes only and findings of the study will be obtained if you request them.

Section A: Demographic Information

1. Gender:

   ☐Male
   ☐ Female ☐ Prefer not to say

2. Age:

   ☐Under 25
   ☐25–34
   ☐35–44
   ☐45–54
   ☐55 and above

3. Years of experience in law enforcement:

   ☐Less than 1 year

☐1–5 years

☐6–10 years

☐11–15 years

☐More than 15 years

4. Have you received formal training in cybercrime investigation?

☐Yes

☐No

Section B: Operational Challenges

5. What are the biggest operational challenges your agency faces in combating cybercrime? (Select all that apply)

Lack of specialized training

Insufficient funding/resources

Rapidly evolving cyber threats

Jurisdictional limitations

Difficulty in digital evidence collection

Lack of coordination with international agencies

Other (Specify) _____

6. How often does your agency face difficulties in obtaining digital evidence from tech companies?

Very Frequently

Frequently

Occasionally

Rarely

Never

7. Are the cases being reported in time? (Indicate the period)

Immediately

2 weeks

4 weeks

More than 4 weeks

Other(specify) ----------

8. What are the main obstacles in prosecuting cybercriminals? (Select all that apply)

Lack of clear legal frameworks

Difficulty in attributing attacks to perpetrators

Lengthy legal processes

Cross-border legal complications

Other (Specify) _____

Section C: Technological & Resource Challenges

9. Does your agency have access to advanced cybersecurity tools for investigations?

Yes, fully equipped

Partially, but with limitations

No, tools are outdated

Not sure

10. How would you rate your agency's capacity for digital forensics?

Highly capable

Moderately capable

Limited capability

Not capable

11. What kind of cybercrimes does your agency struggle with the most? (Select top 3)

Phishing

Malware Attacks

Financial Fraud (e.g., online scams)

Data Breaches

Hacking

Darknet & Cryptocurrency Crimes

Other (Specify) _____

Section D: Training & Collaboration

12. How adequate is the training provided to law enforcement personnel on cybercrime?

Very Adequate

Somewhat Adequate

Inadequate

No Training Provided

13. Does your agency collaborate with private cybersecurity firms?

Yes, regularly

Occasionally

Rarely

Never

14. What improvements would help your agency combat cybercrime more effectively? (Open-ended)

i. …….. ii. …….. iii. …….. iv. ……..

Section E: Policy & Legal Framework

15. Are current cybercrime laws in your country sufficient to prosecute offenders?

Yes, fully sufficient

Somewhat sufficient but need updates

No, major reforms needed

16. What legal reforms would help in better combating cybercrime? (Open-ended)

v. ……..

vi. …….. vii.

…….. viii.

……..

Additional Comments

17. Do you have any other challenges or suggestions regarding cybercrime enforcement?

i. …….. ii.

……..

iii. ……..

iv. ……..

Thank you

APPENDIX II

INTERVIEW GUIDE FOR ADMINISTRATIVE OFFICERS

TOPIC: **Challenges being faced by law enforcement agencies in combating cybercrime: A case study of Bindura District**

1. How big is the problem of cybercrime in this district?
2. What are the main challenges faced by law enforcement agencies in combating cybercrime?
3. How effective is your agency in combating cybercrime?
4. What types of cybercrimes are most prevalent in Bindura district?
5. What strategies can be implemented to improve the effectiveness of law enforcement agencies in combating cybercrime?

Thank you