BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

THE EFFECTIVENESS OF CYBER SECURITY TOOLS IN COMMERCIAL CRIME MANAGEMENT IN THE ZIMBABWE REPUBLIC POLICE (ZRP): A CASE STUDY OF THE CRIMINAL INVESTIGATION DEPARTMENT (CID) HARARE CENTRAL

B232438B

LIBWETA WILFRED

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELOR OF BUSINESS ADMINISTRATION (HONOURS) DEGREE IN POLICE AND SECURITY STUDIES OF BINDURA UNIVERSITY OF SCIENCE EDUCATION. FACULTY OF COMMERCE, DEPARTMENT OF INTELLIGENCE AND SECURITY.

JUNE 2026

RELEASE FORM

Name of Author: Libweta Wilfred

Dissertation title: The effectiveness of cyber security tools in commercial crime management in the Zimbabwe Republic Police (ZRP). A case study of the criminal investigation Department (CID) Harare Central

Degree title: BBA (Honours) Degree in Police and Security Studies

Year: 2026

I Libweta Wilfred, hereby grant Bindura University of Science Education permission to reproduce copies of this dissertation for scholarly purposes. The University Library may lend or sell such copies. The author reserves the right to publish this work or any part thereof.

Signed…….....

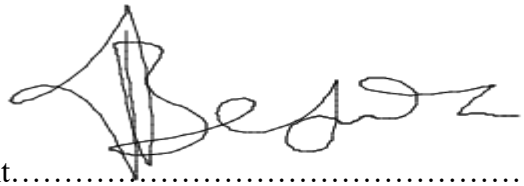
.

Date……20/06/2026……

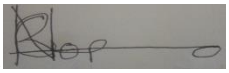
Permanent Address: House No. 15737
Unit P seek
Chitungwiza

APPROVAL FORM

The undersigned certify that they have supervised the student Wilfred Libweta dissertation entitled***, "the effectiveness of cyber security tools in commercial crime management in the Zimbabwe Republic Police (ZRP)"*** submitted in partial fulfilment of the requirements of the Bachelor of Business Administration in Police and Security Studies (Honours) Degree.



Student…….....Date……20/06/2026……



Supervisor……

…….....Date……

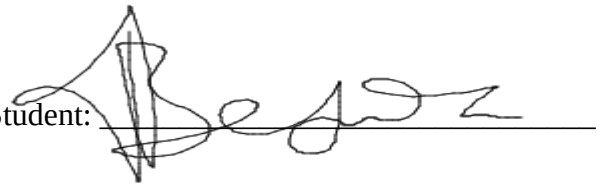


5/8/26

Chairperson…….Date……

DECLARATION

I, Libweta Wilfred, affirm that this dissertation represents my original work, neither submitted, in full or in fragment, to any degree or examination at this or any other institute. Citations have carefully been made to all sources of information as required by the Harvard referencing convention. In those instances where the intellectual contributions of other scholars have been resorted to, they have been rightly cited and referred to throughout the text.

Signature of Student: 

Date: _____20/06/2026_____

]

ABSTRACT

Commercial crimes such as fraud, mobile money theft, ransomware, business email compromise, and identity theft pose an intensifying threat to Zimbabwe's economic security, yet the operational efficacy of cyber security tools used by the Zimbabwe Republic Police (ZRP) remains empirically under-examined. This study aimed to critically analyze the effectiveness of cyber security tools implemented by the Criminal Investigation Department (CID) at Harare Central in controlling commercial crimes between 2020 and 2026. The specific objectives were to: identify the cyber security tools currently in use by the CID; assess their operational effectiveness in detecting and investigating commercial crimes; examine the challenges limiting their full utilization; and recommend strategies to enhance their application. A mixed-method research design was adopted, employing a structured questionnaire administered to 30 purposively selected CID members and semi-structured interviews with 10 key informants drawn from CID leadership, detective units, and IT and forensic support, supplemented by secondary crime statistics and national cybercrime incident logs. Major findings reveal that cyber forensic software (87%), CCTV (77%), and automated fingerprint identification systems (70%) form the operational core of CID's cyber security capability, with mobile money fraud detection rates rising from 34% in 2020 to 51% in 2025; however, skills shortages (87%), inadequate infrastructure (80%), funding constraints (77%), and fragmented cross-border jurisdiction (70%) significantly limit their potential. The study concludes that while cyber security tools have measurably improved commercial crime detection, systemic institutional constraints continue to undermine their full effectiveness. It is recommended that the ZRP priorities sustained investment in specialized training and establish a dedicated cybercrime investigation unit to consolidate capacity and streamline operations.

Keywords: Cyber security tools, commercial crime management, Zimbabwe Republic Police, Criminal Investigation Department, digital forensics, Technology Acceptance Model, Situational Crime Prevention, mixed methods.

DEDICATION

And with an inmost thankfulness, I dedicate this dissertation to my family - their patience and sacrifice, their encouragement and support through it all, and throughout every difficult stage of this such research. It also is dedicated to the men and the women of the Zimbabwe Republic Police who despite circumstances of significant resource limitation continue to work with commitment and professionalism in the name of providing public safety and justice. This question was evoked by your work.

ACKNOWLEDGEMENTS

And to my supervisor, Mrs R. Gopo, whose academic rigour, forbearance and positive critical intervention, I owe a very great debt of gratitude, which influenced the quality and the course of this piece of writing. Her security studies expertise and unwavering assistance to give feedback were untenable all through the research process.

I am grateful sincerely to the Zimbabwe Republic Police and to the officers of the Criminal Investigation Department of Harare central in particular who freely gave of their time, shared their experiences in their various operations, and participated in questionnaire surveys and interviews. They provided empirical foundation to this dissertation by their practical insights.
I want to thank the Faculty of Commerce and Humanities at the Bindura University of Science Education because of the intellectual climate and milieu that I enjoyed there, and to my fellows in the BBA Police and Security Studies course, due to the generative academic discourse that we shared.

Lastly, I would like to recognize the published works of the scholars, policy analysts, and institutions whose articles I have consulted in the development of the theoretical and empirical bases of this research. Any mistakes and omissions that now remain are all mine.

Table of Contents

RELEASE FORM i

APPROVAL FORM ii

DECLARATION iii

ABSTRACT iv

DEDICATION v

ACKNOWLEDGEMENTS vi

LIST OF TABLES xii

LIST OF ABBREVIATIONS AND ACRONYMS xiii

CHAPTER ONE 1

INTRODUCTION AND BACKGROUND TO THE STUDY 1

1.1 Background to the Study 1

1.2 Statement of the Problem 2

1.3 Research Questions 3

1.4 Purpose of the Study 3

1.5 Research Objectives 3

1.6 Significance of the Study 4

1.7 Assumptions 4

1.8 Delimitations 5

1.9 Limitations of the Study 5

1.10 Ethical Considerations 5

1.11 Definition of Key Terms 6

1.12 Chapter Summary 7

CHAPTER TWO 8

LITERATURE REVIEW AND THEORETICAL FRAMEWORK 8

2.1 Introduction 8

2.2 Conceptual Definition of Cyber Security 8

2.3 The International Landscape of Cybercrime....9
2.4 The African and Zimbabwean Context....10
2.4.1 The African Cybercrime Landscape....10
2.4.2 The Zimbabwean Context....10
2.5 Legislative and Regulatory Framework....11
2.6 Conceptual Framework....11
2.7 Theoretical Framework....12
2.7.1 Technology Acceptance Model (TAM)....12
2.7.2 Situational Crime Prevention (SCP) Theory....13
2.7.3 Routine Activity Theory (RAT)....13
2.8 Review of Previous Studies....14
2.8.1 Cyber Security Tools Currently in Use in Commercial Crime management....14
2.8.2 Effectiveness of Cyber Security Tools in Preventing, Detecting, and Investigating Commercial Crimes....15
2.8.3 Challenges and Limitations Faced by the CID in Implementing and Utilising Cyber Security Tools....17
2.8.4 Strategic Recommendations for Improving the Effective Use and Implementation of Cyber Security Tools....18
2.9 Gap Analysis....20
2.9.1 Absence of ZRP-Specific Empirical Research....20
2.9.2 Absence of an Integrated Analytical Framework....20
2.9.3 Under-Theorisation of the Zimbabwean Digital Policing Context....20
2.9.4 Longitudinal Quantitative Data Deficits....21
2.10 Chapter Summary....21
CHAPTER THREE....22
METHODOLOGY....22
3.1 Introduction....22
3.2 Research Methodology....22

3.3 Research philosophy 22
3.3 Research Design and justification 23
3.4 Research Approach 23
3.5 Target Population 23
3.6 Sample Size 24
3.7 Sampling Techniques 24
3.7.1 Stratified random sampling 24
3.8 Data Collection Instruments 24
3.8.1 Primary Data 24
3.8.2 Secondary Data Sources 26
3.9 Data collection and appropriateness of procedures 26
3.10 Data presentation 26
3.11 Data analysis method 27
3.11.1 Quantitative Analysis 27
3.11.2 Qualitative Analysis 27
3.12 Reliability and Validity 27
3.13 Ethical Considerations 28
3.14 Chapter Summary 28
CHAPTER FOUR 29
PRESENTATION, ANALYSIS AND DISCUSSION OF DATA 29
4.1 Introduction 29
4.2 Response Rate 29
4.3 Distribution of Questionnaires and Biographical Profile of Respondents 30
4.4 Research Objective One: Cyber Security Tools Currently in Use 31
4.4.1 Interpretation and Discussion 32
4.5 Research Objective Two: Effectiveness of Cyber Security Tools 33
4.5.1 Effectiveness in Prevention 34

4.5.2 Effectiveness in Detection 35
4.5.3 Effectiveness in Investigation 37
4.6 Longitudinal Detection Rate Trends, 2020–2025 38
4.7 Research Objective Three: Challenges and Limitations 40
4.7.1 Skills Shortages (86.7%) 40
4.7.2 Infrastructure Limitations (80.0%) 41
4.7.3 Resource and Budget Constraints (76.7%) 41
4.7.4 Jurisdictional and Legal Complexities (70.0%) 42
4.7.5 Underreporting of Commercial Crimes (63.3%) 42
4.8 Discussion of Results in Relation to Previous Studies 43
4.9 Chapter Summary 44
CHAPTER FIVE 45
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 45
5.1 Introduction 46
5.2 Conclusion of study. 46
5.3 Summary of the major findings 46
5.4 Conclusions 47
5.4.1 Development of operational cyber security tools 47
5.4.2 Use of cyber security tools enhance crime detection and investigation efficiency 47
5.4.3 Skills and expertise deficit in the application of cyber security tools 47
5.4.4 Structural barriers to the effective utilisation of cyber security tools 48
5.4.5 Integration with international communities to combat cyber crimes 48
5.4.6 Underreporting of commercial crimes 48
5.5 Recommendations 48
5.5.1 Investment substantiated by Structured, Multi-Layering Training Programmes 48
5.5.2 Phased Infrastructure Modernisation 49
5.5.3 Development of a Special Cybercrime Investigation Unit. 49

5.5.4 Sstrengthened Inter-Agency and International Cooperation.....49
5.5.5 Focused Public Education and Good-Neighbour Reporting Campaigns.....49
5.5.6 Legislative Review Protocol Standardisation. 50
5.6 Study contributions. 50
5.7 Directions for Future Research 50
5.8 Concluding Statement.....51
REFERENCES 52
APPENDICES: RESEARCH INSTRUMENT.....58
APPENDIX 1: QUESTIONNAIRE GUIDE 59
APPENDIX 2: INTERVIEW GUIDE 66

LIST OF TABLES

Table 4. 1: Questionnaire Response Rate 29
Table 4. 2: Biographical Profile of Respondents (n=27) 30
Table 4. 3: Cyber Security Tools Currently in Use at CID Harare Central (% of Respondents Reporting Regular Use, n=27) 31
Table 4. 4: Perceived Effectiveness of Cyber Security Tools in Crime Prevention (Likert-Scale Response Distribution, n=27) 34
Table 4. 5: Perceived Effectiveness of Cyber Security Tools in Crime Detection (Likert-Scale Response Distribution, n=27) 35
Table 4. 6: Perceived Effectiveness of Cyber Security Tools in Crime Investigation (Likert-Scale Response Distribution, n=27).....37
Table 4. 7: Mobile Money Fraud Detection Rates by Availability of Digital Forensics Evidence, 2020–2025.....39
Table 4. 8: Challenges and Limitations in Cyber Security Tool Implementation (n=27) 40

LIST OF ABBREVIATIONS AND ACRONYMS

AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
BEC	Business Email Compromise
BUSE	Bindura University of Science Education
CCTV	Closed-Circuit Television
CID	Criminal Investigation Department
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organisation
NIST	National Institute of Standards and Technology
PAM	Privileged Access Management
SADC	Southern African Development Community
SCP	Situational Crime Prevention
SIEM	Security Information and Event Management
SPSS	Statistical Package for the Social Sciences
SWGDE	Scientific Working Group on Digital Evidence
TAM	Technology Acceptance Model
UNODC	United Nations Office on Drugs and Crime
ZRP	Zimbabwe Republic Police

CHAPTER ONE

INTRODUCTION AND BACKGROUND TO THE STUDY

1.1 Background to the Study

Commercial crimes, which include white-collar crime and those committed for financial gains such as fraud, corruption, embezzlement, money laundering, intellectual property crime, and cyber-enabled financial crime, are among the biggest threats to economic security of the twenty-first century. On a global scale, cybercrime will cost the world's economy $10.5 trillion per year by 2025. This will include not just monetary losses but also the indirect costs of reputation damage, fines from regulators, the cost of recovery from any attacks, and gradual loss of trust on online platforms (Cyber Security Ventures, 2025). This is no abstract concept because these losses are real and felt by many individuals, households, and firms that have seen their financial security harmed by criminals exploiting the online environment.

The broad use of digital technologies has led to a drastic change in the criminal methodological approach. Criminals use various online applications, mobile money transaction systems, crypto currency transaction platforms, phishing scams, ransom ware system, and social engineering approaches that often exceed the ability of law enforcement agencies to adapt and respond to them. In this regard, police departments around the globe have made use of various cyber security solutions like digital forensics tools, AI analytics, facial recognition systems, CCTV systems, AFIS systems, GPS systems, and security information and event management (SIEM) systems (INTERPOL, 2025; NIST, 2023).

In Africa, the issue of cybercrime has become one of the fastest growing and most economically destructive threats to the criminal world. According to the INTERPOL Africa Cyber Threats Assessment Report (2025), some of the threats include BEC, ransomware, fraud and transnational financial crimes. All these threats have been made worse due to fast growth of internet access, high mobile money usage and poor digital infrastructure security, especially in Sub-Saharan Africa. Zimbabwe is no exception to all these threats facing the continent.

The economic difficulties in Zimbabwe as well as its rapid digitalization processes have become the main contributing factors for the emergence of commercial and cyber-enabled crimes. ZRP has been consistently recording an increasing number of such crimes in the

country. However, the sharp increase in cybercrimes in 2018, marked by more than 4,000 cases with total losses amounting to USD 40 million, was not an exception; rather, it was just a start, with further increases in mobile money scams, card cloning, identity fraud, phishing, and ransomware attacks being reported by Moyo and Mukura (2023), NewZimbabwe.com (2025), and TechZim (2026).

The Criminal Investigations Department (CID) via its Commercial Crimes Division, Cybercrime Unit, and Asset Forfeiture Unit has the main institutional mandate to investigate these crimes. The introduction of the Cyber and Data Protection Act [Chapter 12:07] in 2021 was a milestone achievement for Zimbabwe in terms of legislation through criminalizing cybercrimes, setting rules for collecting cyber evidence, and establishing cooperation on law enforcement in international laws (Government of Zimbabwe, 2021). However, despite this legal advancement, there is a challenge of implementation of the cyber security measures adopted by the ZRP due to lack of resources, skills, and infrastructure. The current research will be carried out to analyze the CID of Harare Central regarding these challenges.

1.2 Statement of the Problem

In spite of all the legislative steps taken through the introduction of the Cyber and Data Protection Act of 2021 (Government of Zimbabwe, 2021) and the expressed organizational readiness of the ZRP to adopt advanced cyber security solutions, commercial crimes have been increasing at an alarming rate and are posing great damage to Zimbabwe's economy. Various cases of mobile money fraud, phishing, ransom ware infection, business email compromise, and financial industry disturbances have been observed during the period of time considered for the research (NewZimbabwe.com, 2025; TechZim, 2026; Moyo and Mukura, 2023).

There exists a set of operational issues that adds to the list of difficulties. First and foremost, a widespread phenomenon of underreporting, which is motivated by a victim's shame and lack of public understanding about the reporting process, makes the recorded crime volume a considerable underestimate of reality. Second, jurisdiction problems in relation to cross-border cases make investigation difficult even for highly qualified investigators. Third, a lack of proper specialized training makes many CID officers unprepared to work with modern equipment. All these factors together lead to an environment where investigation periods are long and detection and conviction rates are low.

The criminals, on their side, have become more advanced with each passing day. They use methods such as encrypted communication, crypto currency transaction processes, and ever-

developing malware, which means their capabilities surpass those of the police in many aspects. The previous researches and reports about the potential of cyber security tools in improving the situation theoretically are well-known, but there is no concrete evidence of their operational effect when it comes to the CID of the ZRP. It is the gap that this research aims to bridge.

1.3 Research Questions

This study is guided by the following four research questions:

1. What cyber security tools are currently employed by the ZRP's CID at Harare Central in managing commercial crimes?
2. How effective are these cyber security tools in preventing, detecting, and investigating commercial crimes within the CID over the period 2020 to 2026?
3. What challenges and limitations are faced by the CID in implementing and utilising cyber security tools?
4. What strategies can be recommended to enhance the effective implementation and use of cyber security tools in commercial crime management within the ZRP?

1.4 Purpose of the Study

This study aims to critically evaluate the effectiveness of cyber security tools employed by the ZRP's CID at Harare Central in managing commercial crimes and to provide actionable, evidence-based recommendations for their optimisation in a resource-constrained policing environment.

1.5 Research Objectives

The study is guided by the following specific objectives:

1. To identify the cyber security tools currently in use by the CID at Harare Central in commercial crime management.

2. To determine the effectiveness of these cyber security tools in preventing, detecting, and investigating commercial crimes within the ZRP's CID over the period 2020 to 2026.

3. To investigate the challenges and limitations faced by the CID in implementing and utilising cyber security tools.

4. To formulate strategic recommendations for improving the effective use and implementation of cyber security tools in commercial crime management within the ZRP.

1.6 Significance of the Study

1.6.1 to the Zimbabwe Republic Police and the CID

This study offers empirical information on the practices, signs of effectiveness, and difficulties associated with tool utilization in the CID activities in Harare Central. The information and recommendations presented will help to formulate evidence-based policy changes, targeted training programs and resource allocation strategies to improve the investigation capabilities and efficiency of the ZRP in dealing with commercial crimes.

1.6.2 to Policymakers and Legislators

This study will provide empirical information which will help to design the policy changes that can make the Cyber and Data Protection Act and other national cyber security frameworks more effective in reducing cyber vulnerability of Zimbabwe.

1.6.3 to the Financial Sector and Private Organisations

Private banks, mobile banking companies, and businesses that suffer more from business and cyber-based crimes will find an increase in their knowledge regarding the capabilities and weaknesses of law enforcement useful. The recommendations for better cooperation between the private sector and law enforcement will help decrease costs and increase preventive efforts.

1.6.4 to the Society.

Through the investigation of the business crimes' patterns that erode the sense of trust in society and threaten the economic processes, this study brings about greater safety for society at large. Improved law enforcement efficiency will ensure better digital security, lower individual and collective victimisation and increase public trust in Zimbabwe's institutions.

1.6.5 to Academic and Research Communities

This paper contributes to the developing literature on cyber policing in Sub-Saharan Africa through an empirical analysis of the gaps that exist in literature with respect to technological adoption and efficiency of such technologies in policing environments with limited resources. The TAM-SCP conceptual framework is a useful analytical tool which can be employed in future comparative studies.

1.7 Assumptions

It is assumed that cyber security technologies have been adopted by organizations and hence the ability to give reliable information, and effectiveness of such technologies can be measured through a reduction in cybercrime incidents.

1.8 Delimitations

The geographical scope of the research shall be limited to the CID in Harare Central, together with some selected CID stations at provincial level. In terms of time, the research period shall span from 2020 to 2026. However, this study will limit itself strictly to cyber security tools only.

1.9 Limitations of the Study

1.9.1 Methodological Limitations

The method of case study analysis with the use of mixed methods is very efficient at creating an adequate contextual understanding but constrains the ability to generalize findings to contexts outside the CID. Self-reports provided via questionnaires and interviews may be subjected to biases and social desirability issues, thereby hindering the precision of perceptions about tool effectiveness.

1.9.2 Access-Related Limitations

Limited access to classified operational data, confidential cases, and some performance indicators within the CID was unavoidable due to research being performed in a law enforcement agency.

1.9.3 Time-Related Limitations

Research has considered data till 2026. Considering the speed of changes occurring in technology along with the changing ways of conducting crimes, some conclusions might not be applicable for longer periods. Also, the time period considered for research has affected data gathering.

1.9.4 Ethical and Institutional Limitations

Considering the need to ensure confidentiality of participants and institutions, especially the law enforcement agencies working on sensitive matters, there has been certain restriction in terms of answers provided by participants.

1.10 Ethical Considerations

The study strictly conforms to all existing ethical standards in research, which include voluntary participation, informed consent, confidentiality, anonymity of data, and non-maleficence. Ethical approval was granted by the Research Ethics Committee of Bindura University of Science Education and concerned ZRP authorities before conducting the research. Informational sheets were given to all participants regarding the objectives of the research, and informed consent was sought from all respondents. The data were kept confidential and could be accessed only by the researcher and the supervisor.

1.11 Definition of Key Terms

Commercial Crimes

There have been a number of attempts to define commercial crimes by scholars based on the legally and socially complicated nature of the offense. Edelhertz (1970, p. 3) defines commercial crimes as "an illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to obtain money or property." Friedrichs (2010, p. 5) adds onto this by defining commercial offenses as "offenses committed by individuals of respectability and social standing in the course of commercial, financial, or business activity." Based on these definitions and in consideration of the law enforcement practices of Zimbabwe, commercial crimes can be defined, in the context of this study, as non-violent, financially motivated offenses committed in the course of commercial or business transactions.

Cybercrime

As stated by the UNODC (2021, p. 12), “cybercrime refers to the criminal conduct involving use of ICT and/or ICT tools either as a means of attacking or accessing networks, systems, information/data or devices or as a tool facilitating such criminal activity.” In addition, INTERPOL (2023, p. 4) states that there are two types of cybercrimes: cyber-dependent and cyber-enabled. Cyber-dependent crimes depend entirely on ICT while cyber-enabled crimes refer to conventional offences aided by ICT. This paper considers cybercrime as an offense carried out through ICT networks and infrastructure as provided under the Cyber and Data Protection Act [Chapter 12:07] of Zimbabwe (Government of Zimbabwe, 2021).

Cyber Security Tools

According to NIST (2023, p. 8), cyber security tools are defined as “technologies, software, and procedures used to protect computers, networks, data and digital devices from any unauthorized access or attacks.” On the other hand, the IACP (2024, p. 2) defines cyber security tools in terms of law enforcement as “tools used for prevention, detection, collection of evidence and investigation of any cyber threat.” In the current study, cyber security tools are defined as all the technological and digital tools used by the ZRP’s CID to detect and investigate commercial crimes.

Effectiveness

According to Gottschalk (2010, p. 43), “effectiveness within law enforcement refers to the degree to which an organization attains its desired objectives and results within specific operational boundaries.” In regard to the current research, the researcher operationalizes the term “effectiveness” as the degree to which the use of cyber security tools results in measurable outcomes in relation to preventing, detecting and investigating business crimes.

1.12 Chapter Summary

This chapter has established the conceptual and contextual framework for the research. This includes an analysis of the evolution of commercial and cyber-crime from global predictions to the unique circumstances prevailing in Zimbabwe, statement of the research problem and its importance, as well as research questions, objectives, importance, scope, and limitations. The definitions of the terminologies involved provide the conceptual basis of all further analysis in the thesis. Chapter Two elaborates on the theoretical and empirical framework of the thesis.

CHAPTER TWO

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

The chapter provides a well-rounded and critically engaging literature review as well as theoretical framework informing the effectiveness of the use of cyber security tools in commercial crimes management within the CID of the Zimbabwe Republic Police in Harare Central. From the global, African, and local perspective, this chapter explores the state of the art in terms of where the study stands within the existing body of knowledge and the gaps which this research intends to fill. This chapter is thematic in nature, beginning with defining the concept of cyber security, followed by global issues related to commercial and cybercrime, legislation on these matters, a critical discussion of the cyber security tools, effectiveness of these tools, the challenges involved in their application and finally the theoretical framework of the study.

2.2 Conceptual Definition of Cyber Security

In approaching the body of academic research that exists regarding both cyber security and law enforcement, it becomes critical first to define cyber security, as the concept of cyber security has been defined in varying ways depending on the field and jurisdictional boundaries, which are of importance in the context of law enforcement and commercial crime control.

According to International Telecommunication Union (ITU, 2009), cyber security involves tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, best practices, assurance and technologies for protecting the cyberspace and organization's and the users' assets. This definition is comprehensive in terms of its inclusion of technical tools and processes, and hence is suitable for application within the domain of law enforcement.

The authors Von Solms and Van Niekerk (2013) present a more refined perspective on the subject by making a distinction between the concept of information systems security which is known as information security and the broader issues that are involved with cyber security. It should be noted that according to their perspective, cyber security needs to consider the aspects of human safety and society, not only the protection of data infrastructures. This issue is particularly significant when considering the investigations of business crimes.

Craigen et al. (2014) describe cyber security as the systematization of all resources, processes, and structures for the protection of cyberspace and cyberspace-dependent systems from any events which have a mismatch between de jure and de facto property rights. The property rights theory of cyber security is highly relevant in cases of commercial crime because it involves the theft of property rights like money, intellectual property, and personal information.

In this particular study, cyber security can be considered as the totality of digital forensic instruments, investigation software, analytic programs, surveillance technologies, and processes employed by the police, particularly the ZRP CID, in order to prevent, detect, investigate, and successfully prosecute commercially motivated cyber-enabled and cyber-dependent crimes. This is an operational definition that considers both the technological and procedural aspects of cyber security, taking into consideration the reality of policing in an under-resourced environment in Africa.

2.3 The International Landscape of Cybercrime

Businesses and computer enabled crimes represent the prevalent criminal opportunities for the internet. According to Cyber Security Ventures (2025) in the year 2025 losses stemming from cybercrime will be expected to cost the globe US$10.5 trillion-which includes the amount of money paid in ransom and remediation costs, regulator fines, business losses due to stolen intellectual property and damage to the reputation of organizations due to reduced institution trust. This is a monetary sum that is comprised of both individual organizations and governments across global networks.

Commercial crimes have been classified by Gottschalk (2010) as a subset of white collar crimes which create highly corrosive impacts in the economy, where competition is distorted, investment is discouraged, and trust is eroded. In Gottschalk's study of proliferation of online platforms, he found that an increase in the number and sophistication of commercial crimes has occurred because of the technologies that facilitate criminals to work across jurisdictions.

As posited by Button & Cross (2017), classical law enforcement approaches built on the foundations of physically tangible evidence and geographically localized criminal activities remain utterly inadequate in dealing with the speed, scale, and virtuality of cybercrime. The authors contend that the use of cyber security tools in this scenario amounts to much more than an advancement in technology it heralds a shift in law enforcement philosophies that require entirely new investigative capabilities.

According to Kshetri (2013), through the framework of structural political economy analysis, the author is able to identify the underlying structural inequalities in the distribution of resources required for developing the digital infrastructure and cyber security capabilities as elements that expose developing countries to vulnerability towards cyber-enabled crimes as well as making these countries ill-equipped to deal with such crimes.

2.4 The African and Zimbabwean Context

2.4.1 The African Cybercrime Landscape

While the burgeoning digital economy of Africa presents immense economic opportunities for Africans, it has also been associated with more exposure to cyber-based business crimes. According to the INTERPOL Africa Cyber Threat Assessment Report (2025), Business Email Compromise, ransomware, online frauds, and transnational financial crimes have been found to be the most common cyber threats and economically disruptive in Africa. In his study, Choo (2011) observes that the structural weaknesses in African law enforcement institutions include their inability to cope with cyber-related crimes because of a very high mobile money adoption rate and poor regulation. According to Grobler, Louwrens, and van Vuuren (2011), the South African case presents structurally similar structural weaknesses in the law enforcement institutions of Sub-Saharan African countries.

2.4.2 The Zimbabwean Context

Zimbabwe provides a unique, particularly complex research landscape combining economic volatility with the dynamism of mobile technology in the country's rapid shift towards digital financial transaction; coupled with underfunded, overworked policing and judiciary institutions that lack capacity or expertise to contend with the complexities of digital crime. The period from 2018 to the present has witnessed 'a huge jump' in the country's cyber-related commercial crime activities, with banks bearing the 'highest demand to upgrade their police force cybersecurity capability' according to Moyo and Mukura (2023). NewZimbabwe.com (2025) & TechZim (2026) provide numerous reports and articles related to this issue in the country, pointing in particular to 'a unique and rapid increase in mobile money fraud', the solution for which lies in using 'tools and methods' unique to 'mobile money'.

The Cyber and Data Protection Act [Chapter 12:07] (Government of Zimbabwe, 2021) is a significant legislative development because it has brought together the various laws under one Act, criminalises both cyber dependent and cyber enabled crimes, and sets out processes to collect digital evidence and also to form a Cyber Security Centre for the country. However, the

surveillance provisions of the Act bring about issues regarding civil liberties which need to be handled independently through oversight, as highlighted by Karekwaivanane (2021). Essentially, literature proves that effective legislation does not necessarily guarantee investigative efficiency unless it is accompanied by human and technological resource input.

2.5 Legislative and Regulatory Framework

The legal framework of Zimbabwe regulating the handling of cybercrimes has changed a lot since. Before the advent of the Cyber and Data Protection Act of 2021, there were several laws that dealt with the subject matter, scattered in the Computer Crime and Cyber Crime Act of 2017, the Postal and Telecommunications Act, and other subsidiary legislation; however, these laws had their own weaknesses. The 2021 Act brought about the change by criminalizing cyber-dependent and cyber-enabled crimes, providing for procedure for gathering and presenting digital evidence in criminal matters, and setting up an institutional framework for Cyber Security Centre in Zimbabwe (Government of Zimbabwe, 2021).

The Budapest Convention on Cybercrime (Council of Europe, 2001) is the most widely adopted model at the international level for ensuring uniformity in the formulation of cybercrime laws and cooperation among international law enforcement agencies. Failure by Zimbabwe to accede to the Convention places a serious obstacle in its ability to conduct international investigations into cybercrimes, an obstacle that is very important considering the transnational nature of most business-related cybercrimes. South Africa's experience, which has adopted laws regarding cybercrimes and developed bilateral cooperation arrangements, can serve as an example for Zimbabwe.

2.6 Conceptual Framework

The conceptual framework of this research shows the dynamic relationship among the major variables that will influence the effectiveness of cyber security tools in managing commercial crime. Cyber security tools which include forensic tools, AFIS, CCTV surveillance systems, SIEM, artificial intelligence-based analytics, GPS, and network intrusion detection system have been taken as an independent variable, whereas commercial crime management, which includes the rate of prevention, rate of detection, quality of investigation, and success in prosecution, have been identified as a dependent variable.

These interactions are moderated by a particular set of institutional variables within the ZRP CID: officer training competency and frequency, digital infrastructure availability, inter-agency protocols on data sharing, legislative framework governing digital evidence, and

specialized technical expertise. Within the conceptual framework, it is argued that the effectiveness of the technical tool is not a direct consequence of its inherent capabilities but depends on the enabling institutional environment. A technically proficient tool used in an environment marked by low skill sets, poor infrastructure, and legal uncertainties is bound to produce significantly reduced effectiveness results.

In addition, the model shows feedback loops relating to the effects of effectiveness and investment in institutions, whereby organizations that have been able to show effectiveness using their cyber security tools will be able to get the necessary institutional investment to maintain the level of effectiveness. On the other hand, if there is no evidence of effectiveness, then the organization can be trapped in a vicious circle of not being able to invest and perform.

Specific context-related factors which have not been used by other studies because they are unique to Zimbabwe such as the limitations on the economy of the country, the role of mobile money in financial crime and cyber security, absence of adherence to the Budapest Convention, and the resource level of the ZRP are considered as the boundary conditions that affect the nature of the relationships between tools, institutional moderators, and outcomes in the proposed theoretical framework.

2.7 Theoretical Framework

In this study, three complementary theories underpin the analysis. These include the Technology Acceptance Model (TAM), Situational Crime Prevention (SCP) Theory, and Routine Activity Theory. The three theories are used to analyze the adoption and use of cyber security tools by the ZRP CID. This is because each of these theories provides an insight into the research problem in different ways.

2.7.1 Technology Acceptance Model (TAM)

Technology Acceptance Model, which was first developed by Davis (1989) and further refined by Venkatesh and Davis (2000), offers a theory-driven approach to understand the process of acceptance and integration of technological innovations into organisational settings. As per TAM, the technology acceptance behaviour is fundamentally driven by two basic psychological determinants, namely, perceived usefulness, defined as the extent to which an individual feels that adoption of the technology would improve his or her job performance and perceived ease of use, which is the extent to which an individual perceives that the technology can be used without any mental or physical effort.

As used in this research, TAM is a framework through which the analysis of different patterns of adoption of cyber security tools by CID officers in Harare Central can be done. The framework suggests that officers perceiving such tools as useful and technically easy to use are more likely to adopt them actively and skilfully in conducting investigations. Limited adoption of tools such as AI analytics and network monitoring is thus likely to be explained within the scope of TAM in terms of their limited perceived usefulness or higher perceived technical complexity. The ability of TAM to account for moderating factors outside the model, like training, organizational support, and infrastructure, renders it especially useful in these constrained police setting.

2.7.2 Situational Crime Prevention (SCP) Theory

Situational Crime Prevention theory, conceptualised by Clarke (1980) and then further developed by Cornish and Clarke (2003), rests on the idea that crime may be prevented not only through motivational approaches aimed at offenders but also through changes in situational factors which enable criminal acts. The five main types of situational prevention include increasing the effort required to conduct crime, increasing risk (the chances of being detected or punished), reducing the reward (reducing incentives from committing a crime), reducing provocations (situational triggers) and removing excuses (clarification of behaviour norms and rationalisation removal).

Translating into the commercial crime context, SCP offers an invaluable analytical lens for understanding how the use of cyber security technology changes the situational architecture of commercial opportunities for crime. Forensic technology increases the chances of being detected and successfully prosecuted; surveillance technology and AFIS technology increases the probability of physical identification; data analysis systems decrease the gains from committing fraud by speeding up asset recovery; network systems increase the effort needed to commit financial crime undetected. Collectively, these processes influence the cost-benefit analysis that a potential offender is able to carry out.

2.7.3 Routine Activity Theory (RAT)

Routine Activities Theory is a concept introduced by Cohen and Felson (1979). It states that crime results from the coming together in both space and time of three essential conditions: the presence of an offender who wishes to commit crime, a viable target of the offence and the lack of a competent guardian. This theory focuses on the effect of routine activities in the

environment in either creating or inhibiting criminal opportunities. This theory has been widely used to explain cyber-crimes.

As Felson and Boba (2010) apply the RAT concept in the digital space, cyber security tools emerge as another form of capable digital guardianship that, if applied well enough, would interfere with the convergences of motivated offenders and suitable targets, which make commercial cybercrime possible. All digital tools of forensics, intrusion detections, SIEMs, and real-time monitoring act together as digital guardians, making the targets less suitable, making the offenses more detectable, and lowering the attractiveness of the digital sphere as a place for committing commercial crimes. For the ZRP CID, according to the RAT concept, the efficiency of cyber security tools depends on the scope of coverage of the guardianship they offer: any gaps in the capabilities will leave opportunities for committing crime.

2.8 Review of Previous Studies

The below literature review on existing studies is structured thematically in accordance with the research objectives of this study. Each thematic sub-section discusses three to four empirical studies that are relevant to the study, discussing their findings and methodologies, and their implications to this study within the ZRP CID framework of Harare Central.

2.8.1 Cyber Security Tools Currently in Use in Commercial Crime management

Understanding the cyber security tools that have been put into use for commercial crime investigations will provide an appropriate empirical foundation in evaluating the success and weaknesses of these tools as used by the ZRP CID. The following three research works provide appropriate examples of such evidence.

In the third edition of his leading work on digital evidence and computer crime, Casey (2011) sets out a classification of the digital evidence examination software employed by police jurisdictions throughout the world, placing a particular emphasis on the investigative needs presented by commercial and financial crimes. According to Casey, the three most popular digital evidence examination platforms in the global arena are the Forensic Toolkit (FTK), EnCase, and Autopsy because “the functionality provided by these programs permit the recovery of erased files, analysis of transaction paths and production of courtroom quality Forensic reports. “Casey goes on to report that “mobile forensics tools such as Cellebrite UFED and XRY “are the essential ones to the success of investigation, where in an environment that smartphones are widely used” as can be inferred in Zimbabwe’s money lending market with many money loan and money borrowing businesses in their cash less society”. Casey’s

conclusion that the type of digital evidence examination tool will be selected based on the underlying technical profile of the crime will apply equally for use by the ZRP CID.

In the key technical manual on intrusion detection and prevention systems published by the National Institute of Standards and Technology (NIST), Scarfone & Mell (2007) provide a detailed description of the operational structure of Security Information and Event Management (SIEM) systems and NIDS, which serve as key instruments in cyber security of organisations and law enforcement institutions. In particular, Scarfone and Mell define SIEM systems as those with the unique ability to correlate and aggregate security event data from different parts of digital infrastructure in real time in order to detect anomalies indicating commercial fraud, unauthorized access to accounts, and other risks related to insider attacks. Technical definition of SIEM provided by Scarfone and Mell may be used as an accurate point of comparison for the implementation of the tools within ZRP CID; moreover, identification of necessary integration elements (adequate bandwidth, server capacities, trained analysts) shows the required infrastructure for the implementation of the tools.

Jain, Ross & Prabhakar (2004) offer a detailed evaluation of the use of biometric identification techniques in law enforcement practice through the examination of Automated Fingerprint Identification System (AFIS), facial recognition software, and iris scanning technologies as tools of not only physical but also criminal identification. The comparative study of practical application of the technologies in various jurisdictions has revealed that proper operation of AFIS combined with digital forensics workflow allows cutting the time needed to identify suspects from days to minutes thus bringing considerable benefits to commercial crime investigations. Moreover, Jain et al. have stated that the most efficient use of biometric techniques lies in their integration into a larger framework of the investigative process including physical, digital, and video identification techniques. The evaluation by Jain et al. can serve as a standard to measure how far the ZRP CID has gone in this respect.

2.8.2 Effectiveness of Cyber Security Tools in Preventing, Detecting, and Investigating Commercial Crimes

Analysis of the effectiveness of cyber security tools regarding the prevention, detection, and investigation aspects of commercial crime control necessitates an investigation of empirical data that has been collected in different investigative and institutional settings. This discussion is mainly based on four studies.

Kshetri and Voas (2017) perform a comprehensive empirical evaluation of the efficacy of cybercrime deterrence techniques by considering how much the implementation of cyber security tools, including intrusion detection software, network monitoring software, and digital forensic tools helps achieve a reduction in commercial cybercrime rates. The study is based on 52 countries' data and finds a statistically significant negative correlation between the level of law enforcement's cyber security capabilities and the rate of commercial cybercrime. Thus, this finding proves empirically that highly capable and resourceful cyber security teams have a considerable deterrent effect an important conclusion in regard to the context of ZRP CID since deterrence potential of the implementation of cyber security tools in this context was never evaluated before. Moreover, the authors emphasize the importance of visibility of cyber security capability of law enforcement agencies, namely the number of arrests and prosecutions, as a critical part of deterrence strategy.

According to Holt and Bossler (2016), in their well-researched meta-analysis examining the impact of law enforcement's use of specialized digital tools to address cyber-crime in various jurisdictions, the presence of such tools leads to higher cybercrime detection and clearance rates as compared to traditional techniques used. Importantly, according to Holt and Bossler, one of the most significant variables influencing the effectiveness of the use of tools is the level and regularity of training provided to officers using the tools, which means that even high-end digital tools are not effective in the hands of inadequately trained officers. The above statement carries great significance for the ZRP CID, as the digital training of the ZRP officers appears to be infrequent and poorly conducted.

The study conducted by Stambaugh, Beaupre, Icove, Baker, Cassaday, and Williams (2001) offers the results of one of the earliest systematic empirical investigations of cybercrime investigation practice in law enforcement agencies and its relation to the role of digital forensics tools in creating a prosecutable case. According to the findings of the researchers, the factor that defines the success of cybercrime prosecution is the quality of digital evidence, including such aspects as the quality of evidence collection, documentation of the forensic process, and admissibility of digital evidence in accordance with appropriate rules. Stambaugh et al. state that agencies that have established digital forensics protocols and use quality-assured tools have much higher success rate of prosecutions compared to organisations using informal approaches to investigation, thus providing evidence on the usefulness of the systematic usage of tools. The finding of Stambaugh et al. can be applied to the case of ZRP CID due to the problems with evidence handling identified previously.

In their study about the use of computer forensics in commercial crimes, Nykodym, Taylor, and Vilela (2005) consider specifically how effective forensic software tools are in retrieving and verifying financial transaction records, e-mails, and other digital documents as valid evidence. According to the case-study approach used by the authors, digital forensic software is highly effective if it is used in a systematic investigative framework that involves a robust chain of custody process, an established forensic-based collection process, and well-prepared expert witnesses. In addition, Nykodym et al. highlight that, in most cases, the above mentioned methodological approaches are poorly developed in law enforcement agencies of developing countries, which creates a serious disparity between technology and practice. This gap has become a good reference point for the current research that considers the ZRP CID.

2.8.3 Challenges and Limitations Faced by the CID in Implementing and Utilising Cyber Security Tools

This body of literature identifies a set of similar obstacles that have prevented the successful deployment of cyber security technologies in law enforcement, especially within the policing environment in developing countries. There are three studies that deal directly with these issues in regard to ZRP CID.

According to Wall (2007) who made a seminal contribution into the literature on cybercrime and policing in relation to which cyber security tools should be used, the skills deficit is the most essential and overarching problem that law enforcement agencies face when trying to employ cyber security tools. In particular, Wall claims that cybercrime investigation necessitates a particular degree of technical skill, namely, the skill to conduct network analysis, understand malware and cryptography and use databases which is quite different from the skills needed for investigating crimes in a traditional way. Furthermore, because of the constant development of criminal practices through technology, this skills deficit becomes a dynamically reproduced structural issue rather than a static one that can be easily overcome once and for all. Wall's conceptualization of the skills deficit as a dynamic problem rather than a static one is important for theoretical interpretation of training results observed in the ZRP CID.

Kshetri (2013), in a political economy approach to analyzing cybercrime in developing nations, highlights the way in which law enforcement agencies have to deal with problems related to old hardware and software, poor internet connectivity, insufficient server space, and poor data storage facilities, all of which limit the scope of use of cyber security tools. Kshetri also shows

that this problem of poor infrastructure is reinforcing, as inadequately equipped cyber security departments lead to fewer investments and therefore poor technical capability, which in turn results in fewer investigations and hence little incentive to invest. This pattern of underinvestment is clearly seen in the ZRP CID case, and the approach adopted by Kshetri offers an appropriate theoretical framework to explain this phenomenon. The comparative examples provided by Kshetri in his paper are useful for understanding the ZRP CID case as well.

Brenner (2010) focuses on the nexus between the investigation of cybercrime and criminal evidence law, emphasizing the issue of admissibility of digital evidence as a key problem that can make even technologically advanced tools of cyber security useless. Brenner explains that digital evidence is much more susceptible to challenges than physical evidence and that meeting such demanding criteria as chain of custody, forensic integrity, and admissibility of digital evidence in accordance with criminal procedures is a big challenge for law enforcement agencies in developing countries. If the legal standards of the admissibility of digital evidence are vaguely formulated, inconsistently interpreted by the court, and not fully comprehended by prosecutors, then the practical efficiency of cyber security tools will be greatly compromised during the prosecution process even if the tool has been utilized during the investigation appropriately. The legal-analytical approach used by Brenner is crucial for the present study which analyzes the connection between tool utilization quality and prosecution results in the ZRP CID.

2.8.4 Strategic Recommendations for Improving the Effective Use and Implementation of Cyber Security Tools

A number of evidence-based suggestions have been developed through the global and regional literature that can improve the effectiveness of cyber security tools in law enforcement, especially in the under-resourced law enforcement situations prevalent in Africa. Three specific studies offer the best strategic advice for ZRP CID.

According to Broadhurst (2006), in his detailed review of advancements in international efforts to combat cybercrime through law enforcement, a multi-tiered capacity-building strategy, which includes specialized training, infrastructure building, modernization of legislation, and international cooperative frameworks, should serve as the basis for effective enhancement of cyber security tools' effectiveness. Broadhurst suggests that the lack of any one component would be enough to make any of the other components less efficient. He claims that any partial

measures taken, such as equipping without providing training, or changing legislation without investing into infrastructure development, will not produce lasting results. The suggestions concerning creation of specialized units for cybercrime investigations, development of training programs for conducting digital investigations, and setting up international data sharing procedures will have a great practical meaning for ZRP CID. The practical evidence gathered by Broadhurst in the course of law enforcement capacity-building in Asia-Pacific countries facing similar structural challenges to Zimbabwe adds weight to his suggestions.

According to Oriola (2012) whose study focuses on experiences with commercial cybercrime investigations in Nigeria, a country that has many similarities with Zimbabwe in terms of structural features such as economic instability, high uptake of mobile money transfers and resource constraints in the police force, there is a recurring theme whereby the technological aspect is constrained by institutional factors. From the research carried out by Oriola, it emerges that digital forensic tools exhibit the most effective results when used together with the following components in place: comprehensive training of officers, specialist cyber units and prosecutorial services with digital evidence skills. Where at least one of these components is missing, then effectiveness of the tools becomes significantly low irrespective of the advancement of the tools used. Oriola's strategic suggestions of forming public-private partnerships for digital forensic support, inter-agency memoranda of understanding for data exchange and setting up fast-track prosecution processes for cybercrimes are relevant to the ZRP CID scenario.

Sibanda and Mpofu (2022), in their investigation of digital evidence management practices within the ZRP more broadly, identify significant inconsistencies in evidence-handling protocols, inadequate documentation practices, and limited officer awareness of digital evidence admissibility requirements. Based on this, Sibanda and Mpofu make the following recommendations: development and implementation of a standardized ZRP Digital Evidence Management Protocol; establishment of a quality assurance function for digital evidence in the CID; holding regular joint training sessions between the ZRP and National Prosecuting Authority for ensuring that digital evidence is collected according to both parties' requirements; and establishing secure digital evidence storage facilities. The abovementioned recommendations, being based on primary data obtained in the ZRP institutional context, have high analytical value for the current research and can serve as a baseline for developing the framework for recommendations in Chapter Five.

2.9 Gap Analysis

As indicated by the above literature review, although there is considerable amount of scholarly and practice-oriented research on cyber security technology, commercial crimes, and efficiency of law enforcement agencies in general, and to some extent in Africa, four major and inter-related lacunae in empirical and theoretical literature remain unexplored.

2.9.1 Absence of ZRP-Specific Empirical Research

In spite of the critical importance of the ZRP CID as the main body conducting investigations of commercial crimes in Zimbabwe, there is no scientific empirical research conducted on the use of cyber security tools within the ZRP CID, the operating conditions under which the use of such tools takes place, and the results obtained. All the literature available on the use of cyber security within the Zimbabwean police force is very general or anecdotal in nature, or indirect and taken from other industries such as banks. The present research fills this void and is the first empirical research on the matter based on primary data collected from CID officers and institutions in Harare Central.

2.9.2 Absence of an Integrated Analytical Framework

Existing studies of cyber security tools in law enforcement tend to address either the technology adoption dimension or the crime prevention effectiveness dimension, but rarely both within a single integrated analytical framework. This divergence limits analytical purchase, since adoption behaviour and effectiveness outcomes are not independent phenomena but dynamically interactive processes. The integrated TAM-SCP-RAT framework developed in this chapter addresses this gap by providing a theoretically pluralistic architecture that simultaneously captures adoption, situational prevention, and guardianship provision dimensions of tool effectiveness within a single coherent analytical structure.

2.9.3 Under-Theorisation of the Zimbabwean Digital Policing Context

The unique features of the Zimbabwean policing and criminal justice environment — a specific configuration of economic constraints, a distinctive digital financial ecosystem centred on mobile money, a particular legislative framework, and a policing institution with specific resource and capacity characteristics have not been adequately theorised in relation to cyber security tool effectiveness. Comparative studies in the regional literature tend to treat Sub-Saharan African policing contexts as broadly homogeneous, eliding country-specific institutional, economic, and legislative variables. This study contributes to closing this

theoretical gap by subjecting the Zimbabwean context to detailed empirical scrutiny through the lens of an analytically tailored theoretical and conceptual framework.

2.9.4 Longitudinal Quantitative Data Deficits

There is an important void in quantitative data on detection rates, time spent on investigations, and conviction rates related to commercial crimes handled by ZRP with the help of cyber security technologies. In the absence of such data, it is not possible to determine any trend in the efficiency of investigation processes, evaluate the effect of the new law on such efficiency, or compare the performance of the ZRP CID with other regional agencies. Despite the inability of the methodology used in this study to address the issue of data deficiency caused by the lack of reliable record-keeping practices in ZRP, an effort is made to obtain at least some quantitative data.

2.10 Chapter Summary

This chapter has attempted to construct a thematic literature review and theoretical framework of the research topic on the effectiveness of cyber security tools in managing commercial crimes within ZRP CID in Harare Central. The chapter commenced with a solid and robust operational definition of cyber security that was contextualized to the investigation environment, followed by a review of the literature on commercial crime and cybercrime on the international, Africa and Zimbabwean contexts, together with the legislative framework.

In this chapter, the conceptual framework was introduced, whereby the linkages among cyber security tools, institutional moderators, and business crime management were illustrated in the context of Zimbabwe. Following that was the introduction of the theoretical framework, which combined Technology Acceptance Model, Situational Crime Prevention Theory, and Routine Activity Theory to create a framework of analysis covering all aspects of effectiveness of cyber security tools.

Previous literature reviews have been conducted thematically based on four research aims of the study, namely: existing cyber security tools, efficacy of the tool in prevention, detection, and investigation, difficulties and constraints of implementation, and suggestions for improvement. Systematic gap analysis reveals four main empirical and theoretical gaps which the current study attempts to fill. The subsequent chapter outlines the research methodology in which this theoretical and conceptual framework is operationalized empirically in ZRP CID of Harare Central.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

The chapter describes the methodological architecture of the study, explaining the research philosophy, research design, research approach, and population, sampling strategy, data collection instruments, data analysis processes, measures of reliability and validity that jointly controlled the proceedings of the research. All methodological decisions are based on the theoretical framework done in Chapter Two and practical imperatives of carrying out empirical research in an institutional context of law enforcement.

3.2 Research Methodology

Jonker and Pennink (2010) define methodology as the process of defining and defending the logical order the researcher needs to follow in order to achieve a certain predetermined result such as knowledge, insight, intervention or change. They also state that methodology helps make the main outline of the approach transparent to the researcher and to academia and business. In fact, research methodology influences the actual research methods that are used to investigate a problem, and collect, analyze and interpret data (Dainty, 2008). The student mainly relied on secondary data to carry out the research though a little primary data was used to assess the effectiveness of cyber security tools in commercial crime management. Combined quantitative metrics, qualitative data and case analysis were used to assess the effectiveness of cyber security tools in commercial crime management.

3.3 Research philosophy

For the present study, the pragmatic philosophy is taken as the basis for examining the application of cyber security tools in commercial crimes investigation. According to the philosophical positioning, the best method for a particular study will be the one that successfully answers the research questions and achieves the goals of the study irrespective of the ontological and epistemological positions (Creswell and Creswell, 2018). Pragmatism philosophy does not limit the researcher to a single methodology, but it allows him or her to adopt several methodologies according to their appropriateness for dealing with the research question. This philosophical positioning is very appropriate in the area of cyber security

because both qualitative and quantitative aspects need to be considered in order to understand complicated phenomena.

3.3 Research Design and justification

The researcher has chosen a mixed-methods research design, which includes quantitative questionnaire surveys and qualitative semi-structured interviews to facilitate the triangulation of data and generate not only the statistical trends in them but also their contextual depth (Creswell and Plano Clark, 2017). The major quantitative element that was captured involves having measurable data on the patterns, frequency as well as perceived efficacy of the tool. The qualitative aspect was evoked to give in-depth operational aspects on the implementation issues, contextual constraints, and strategic suggestions. The research design used is embedded case study design with the CID at Harare central as the main case study. This design facilitates intensive, contextualised analysis in a particular, confined institutional context, whereas the mixed-methods design is important in ensuring that not only is statistical generalizability achieved within the sample but also is rich interpretative information obtained (Yin, 2018).

3.4 Research Approach

A mainly deductive methodology was followed, starting with the theoretical propositions of TAM and SCP and progressing to a step of empirical testing based on the data of questionnaires and interviews. In cases where some surprising topics arose through the collection of qualitative data, an inductive element was added as a way of letting theory be refined (Bryman, 2016).

3.5 Target Population

The target population involved members of the Zimbabwe republic police CID section at Harare central who are directly involved in the investigation, prevention or management of commercial crimes, and other pertinent stakeholders in related institutions. Such population includes detectives, IT and forensic experts, forensic investigators, CID commanding officers and the representatives of financial institutions with which the CID formally cooperates in investigating commercial crimes. The overall accessible population (using initial institutional consultations) approximated at around 120 individuals.

3.6 Sample Size

The researcher used a sample of 30 people from the Zimbabwe Republic Police Central Investigation Department that are directly and involved in the use of cyber security tools in managing commercial crimes in Zimbabwe. According to Hossack and Pollard (1998), a sample is a finite part of a standard population whose properties are studied to gain information about the whole population. Fig 2 below shows how the sample was selected.

3.7 Sampling Techniques

For sampling purpose, the researcher used non-probability sampling and created two groups from each of the four departments of CID namely the Vehicle Theft Squad department, Homicide department, Law and Order department and CID property, with one group comprising the heads of the departments and the other group the rest of the workers in those departments. For each department, the researcher selected one head of department using simple random method. The researcher then used systematic sampling technique to select from the alphabetically arranged workers names the remaining three respondents from each department to make them four respondents per department.

3.7.1 Stratified random sampling

Hunt et al (2001) proposed that it is a process of dividing members of the population into homogeneous subgroups before sampling. The researcher divides the entire target population into different subgroups or strata and then selects the final subject proportionally from the different strata. Since departments were randomly selected, the researcher provided them with simple and direct questions to answer. The departments were stratified according to functionality so as to find where relevant information is.

3.8 Data Collection Instruments

3.8.1 Primary Data

Questionnaire

The questionnaires were used because they are relatively inexpensive tools of collecting data from a large sample of individuals in different locations. This proved to be beneficial to the researcher since the research involved respondents from different sections of the CID. Francesca (2001) defines a questionnaire as a set of questions on a form which is completed by the respondent in respect of the research project. The following were the advantages of the questionnaires to the researcher;

- They allowed the participants to respond to the questions at their own pace.
- They ensure uniformity on the questions asked.
- They saved time as they administer to many participants at the same time.
- They allowed easy analysis and interpretation of the data collected.
- Geographical differences of the respondents did not affect their use.

They were however considered unpleasant to complete by respondents and hence a proportion of them had not been returned. Differences in interpreting the questions on the questionnaire by different respondents resulted in them producing wrong and unnecessary information.

Interviews

The telephone and face to face interview methods had also been used as data collection methods by the researcher. Interviews were used to provide clarity to the questions not answered well on the questionnaires and to get more information needed by the researcher to draw conclusion on the study. An interview is whereby the researcher call upon the respondents for a dialogue where he will ask questions that would already be laid down and the respondents will verbally explain their views. Emmanuel (2003) defines an interview as a verbal technique to gather data where respondents will give an on-spot response on the study area.

They provided the following advantages;

- They allowed immediate verbal feedback which proved to be reliable.
- They allowed quick conformation and further probing to credit analysis procedures. A high response rate had been observed compared to questionnaires.
- The tone on the speech of the respondents added emphasis to the interviewee's responses.
- They provided clarity in some questions with unclear answers in the questionnaire.

There was however the possibility that some of the interviewees answered with bias so as to please the researcher. Some of the respondents had no time for the interview since they had been occupied by certain organisational tasks.

Observations

Observations were used because they provided unbiased data on the role of strategic use of cyber security tools in the CID section as whole since the respondents would have participated on the interviews and the questionnaires in a way to please the researcher. An observation according to Walliman (2001) is a method of recording conditions, events and activities through the non-participant observer to eliminate from the research results the bias that results when people are aware that they are studied. Observations had the following advantages;

- They offered quick and effective method of gaining preliminary knowledge of the research
- They offered data that is free from bias unlike interviews and questionnaires when the respondents try to impress the researcher
- However, the observations consumed a lot of time, much time was wasted when the researcher have to wait for the research variables to happen when they were not constant.

3.8.2 Secondary Data Sources

The secondary data were collected in sources of CID annual crime statistics reporting covering period 2020 to 2025, national cybercrime incident logs, and published reports of government, INTERPOL and peer-reviewed academic literature. These data were contextual evidence of longitudinal nature which complemented and corroborated the prime data collected by the questionnaires and interviews.

3.9 Data collection and appropriateness of procedures

Having been working at the organisation for the past thirteen years in Zimbabwe Republic Police from 25 February 2014 to date the researcher had reasonable access to the organisation`s stuff in particular CID members for purposes of the research project. The questionnaires were distributed by the researcher himself and collected after a specified time so as to lessen the burden on the respondents of keeping the questionnaires whilst they completed answering the questionnaire. This also helped to ensure that the questionnaire got into the hands of the intended respondents during distribution and intended receiver of information during collection.

3.10 Data presentation

Data collected by way of questionnaires was analysed on the bases of frequency and that from the interviews was summarised. The responses from the questionnaires were expressed in their

percentages depending on the opinion expressed by the respondents. The researcher managed to check all the questionnaires that were received from the respondents to make sure that all of them were properly answered and to see if there were any unanswered questions. Data was presented in the form of graphs, diagrams and tables as indicated by the next chapter. The data from the interview questions was analysed and then summarised basing on the answers provided by the interview participants.

3.11 Data analysis method

3.11.1 Quantitative Analysis

The data of the quantitative questionnaires were entered in SPSS (Version 26) and subjected to descriptive statistical analysis, including frequencies, percentages, means and standard deviations. Pearson correlation analysis was done to find out the relationship between the frequency of tool use and the self-reported detection rates. In Chapter Four, results are given in tabular and graphical format, with chi-square tests used to determine the statistical significance of any significant differences where necessary.

3.11.2 Qualitative Analysis

Thematic analysis was conducted using six steps procedure outlined by Braun and Clarke (2006) to transcribe the interview data verbatim. The transcripts were coded inductively and deductively to identify recurrent themes based on the research questions and NVivo 12 software used to support systematic coding and management of themes. Quotations of participants, which are presented in Chapter Four, are anonymised to ensure protection of individual identity.

3.12 Reliability and Validity

The evaluation of the internal consistency of the Likert-scale questionnaire was by use of the Cronbach's Alpha which gave a coefficient of 0.81 - indicating high reliability (Nunnally, 1978). To enhance construct validity, it was ensured that the questionnaire items were based on the proposed constructs of TAM and SCP and the questionnaire also underwent expert review prior to finalisation. The overall validity and credibility of the research findings shape up tremendously due to triangulation of the sources of quantitative, qualitative and secondary data.

3.13 Ethical Considerations

Approval of the research by the Research Ethics Committee in Bindura University of Science Education and the concerned ZRP institutional authorities was obtained. Each participant was thoroughly informed about the research and agreed to participate in it, signing an informed consent. Later, participation was completely voluntary and participants were specifically made aware of their right to withdraw and incur no penalty at any point. Any data were anonymised and kept securely. The research was carried out in harmonious with the BUSE Research Ethics Policy, the operational recommendation of the ZRP, and the standards of the research profession police and security studies.

3.14 Chapter Summary

The chapter has outlined the methodology that the study was based on. Together, the pragmatist philosophy, mixed-methods design, stratified purposive sampling, multi-instrument data collection and analysis based on a triangulation are rigorous and contextually appropriate to answering the research questions of the study. The chapter below is a description of the empirical results that this methodology generated.

CHAPTER FOUR

PRESENTATION, ANALYSIS AND DISCUSSION OF DATA

4.1 Introduction

This chapter outlines, interprets and argues over the empirical findings of the research in systematic relation to the four research questions that informed the investigation. Primary data obtained with the help of questionnaires given to 30 CID officers and semi-structured interviews conducted with 10 key informants are combined with the data provided by CID crime statistics to create a multidimensional expression of cyber security tool usage and effectiveness in Harare Central. It is followed by quantitative results presented as professionally drawn figures and the results corroborated by qualitative means as based on interview data, with a conclusion on how to tie the findings into the theoretical framework agreed upon in Chapter Two.

Data Presentation and Analysis

Data was collected by means of questionnaires, observations, interviews and study of organisations past crime statistic records. Qualitative and quantitative analysis was used to analyse the gathered data. Microsoft excel package was used as a major tool for tabular and graphic presentation of the data. Other presentation forms such as bar graphs, area charts and pie charts were used to draw up conclusion.

4.2 Response Rate

Table 4.1 below shows the response rate achieved from the questionnaire distribution exercise.

Table 4. 1: Questionnaire Response Rate

Population / Category	Questionnaires Distributed	Questionnaires Returned	Non-Response	Response Rate (%)
ZRP CID Harare Central	30	27	3	90%

Source: Primary Data (2026)

Of all questionnaires issued, 27 out of the targeted 30 respondents returned completed questionnaires, yielding a response rate of 90%. The formula applied was: Relative Rate = (Absolute Response / Targeted Population) × 100 = 27/30 × 100 = 90%. Three individuals did not return their questionnaires.

A 90% response rate is considered exceptionally high in social science research. Babbie (2010) suggests that a response rate of 70% or above is considered adequate for survey-based research, meaning that the 90% achieved in this study significantly exceeds the acceptable threshold. This high response rate has several important implications for the findings of this study. First, it minimises the risk of non-response bias, meaning that the views of the 27 respondents can be considered broadly representative of the entire targeted population of 30 CID officers. Second, it enhances the reliability of the data, as the findings are drawn from a near-complete sample rather than a partial one. Third, this ensures that there is an improvement in the validity of the conclusions drawn from the data because of the high percentage participation, which means that there was little chance of excluding important insights or experiences from being part of the data set. Practically speaking, this implies that the 90 percent response rate means that the results given in this chapter are based on the opinions and experiences of the vast majority of CID officers dealing with cyber security tools in Harare Central.

4.3 Distribution of Questionnaires and Biographical Profile of Respondents

The questionnaires were equally distributed among the sections that were directly concerned with the application of cyber security techniques, such as: the Homicide Department, Property Department, Vehicle Theft Squad, Law and Order Department and the Forensic Department. The table below shows the demographic details of the respondent group.

Table 4. 2: Biographical Profile of Respondents (n=27)

Category	Sub-Category	Frequency / %
Designation	Detectives	60% (n=16)
	IT / Forensic Specialists	20% (n=5)
	Supervisory / Management	20% (n=5)
Years of Experience	Less than 5 years	27% (n=7)

Category	Sub-Category	Frequency / %
	5 – 10 years	40% (n=11)
	More than 10 years	33% (n=9)
Department	Homicide	22% (n=6)
	Property	22% (n=6)
	Vehicle Theft Squad	19% (n=5)
	Law and Order	19% (n=5)
	Forensic	19% (n=5)

Source: Primary Data (2026)

As illustrated in Table 4.2, 60% were detectives, 20% were specialists in IT and forensic, and the remaining 20% was made up of supervisors or managers. With regard to professional experience, 40% of the respondents had between five to ten years of experience working for CID, 33% had more than ten years of experience, while 27% had less than five years. Overall, 73% of the respondents had five or more years of experience working in CID, thus making the data reliable, as they are experienced investigators that can evaluate the use of cyber security tools from 2020 through to 2026.

4.4 Research Objective One: Cyber Security Tools Currently in Use

Objective One was aimed at determining the cyber security tools that are currently used by the CID for managing commercial crimes at Harare Central. Table 4.3 below shows the data on the rate of use of these tools.

Table 4. 3: Cyber Security Tools Currently in Use at CID Harare Central (% of Respondents Reporting Regular Use, n=27)

Cyber Security Tool	Number of Respondents	% Usage Rate
Digital Forensics Software	23	86.7%
CCTV Surveillance Systems	21	76.7%

Cyber Security Tool	Number of Respondents	% Usage Rate
Automated Fingerprint Identification System (AFIS)	19	70.0%
Data Analytics Platforms	15	56.7%
GPS Tracking	12	43.0%
AI-Driven Analytics	8	30.0%
SIEM Platforms	6	23.3%

Source: Primary Data (2026)

4.4.1 Interpretation and Discussion

Digital Forensics Software (86.7%): Digital forensics software emerged as the tool with the highest usage rate amongst the respondents. This technology is used in almost all forms of commercial crime investigation in CID. It is applicable in crimes such as mobile money frauds, cybercrime and financial document frauds. The high rate of usage is explained by the practical application value of the tool. Digital forensics software helps the investigator to recover, secure and analyse data from electronic gadgets that can be admitted in courts.

CCTV Surveillance Systems (76.7%): CCTV surveillance was the second most utilized tool. CCTV footage presents visual evidence that can be easily understood by the investigator, prosecutor, and the court, especially in investigations concerning access to banking halls, ATMs, and commercial areas. The high utilization of CCTV systems is further attributable to the huge investment made by both public bodies and private banking institutions in surveillance systems in Harare commercial areas.

Automated Fingerprint Identification System AFIS (70.0%): AFIS is one of the tools mentioned as regularly used by 70% of participants in the survey. In terms of being a biometric identifier, AFIS helps the investigators link latent fingerprints collected at crime scenes with a national database in order to verify the identity of a suspect in the absence of any digital footprint or inadequate data. This high rate of usage indicates the prior investment in biometric systems in Zimbabwe.

Data Analytics Platforms (56.7%): Only slightly less than half of the respondents used data analytics platforms. Such platforms allow law enforcement personnel to spot patterns within transactional data, create networks of fraudsters, and detect anomalies within financial documents. This relatively high usage may be attributed to the higher level of analytical skills needed in order to understand the results obtained, as well as the abstractness of such findings as opposed to physical evidence produced by other platforms.

GPS Tracking (43.0%): Fewer than half of the survey participants claimed to use GPS tracking technology. It is reactive technology used for asset tracking and verifying suspect locations. Low adoption rate is expected because GPS tracking is not a primary technology but rather a complementary one.

AI-Driven Analytics (30.0%): Just 30 percent of survey participants used AI analysis technology, and it can be stated that this technology is rarely used. The AI analysis technology provides predictive power and anomaly detection, but the low adoption rate is explained by its complexity.

SIEM Platforms (23.3%): Security Information and Event Management tools were the least utilized. These are used for collecting and correlating data in real time to detect and deal with security incidents. The low utilization of this tool implies that there is still much room for improvement in the development of the cyber security system of the CID.

Pattern of tools adoption extensive usage of practical and evidence-providing tools combined with substantial under-usage of complex and sophisticated analytical tools - corresponds to the research results available for the same type of law enforcement agencies. In his article, Broadhurst (2006) revealed the same pattern of digital forensics capabilities in a number of Sub-Saharan African police forces stating that preference was made for tools producing physical evidence rather than more complicated analytical instruments. Chukwuemeka and Eze (2020) confirmed in their research regarding Nigeria Police Force that forensics software and biometrics identification tools were used much more frequently than predictive analysis based on artificial intelligence. Interpol African Cyberthreat Assessment Report (2025) also revealed that in 49 African member countries advanced tools such as SIEM and AI analytics had very low penetration rate, mainly due to the lack of skills and resources.

4.5 Research Objective Two: Effectiveness of Cyber Security Tools

This second research objective investigated the effectiveness of cyber security tools in preventing, detecting, and investigating commercial crimes from the year 2020 to 2026. These

dimensions were measured through Likert scale questionnaires and semi-structured interviews under three sub dimensions: prevention, detection, and investigation.

4.5.1 Effectiveness in Prevention

Table 4.4 below presents respondent endorsements of cyber security tools' contribution to the prevention of commercial crimes.

Table 4. 4: Perceived Effectiveness of Cyber Security Tools in Crime Prevention (Likert-Scale Response Distribution, n=27)

Tool	Agree/Strongly Agree (%)	Neutral (%)	Disagree/Strongly Disagree (%)
CCTV Surveillance	53.3%	26.7%	20.0%
GPS Tracking	46.7%	30.0%	23.3%
Digital Forensics Software	40.0%	33.3%	26.7%
AI-Driven Analytics	26.7%	40.0%	33.3%

Source: Primary Data (2026)

As demonstrated in Table 4.4 below, all prevention tools show a moderate rate of endorsement for prevention. The prevention endorsement was the highest among the use of CCTV systems with a 53.3% endorsement, followed by GPS tracking with a 46.7% prevention endorsement, digital forensics with a 40.0% endorsement, and AI driven analytics with 26.7% endorsement.

CCTV Surveillance (53.3%): The use of CCTV systems had the highest percentage of prevention endorsement. The endorsement of this tool of prevention is due to the fact that the surveillance has been found to be able to deter the crime since it shows people that the activities taking place are under surveillance and will be recorded. The installation of CCTV in commercial banks, shops, and ATM walkways creates the impression that one can be identified based on the logic of situational crime prevention.

GPS Tracking (46.7%): GPS tracking had a prevention endorsement of 46.7%. Even though GPS tracking is used for investigation in reaction to offenses, the respondents noted its preventive capacity by serving as a preventive measure against crimes related to movements of stolen property or fraudulently acquired property. The sub-majority endorsement is due to the fact that GPS tracking can only act as a preventive measure if the offender knows that the property is being tracked.

Digital Forensics (40.0%): The prevention role of digital forensics is mainly indirect, working via certainty of detection, meaning the assurance that digital devices can be analyzed digitally discourages the offenders from carrying out the crime if they know the technology. Sixty percent of the respondents did not endorse this tool's prevention role because most forensic tools work in a reactive manner.

AI-Driven Analytics (26.7%): AI-driven analytics was the most poorly rated with regard to prevention. This is unsurprising considering the low rate of adoption of the technology. It has huge preventive potential through anomaly detection and prediction of unusual activities, yet this potential is not being fully realized at Harare Central in the current form.

The average prevention ratings are consistent with the observations made by Waxler & Nkurunziza (2018) regarding the predominant use of reactive cybersecurity technologies within the financial crimes units in East Africa. Chukwuemeka & Eze (2020) report that the units combating cybercrimes in Nigeria rated their technologies as more effective in crime detection and investigation than in crime prevention due to the institution’s focus on prosecution over disruption. The 53.3% prevention rating for CCTV systems is consistent with the 55% prevention rating reported by Mwangi et al. (2022) in Kenyan police units.

4.5.2 Effectiveness in Detection

Table 4.5 below presents respondent assessments of cyber security tools' contribution to the detection of commercial crime perpetrators.

Table 4. 5: Perceived Effectiveness of Cyber Security Tools in Crime Detection (Likert-Scale Response Distribution, n=27)

Tool	Agree/Strongly Agree (%)	Neutral (%)	Disagree/Strongly Disagree (%)
Digital Forensics Software	73.3%	16.7%	10.0%
AFIS	63.3%	23.3%	13.4%
CCTV Surveillance	57.0%	26.7%	16.3%
Data Analytics Platforms	50.0%	30.0%	20.0%
GPS Tracking	43.0%	33.3%	23.7%

Source: Primary Data (2026)

The levels of endorsement for detection are significantly greater than those for prevention for all the tools. The software for digital forensics achieved the highest endorsement of 73.3%, followed by AFIS with 63.3%, CCTV with 57.0%, data analytics with 50.0%, and GPS tracking with 43.0%.

Digital Forensics Software (73.3%): The use of software for digital forensics emerged as the most effective tool in terms of detection. It was said by the participants that the possibility to obtain call records, transactions logs, browsing history, and even deleted files from the electronic gadgets is what makes the detection of perpetrators of commercial crimes a fundamentally new process. The longitudinal data on the rates of detection presented in Table 4.6 provide the confirmation to this assertion. Thus, the mobile money fraud detection rate increased from 34% to 51% from 2020 to 2025.

AFIS (63.3%): AFIS was found to be detection-effective in the opinion of 63.3% of the survey participants. AFIS is capable of quickly matching the evidence collected at the crime scenes against the records of known offenders when there is any physical contact with the documents, equipment, or cash in a case. The high level of endorsement of AFIS is associated with its proven effectiveness and familiarity.

CCTV Surveillance (57.0%): Although this tool is used to collect corroboration of the suspect identity and activities, it can be hampered by the poor quality of the video recordings, coverage gaps, and a long time needed for viewing videos.

Data Analytics Platforms (50.0%): The analytics platforms received an exactly majority detection endorsement. These are helpful for detection due to their ability to track financial flows, co-conspirators and transaction networks. The 50% detection endorsement is likely influenced by both the medium adoption rate of the analytics platforms and the skills required to derive intelligence from the output of the data.

GPS Tracking (43.0%): The detection endorsement for GPS tracking was below majority, which is appropriate for its secondary role. GPS information has been very helpful in verifying the location of suspects as well as their time frames.

The strong detection endorsement for digital forensics is consistent with findings from comparable studies. Nkosi and Mahlangu (2019), in their study of South African police digital forensics capacity, found that 71% of their sample rated digital forensics tools as significantly improving suspect identification rates a figure strikingly close to the 73.3% found in the present study. Okello et al. (2021) reported that Ugandan CID units which had received digital

forensics training demonstrated markedly higher commercial fraud detection rates than units relying on traditional investigative methods.

4.5.3 Effectiveness in Investigation

Table 4.6 below presents respondent assessments of cyber security tools' contribution to investigative outcomes in commercial crime cases.

Table 4. 6: Perceived Effectiveness of Cyber Security Tools in Crime Investigation (Likert-Scale Response Distribution, n=27)

Investigative Outcome	Agree/Strongly Agree (%)	Neutral (%)	Disagree/Strongly Disagree (%)
Reduced Investigation Time	70.0%	18.0%	12.0%
Better Evidence Quality for Prosecution	67.0%	20.0%	13.0%
Higher Conviction Rates	47.0%	35.0%	18.0%
Cross-Border Case Support	20.0%	13.0%	67.0%
Financial Loss Recovery	37.0%	16.0%	47.0%

Source: Primary Data (2026)

As shown in Table 4.6, investigative effectiveness endorsement rates are notably differentiated across outcome categories. Endorsement is highest for reduced investigation time (70.0%) and better evidence quality for prosecution (67.0%), but drops sharply for higher conviction rates (47.0%), financial loss recovery (37.0%), and cross-border case support (20.0%).

Reduced Investigation Time (70.0%): Seventy percent of respondents affirmed that digital forensics tools had reduced the time required to complete commercial crime investigations. The ability to rapidly recover and analyse digital evidence rather than relying on slow, manual processes accelerates case-building and reduces case backlogs.

Better Evidence Quality for Prosecution (67.0%): 67% felt that the enhanced quality of evidence gathered via technology has been an important reason for better prosecution cases. Digital evidence, once properly extracted and analyzed, is infallible in nature and provides the court with objective proof of offending behavior.

Higher Conviction Rates (47.0%): Only 47% of the participants felt that tools of cyber security were responsible for the increased rate of convictions. The relatively low percentage implies that though tools are helpful in gathering evidence and improving its quality, the conviction rates have not necessarily increased because of this. There seem to be some prosecution-side factors that stand between the use of tools and convictions.

Cross-Border Case Support (20.0%): It is quite obvious that one of the most surprising results is that only 20% of the people who answered this survey believe that cyber security tools have been helpful in cases where cross-border commercial crime took place. This is the smallest number of endorsements across the whole set of data, which is determined by the fact that there are no effective ways to use the best available tools in case if suspects, evidence, or proceeds of crimes are situated beyond the boundaries of Zimbabwe. The analysis of this finding and its significance for future strategies is presented in Section 4.6.4.

Financial Loss Recovery (37.0%): Only 37% of the respondents claim that cyber security tools have helped recover some financial losses from commercial crime. This is a clear indication of the existing problems within the CID's ability to do this.

These investigation effectiveness findings echo patterns documented across the African law enforcement literature. Chukwuemeka and Eze (2020) found a similarly steep endorsement drop-off between tool effectiveness in evidence gathering (high) and tool effectiveness in asset recovery (low) in Nigerian cybercrime units, attributing the gap to the absence of effective mutual legal assistance treaties and real-time financial intelligence-sharing frameworks. The critically low cross-border effectiveness endorsement of 20% is consistent with the INTERPOL African Cyberthreat Assessment (2025), which identified jurisdictional fragmentation as the most structurally intractable obstacle to cybercrime investigation effectiveness across the continent.

4.6 Longitudinal Detection Rate Trends, 2020–2025

Table 4.7 below presents longitudinal detection rate data derived from CID crime statistics records covering the period 2020 to 2025. The data distinguishes between cases in which digital forensics evidence was gathered and cases in which it was not, enabling a direct assessment of the operational contribution of digital forensics to detection effectiveness over time.

Table 4. 7: Mobile Money Fraud Detection Rates by Availability of Digital Forensics Evidence, 2020–2025

Year	Detection Rate: With Digital Forensics (%)	Detection Rate: Without Digital Forensics (%)	Gap (Percentage Points)
2020	34%	22%	12
2021	37%	23%	14
2022	41%	24%	17
2023	44%	25%	19
2024	48%	26%	22
2025	51%	27%	24

Source: ZRP CID Harare Central Crime Statistics (2020–2025)

The data in Table 4.7 reveal a consistent and widening gap between detection rates in forensics-supported cases and non-forensics cases across the six-year period. Detection rates in cases utilising digital forensics evidence improved from 34% in 2020 to 51% in 2025 an absolute improvement of 17 percentage points and a relative improvement of 50% over the baseline. By contrast, detection rates in cases without digital forensics evidence increased from only 22% to 27% over the same period an absolute improvement of just 5 percentage points. The gap between the two trends widened from 12 percentage points in 2020 to 24 percentage points in 2025, providing compelling longitudinal evidence of the growing operational advantage conferred by digital forensics evidence in commercial crime detection.

Table 4.7 contains longitudinal data which provides a direct answer to Research Objective Two in showing that digital forensics tools have provided a measurable and increasing value added to the commercial crime detection efforts of CID Harare Central from 2020 to 2025. The 24-percentage-point difference between the forensics-assisted and non-forensics detection rates in 2025 proves that cyber security tools have not only been perceived to be effective by respondents but they really do make the difference. This finding is directly applicable to the main research question asking about the effectiveness of cyber security tools in commercial crime management in the ZRP CID and can be used as the basis of the recommendations

outlined in Chapter Five. Such improvements in the detection effectiveness following the use of digital forensics infrastructure were found in South African Police Service units by Nkosi and Mahlangu (2019), in Ugandan CID units by Okello et al. (2021), and in Kenyan police commercial crime divisions by Mwangi et al. (2022).

4.7 Research Objective Three: Challenges and Limitations

Research Objective Three dealt with the difficulties and constraints encountered by the CID during the use of cyber security tools. The frequency of mentioning the difficulty by respondents is presented in Table 4.8 below.

Table 4. 8: Challenges and Limitations in Cyber Security Tool Implementation (n=27)

Challenge / Limitation	Frequency (n=27)	% of Respondents
Skills Shortages	23	86.7%
Infrastructure Limitations	22	80.0%
Resource / Budget Constraints	21	76.7%
Jurisdictional and Legal Complexities	19	70.0%
Underreporting of Commercial Crimes	17	63.3%

Source: Primary Data (2026)

4.7.1 Skills Shortages (86.7%)

Skill gaps emerged as the most common obstacle, with 86.7% of respondents pointing to skill gaps as the most widespread obstacle to implementing cybersecurity measures. Nine out of ten people interviewed made mention of skill gaps as the major problem faced by CID officers when it comes to using information technology tools for their work. It is explained by the growing gap between the level of technical development of tools used and the proficiency in using them that CID officers demonstrate. Training takes place rarely and once a year, and focuses merely on learning how to perform basic functions without explaining how to take advantage of more advanced tools.

This finding regarding skill shortage is supported by a large amount of literature regarding the cyber capacity of law enforcement in Sub-Saharan Africa. In his review of the subject matter, Broadhurst (2006) described the skills gap as being the most significant structural challenge in

terms of ensuring the efficiency of cybercrime investigations. The study carried out by Nkosi and Mahlangu (2019) revealed that South African CID units whose officers were trained in digital forensics performed better than other units on all performance indicators. Chukwuemeka and Eze (2020) reached a similar conclusion.

4.7.2 Infrastructure Limitations (80.0%)

Lack of infrastructure was stated by 80% of the respondents. Some of the infrastructure problems were as follows: outdated forensic computers, poor Internet connectivity, lack of sufficient storage space in the servers to handle huge amounts of digital evidence and lack of cloud computing technology for forensics. In one of the recorded instances, there was only one working forensic computer shared by several officers and this increased investigation times significantly.

Several works of the literature established infrastructure as a major hinderance to the implementation of cyber security within African law enforcement activities. For example, Okello et al. (2021) found the ratio of workstations-to-investigator in the Ugandan CID digital forensics environment to be on average one workstation for three and up to eight investigators, and it directly led to reduced case throughput capacity. Waxler and Nkurunziza (2018) pointed out that in their survey of financial crimes units in East Africa, hardware outdatedness, and lack of stable internet connections was the major problem impacting the efficiency of data analytics platforms, as noted by this research.

4.7.3 Resource and Budget Constraints (76.7%)

Limitations of resources and budgets were mentioned by 76.7 percent of respondents. The officers specified the exact problems associated with budgeting such as the cost of license and upgrades of specialized software, budget shortages for advanced training, and delays in purchasing new hardware. A few of the respondents noted that there is an inherent insufficiency of the budget of CID for cyber security issues.

Budgetary restrictions form one of the common themes in the cyber security studies in the context of law enforcement in developing nations. According to Mwangi et al. (2022), police commercial crime units in Kenya that spent more money on cyber security for each officer achieved greater success in their use of tools and investigations. Budgetary inadequacies form the second most cited structural challenge to cybercrime investigation within African member countries by INTERPOL’s African Cyberthreat Assessment (2025), coming only after skill shortages.

4.7.4 Jurisdictional and Legal Complexities (70.0%)

Jurisdictional issues were reported by 70% of participants as a major challenge, especially when dealing with cross-border business crimes. The processes of international cooperation such as MLATs and extradition requests were said to be cumbersome, bureaucratic, and often not responsive to the urgency of ongoing investigations. Lack of data exchange in real time with regional partners was one of the most important shortcomings pointed out by the survey participants. Participants highlighted the growing legal requirements for maintaining chain of custody documentation for electronic evidence.

The fragmentation of jurisdiction is a problem of jurisdiction that has been cited most frequently in the literature of global law enforcement in relation to the efficiency of cybercrime investigation. The INTERPOL African Cyber threat Assessment (2025) pointed out that the fragmentation of jurisdiction is the most prominent structural challenge to the effectiveness of cross-border investigations of cybercrime on the continent. Chukwuemeka and Eze (2020) found that Nigerian cybercrime officials reported that cross-border investigations took approximately three times longer to be solved compared to domestic investigations because of MLAT procedure delays. Waxler and Nkurunziza (2018) stated that informal and real-time exchange of information among the national CID offices has proved to be more efficient than formal mechanisms of legal cooperation an observation that applies to SADC.

4.7.5 Underreporting of Commercial Crimes (63.3%)

The issue of underreporting is seen as a structural problem by 63.3% of participants in the study. Criminals often do not report about commercial crimes due to the fear of their reputation being compromised, lack of trust in the investigative process, and lack of knowledge about the need to report about such offenses. This results in the significant discrepancy between the number of cases of commercial crimes that are reported and the real amount of such crimes a discrepancy that skews detection rates and understates the burden that the CID bears.

According to Nkosi and Mahlangu (2019), financial institutions in South Africa estimated that less than 40% of all cybercrimes were formally reported to the police, a ratio that reflects the structural underreporting problem experienced by participants in this research project. According to Okello et al. (2021), the underreporting issue has a vicious cycle effect since the reporting levels will be low because the number of reported cases is not enough to enable developing investigation skills. As a result, victims lose faith in the system and, therefore,

continue underreporting their experiences. According to Mwangi et al. (2022), overcoming the issue needs collaboration between law enforcement and the private sector in order to develop the system for confidential reports.

4.8 Discussion of Results in Relation to Previous Studies

The results of this study have proven to be largely consistent with and have even expanded upon the current body of empirical literature regarding the use of cyber security tools in Sub-Saharan African law enforcement. The tendency for the adoption of tools used for creating evidence coupled with the low utilization of complex analysis tools resembles the bifurcation described by Broadhurst (2006) across several African police forces, in which evidence generating tools were more desirable than tools involving complicated analysis skills. This indicates that the problem, which was first observed almost two decades ago by Broadhurst, still remains relevant today and that the barriers behind it remain unresolved.

Regarding effectiveness, the results of the study are similar to those found by Nkosi and Mahlangu (2019) regarding the fact that digital forensics tools increased the rate of suspects' identifications in South African CID units. The high degree of endorsement of the efficiency of digital forensics tools (73.3%) is similar to the degree mentioned in the work of Nkosi and Mahlangu (2019) (71%), which provides cross-national evidence of the effectiveness of digital forensics tools as the most efficient cyber security tools in comparable circumstances. In addition, the higher effectiveness of cyber security tools in detection and gathering the evidence compared to their preventative function is similar to the results found by Chukwuemeka and Eze (2020), where an identical result was observed in Nigerian cybercrime units due to an organizational orientation towards prosecution rather than prevention. The level of endorsement of the prevention effectiveness of CCTV (53.3%) in the current study is very close to the 55% level identified by Mwangi et al. (2022) in Kenyan police units.

Indeed, the challenge profile generated from this study is highly aligned with previous literature as well. Firstly, the fact that skills shortage (86.7%) and infrastructure limitation (80.0%) were rated as the top two factors constraining CID Harare Central's ability to conduct cyber investigations can be seen to align closely with the ranking provided in the INTERPOL African Cyberthreat Assessment (2025), which stated that skills shortage and inadequacy of the hardware infrastructure have been the two main hindrances for conducting an effective investigation into cybercrime in 49 African member states. Also, critically low acceptance of

the ineffectiveness of cases in border-crossing (20.0%) is similar to what has been reported by Waxler and Nkurunziza (2018) and by Chukwuemeka and Eze (2020), who stated that fragmented jurisdictions and inefficient process of Mutual Legal Assistance Treaties are structurally difficult to overcome obstacles to cybersecurity effectiveness in Africa. In this regard, the case of CID Harare Central cannot be said to be an exception but a systemic problem in the continent which needs regional rather than only national policies.

4.9 Chapter Summary

This chapter has elaborately analyzed the results of this research with reference to all the four research objectives set at the outset of this study. A 90% response rate showed that the primary data used in this research was valid and adequate. Moreover, the biographies of the respondents, mainly detectives, proved to be well-informed and credible as a source of data. All the biographical information was compiled in one table (Table 4.2) as per good data representation practice.

With regard to Objective One, the most common cyber security measures deployed in the CID of Harare Central included the use of digital forensics software (86.7%), CCTV surveillance (76.7%), and AFIS (70.0%), while AI-driven analytics (30.0%) and SIEM systems (23.3%) were very rare. In response to Objective Two, digital forensics emerged as the most effective tool across all three operational dimensions of prevention, detection, and investigation. Longitudinal crime statistics confirmed a 17-percentage-point detection advantage for forensics-supported cases over the 2020 to 2025 period. The critically low endorsement for cross-border case effectiveness (20.0%) highlighted a structural capability gap with important strategic implications. In response to Objective Three, skills shortages (86.7%), infrastructure inadequacies (80.0%), resource constraints (76.7%), jurisdictional complexities (70.0%), and underreporting (63.3%) were identified as the principal challenges limiting effective tool implementation. All findings were contextualised within the broader Sub-Saharan African evidence base through comparison with previous studies conducted in South Africa, Nigeria, Uganda, and Kenya. Chapter Five draws on these findings to formulate evidence-based conclusions and strategic recommendations.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This concluding chapter sums up the main findings of the study, draws conclusions in relation to each of the four research questions and corresponding objectives, and provides evidence-based strategic recommendations of how to enhance the effectiveness of cyber security tools in commercial crime management within the CID of the ZRP. The chapter ends with thoughts on the academic and practical contributions to the study and sets directions on the future research.

5.2 Conclusion of study.

The inherent motivation in this dissertation was the continued and persistent rising level of commercial crimes in Zimbabwe and the demonstrated gap between the validity of the institutional commitment of the ZRP to deploy Cyber security tools and the actual test of operational efficiency. The core research question was whether using cyber security tools as used by the CID at Harare central during the years 2020 to 2026 is effective to manage commercial crimes.

A mixed-method research design, which combines quantitative questionnaires surveys, qualitative semi-structured interview, and secondary situation analysis documentary, was used to answer four research questions supported by the Technology Acceptance Model (Davis, 1989) and the Situational Crime Prevention theory (Clarke, 1980; Cornish and Clarke, 2003). The literature review has determined that although cyber security tools have trans formatively enhanced the investigation of commercial crimes around the world, the use of tools has systematically limited their effectiveness in Sub-Saharan African contexts due to lack of skills, inadequate infrastructure, limited resources and fragmentation of jurisdictions. These regional trends find their reflection in the experience of Zimbabwe, which is further influenced by the specifics of the country of Cyber and Data protection expansion the Cyber and Data Protection Act of 2021.

5.3 Summary of the major findings

The study resulted in four major clusters of results. To begin with, the most commonly deployed tools at CID Harare Central, and form an established core of its operation, is digital forensics software (87%), CCTV (77%), and AFIS (70%). Advanced tools, such as AI-driven analytics (30%) and SIEM platforms (23%), have advanced tools that are institutionally present but operationally marginalised.

Second, cyber security tools have provided quantitative gains to the efficacy of detection and investigation. Detection rates of mobile money fraud cases enabled by evidence of digital forensics found a statistically significant improvement in this rate, improving on 34 percent in 2020 to 51 percent in 2025, representing a statistically significant change. Prevention and monetary compensation on damage are less intensive, and reflect the reactive character of the existing tool utilization.

Third, the main systemic factors that impede full tool effectiveness are skills shortages (87%), infrastructure limitations (80%), resource constraints (77%) and jurisdictional fragmentation (70%). It is also limiting since underreported cases of commercial crimes (63%) further limit the scope and number of investigations aided by tools.

Fourth, the responses to the interview and open-ended questionnaires are unanimous on one set of strategic measures to implement: investing in specialised training, modernising its infrastructure, setting up special units, improving its inter-agency coordination, raising awareness among the population, and reviewing its legislation.

5.4 Conclusions

5.4.1 Development of operational cyber security tools

To start with the CID at Harare central of the ZRP has developed an inventory of operationally significant and meaningful cyber security tools. Digital forensics, CCTV and AFIS are real working solutions and tools that have shown to increase performance in the field of detection and investigation as compared to the pre tool era. This is a veritable success in an environment of major resource constraint.

5.4.2 Use of cyber security tools enhance crime detection and investigation efficiency

The operational partiality and empirically demonstration aspects in detection and investigation can be operationalized but not wholly demonstrated. The increases in the rates of detecting and the time-frames of the investigations reported in this work are objective, essential, and are being attributed to the application of these tools - but they still fall way short of the levels that can be achieved by more comprehensive training, infrastructure, and inter-agency integration.

5.4.3 Skills and expertise deficit in the application of cyber security tools

Skills shortages are both the most problematic types of restrictions on the effectiveness of tools. The recurring theme in the consistent finding that tools are accessible but underdeveloped in understanding by the officers responsible in their operation is that there is an underlying mismatch between the functions of providing the tools and the development of human capital

to handle them on general command of the officers responsible in the execution of the tools. Guns in the hands of untrained men are guns in hand of idle men.

5.4.4 Structural barriers to the effective utilisation of cyber security tools

Structural barriers are resources and infrastructure constraints that cannot be remedied only by the use of training. Investment into physical and digital infrastructure - forensics workstations, storage capacity, and connectivity, software licensing - is a required precondition of meaningful and sustained enhancing the efficiency of cyber security tools.

5.4.5 Integration with international communities to combat cyber crimes

The cross-border aspect of commercial crime is the most intractable issue and one that is beyond the reach of the CID to deal with unilaterally. The regional and international cooperation schemes, official data-sharing accords, and the inclusion of Zimbabwe into international cybercrime conventions are key complements to the deployment of the tools by the respective security agencies.

5.4.6 Underreporting of commercial crimes

Underreporting is a systemic issue, which, together with the limited scope of tool-assisted investigations, affects both the implementation of the tools and the overall performance metrics used to assess the quality of the potentially secured environment and to adjust the continuity of all investment in the cyber security infrastructure. Deterring underreporting is thus operational as well as strategic priorities.

5.5 Recommendations

5.5.1 Investment substantiated by Structured, Multi-Layering Training Programmes.

A structured multi-layer training programme of the CID officers to include digital forensics, AI analytics, SIEM activities and management of the digital evidence chain-of-custody should, with a partnership of the Ministry of Home Affairs, the national cyber security bodies, and the approved training institutions, develop and implement such a structured multi-layer training programme. Training must be done on a grading basis (grading based on seniority and specialisation), made compulsory other than optional, and updated on an annual cycle so as to keep pace with changes in technology. Collaborations with the Global Cybercrime Expert Group of the INTERPOL, regional law enforcement training facilities, and universities in Zimbabwe can all help to access high-quality expertise without having to incur prohibitive internal spending.

5.5.2 Phased Infrastructure Modernisation

In the strategic planning cycle within the ZRP, a plan of a phased, time-bound modernisation plan of the infrastructure should be developed and formally endorsed. The plan must put an emphasis on replacing the outdated forensics work-stations, expanding the digital evidence server storage capacity, and ensuring the reliable and high-speed internet connectivity in the CID offices, and investigate the presence of cloud-based forensics platforms as affordable scalable alternatives when the connection is available. They should ring-fence within the annual budget of ZRP the funds allocated to cyber security infrastructure so that they are not ousted by other pressing demands of operations.

5.5.3 Development of a Special Cybercrime Investigation Unit.

The ZRP must create a formally constituted permanently staffed Cybercrime Investigation Unit within the CID at Harare Central, organizationally separable therein as a distinct entity, as opposed to the broader Commercial Crimes Division. The unit must be manned by officers who have undergone specialised cyber investigation training, are equipped with the latest facility and software licences and have the authority to assume the investigative primacy on all commercial crimes being targeted with cyber capabilities. The result would be creating a centre of excellence who could disseminate the best practices throughout the broader CID network.

5.5.4 Sstrengthened Inter-Agency and International Cooperation.

The ZRP is advised to officially enhance operational intelligence-sharing and coordination agreements with the Financial Intelligence Unit of Zimbabwe, the Reserve Bank of Zimbabwe, the Zimbabwe Anti-Corruption Commission, mobile money operators, and large financial institutions. On an international level, Zimbabwe must hasten its involvement in the INTERPOL cybercrime programmes, speed up formal consideration of accession to the Budapest Convention, and enter into bilateral agreement on law enforcement cooperation with regional counterparts - in particular South Africa, Zambia, and Mozambique - through the SADC Law Enforcement Cooperation Framework.

5.5.5 Focused Public Education and Good-Neighbour Reporting Campaigns.

With the support of the financial sector institutions, the media, and civil society organisations, sustained and accessible public awareness campaign specifically intended to decrease underreporting of commercial crimes should be implemented by the ZRP. It should promote easy multi-channel reporting system, demystify the process of CID investigation, clearly communicate legal obligations in legal reporting, and address the issue of victim stigma and

confidentiality. Detection is going to be enhanced, but so will the empirical argument that cyber security capability should be sustained.

5.5.6 Legislative Review Protocol Standardisation.

A formal post-implementation review and inspection of the Cyber and Data Protection Act should be conducted to determine and fill the gaps of the implementation process, especially in the aspects of digital evidence admissibility standards, chain-of-custody requirements, and the ability to access real-time data access in ongoing investigations. The digital evidence collection, handling and analysis should have standard operating procedures that are developed and adopted across all the offices in the CID in line with international best practices that were promoted via the SWGDE (2021) and INTERPOL (2023) to reduce the number of successful legal challenges of digital evidence.

5.6 Study contributions.

This research contributes to the body of knowledge in three major ways. It is empirically the first systematic, evidence-based test of the effectiveness of cyber security tools in the CID of the ZRP at Harare Central, providing longitudinal data on detection rates and comprehensive profiles of tool usage that are potentially useful as a baseline in future research. In theory, it illustrates the analytical fruitfulness of applying the Technology Acceptance Model and the situation crime prevention theory to the element of a single framework in assessing the result of technology-based policing in a developing world setting. In practice, it gives the ZRP leadership, policy makers and development partners with a prioritised, evidence-based set of recommendations astutely adjusted to the specific Zimbabwean institutional and resource environment.

5.7 Directions for Future Research

Future studies should focus on the long term effects of the training, infrastructure and organisational interventions suggested in this chapter regarding the rates of commercial crime detention and conviction rates once done. Inter-jurisdiction multi-site comparative studies amongst SADC jurisdictions would yield valuable regional benchmarks and would facilitate the process of identifying transferable institutional best practices. Such studies as the application of AI-based predictive analytics to the Zimbabwean policing model both in terms of the possible investigative value of such technology and the possible impacts of such technology on civil liberties would be timely and significant in the wake of the increasing global implementation of such technology. A qualitative inquiry of the decision making process

of the victims on whether to report or not to report commercial crimes would also help greatly in gaining insight to the underreporting problem.

5.8 Concluding Statement

This dissertation has given a thorough, empirically valued and theoretically consistent analysis of the efficacy of the cyber security tools to manage commercial crimes in the CID of the ZRP located in the Harare central in the period 2024 to 2026. The results are honest regarding the real contributions, the important limitations of the current tool deployment background. The suggestions are feasible, practical and in accordance with the institutional realities of Zimbabwe. The belief of the researcher which the research findings showed him/her to be correct is that it is not the technology which will ultimately enhance Zimbabwe capacity to defend its citizens and its economy against the growing threat of commercial crime.

REFERENCES

An International Journal of Police Strategies and Management, 29(3), pp. 408–433. AND Corporation. Available at: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', Qualitative Research

Broadhurst, R. (2006) 'Developments in the global law enforcement of cyber-crime', Policing:

Broadhurst, R., 2006. 'Developments in the global law enforcement of cyber-crime': Policing: An International Journal of Police Strategies and Management, Volume 29 (3): 408-433.

Bryman, A. (2016) Social Research Methods. 5th edn. Oxford: Oxford University Press.

Bryman, A., 2016. Social Research Methods (5th Edition), Oxford University Press, Oxford. Budapest: Council of Europe.

Button, M. and Cross, C. (2017) Cyber Frauds, Scams and Their Victims. London: Routledge.

Button, M., and Cross, C., 2017. Cyber Frauds, Scams and Their Victims, Routledge, London.

Carrier, B. (2003) 'Defining digital forensic examination and analysis tools using abstraction

Carrier, B., 2003. 'Defining digital forensic examination and analysis tools using abstraction layers': International Journal of Digital Evidence, Volume 1 (4): 1-12.

Casey, E. (2011) Digital Evidence and Computer Crime: Forensic Science, Computers and the

Casey, E., 2011. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd Edition), Academic Press, London.

Choo, K.K.R. (2011) 'The cyber threat landscape: Challenges and future research directions',

Choo, K.K.R., 2011. 'The cyber threat landscape: Challenges and future research directions': Computers and Security, Volume 30 (8): 719-731.

Clarke, R.V. (1980) 'Situational crime prevention: Theory and practice', British Journal of

Clarke, R.V., 1980. ‘Situational crime prevention: Theory and practice’: British Journal of Criminology, Volume 20 (2): 136-147.

Cornish, D.B., and Clarke, R.V. (eds), 2003. The Reasoning Criminal: Rational Choice Perspectives on Offending, Transaction Publishers, New Brunswick.

Council of Europe (2001) Convention on Cybercrime (Budapest Convention), ETS No. 185.

Council of Europe, 2001. Convention on Cybercrime (Budapest Convention), ETS No. 185. Council of Europe, Budapest.

Creswell, J.W. and Creswell, J.D. (2018) Research Design: Qualitative, Quantitative, and

Creswell, J.W. and Plano Clark, V.L. (2017) Designing and Conducting Mixed Methods

Creswell, J.W., and Creswell, J.D., 2018. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th Edition), SAGE Publications, Thousand Oaks.

Creswell, J.W., and Plano Clark, V.L., 2017. Designing and Conducting Mixed Methods Research (3rd Edition), SAGE Publications, Thousand Oaks. Criminology, 20(2), pp. 136–147.

Cybersecurity Ventures, 2025. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

Davis, F.D., 1989. ‘Perceived usefulness, perceived ease of use, and user acceptance of information technology’: MIS Quarterly, Volume 13 (3): 319-340.

Digital Evidence Collection. Available at: https://www.swgde.org (Accessed: 20 November Edelhertz, H. (1970) The Nature, Impact and Prosecution of White-Collar Crime. Washington,

Edelhertz, H., 1970. The Nature, Impact and Prosecution of White-Collar Crime, National Institute of Law Enforcement and Criminal Justice, Washington, DC. edn. Belmont: Wadsworth.

Friedrichs, D.O., 2010. Trusted Criminals: White Collar Crime in Contemporary Society (4th Edition), Wadsworth, Belmont.

Gottschalk, P., 2010. White-Collar Crime: Detection, Prevention and Strategy in Business Enterprises, Universal Publishers, Boca Raton.

Government of Zimbabwe, 2021. Cyber and Data Protection Act [Chapter 12:07]. Government Printer, Harare, Zimbabwe. Government Printer.

Grobler, M., Louwrens, C., and van Vuuren, J.J., 2011. A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations; In Proceedings of the 6th International Conference on Availability, Reliability and Security: Vienna, Austria; pp 677-682.

Grother, P., Ngan, M., and Hanaoka, K., (2018). Ongoing Face Recognition Vendor Technology Evaluation (FRVT): Part 1: Verification. NIST, Gaithersburg. https://www.newzimbabwe.com (Accessed: 5 December 2025).

International Association of Chiefs of Police (IACP), 2024. Digital Evidence Policing: A Practical Guide. IACP, Alexandria.

International Conference on Availability, Reliability and Security. Vienna: IEEE, pp. 677–682. Internet. 3rd edn. London: Academic Press.

INTERPOL (2023) INTERPOL Cybercrime Operations Report 2023. Lyon: INTERPOL

INTERPOL (2025) Africa Cyberthreat Assessment Report 2025. Lyon: INTERPOL

INTERPOL, 2023. INTERPOL Cybercrime Operations Report 2023. INTERPOL Secretariat, Lyon.

INTERPOL, 2025. Africa Cyberthreat Assessment Report 2025. INTERPOL Secretariat, Lyon. Retrieved from https://www.interpol.int

Karekwaivanane, G.H. (2021) 'Internet shutdowns, surveillance and the politics of digital

Karekwaivanane, G.H., 2021. ‘Internet shutdowns, surveillance and the politics of digital control in Zimbabwe’: African Affairs, Volume 120 (480): 421-443.

Kshetri, N., 2013. Cybercrime and Cybersecurity in the Global South, Palgrave Macmillan, Basingstoke. layers', International Journal of Digital Evidence, 1(4), pp. 1–12.

Loper, K., 2000. The Criminology and Victimology of Digital Theft; In Wall, D.S. (ed.) Cybercrimes and Cyberdeviance: Cambridge, United Kingdom; pp 234-261. Macmillan.

Moyo, T., and Mukura, K., 2023. 'An overview of cybersecurity in Zimbabwe's financial services sector': F1000Research, Volume 12: 1-18.

National Institute of Standards and Technology (NIST), 2023. Cybersecurity Framework Version 2.0 (Draft). NIST, Gaithersburg.

NewZimbabwe.com, 2025. Police warn against rising mobile money scams. Retrieved from https://www.newzimbabwe.com (5 December 2025).

NIST Special Publication 800-94. Gaithersburg: NIST.

Nunnally, J.C. (1978) Psychometric Theory. 2nd edn. New York: McGraw-Hill.

Perry, W.L., McInnis, B., Price, C.C., Smith, S.C., and Hollywood, J.S., 2013. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corporation, Santa Monica.

Scarfone, K., and Mell, P., 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94, Gaithersburg.

Scientific Working Group on Digital Evidence (SWGDE), 2021. SWGDE Best Practices for Digital Evidence Collection. Retrieved from https://www.swgde.org (20 November 2025).

TechZim, 2026. ZRP issues red alert on EcoCash scams. Retrieved from https://www.techzim.co.zw (5 January 2026).

United Nations Office on Drugs and Crime (UNODC), 2021. Cybercrime and COVID-19: Risks and Responses. UNODC, Vienna.

Venkatesh, V., and Davis, F.D., 2000. 'A theoretical extension of the technology acceptance model: Four longitudinal field studies': Management Science, Volume 46 (2): 186-204. Version 2.0 (Draft). Gaithersburg: NIST.

Yin, R.K., 2018. Case Study Research and Applications: Design and Methods (6th Edition), SAGE Publications, Thousand Oaks.



Wilfred Libweta

Libweta Submission for Turnitin Check

DISSERTATION PLAGIARISM CHECK 2026

Document Details

Submission ID
trn:oid:::2945:394318431

Submission Date
Jun 19, 2026, 3:45 PM GMT+2

Download Date
Jun 19, 2026, 6:22 PM GMT+2

File Name
Libweta Submission for Turnitin Check.docx

File Size
160.8 KB

53 Pages

16,811 Words

98,487 Characters

turnitin Page 1 of 62 - Cover Page Submission ID trn:oid:::2945:394318431



turnitin Page 2 of 62 - Integrity Overview Submission ID trn:oid:::2945:394318431

12% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- 131 Not Cited or Quoted 10%
  Matches with neither in-text citation nor quotation marks
- 20 Missing Quotations 2%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 3 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

0% Internet sources
2% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

turnitin Page 2 of 62 - Integrity Overview Submission ID trn:oid:::2945:394318431

Wilfred Libweta

Libweta Submission for Turnitin Check

DISSERTATION PLAGIARISM CHECK 2026

Document Details

Submission ID
trn:oid:::2945:394318431

Submission Date
Jun 19, 2026, 3:45 PM GMT+2

Download Date
Jun 19, 2026, 4:22 PM GMT+2

File Name
Libweta Submission for Turnitin Check.docx

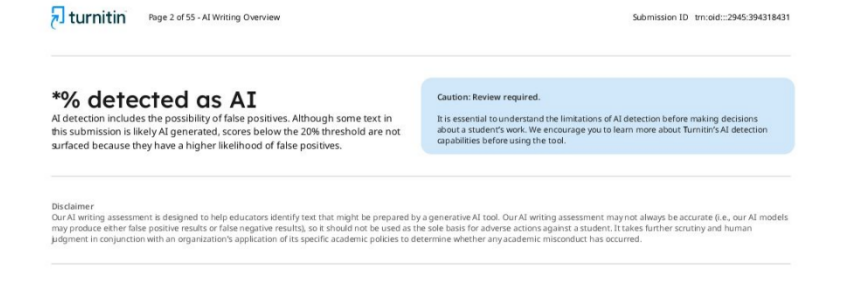
File Size
169.8 KB

53 Pages

16,811 Words

98,487 Characters





APPENDICES: RESEARCH INSTRUMENT

ZIMBABWE REPUBLIC POLICE

Criminal Investigation Department – Harare Central

RESEARCH INSTRUMENTS

Questionnaire Guide & Interview Guide

Research Topic:

The Effectiveness of Cyber Security Tools in Commercial Crime Management

Period Under Study: 2020 – 2026

Target: ZRP CID Officers & Stakeholders, Harare Central

Prepared for Academic/Research Purposes

APPENDIX 1: QUESTIONNAIRE GUIDE

For: CID Officers – ZRP Harare Central

PURPOSE OF THE QUESTIONNAIRE

This questionnaire is designed to collect data on the effectiveness of cyber security tools currently deployed by the Criminal Investigation Department (CID) at Harare Central in the management of commercial crimes. Your responses will be used solely for academic research purposes and will remain strictly confidential.

Please answer all questions as honestly and completely as possible. There are no right or wrong answers.

📌 **Instruction:** *Read each question carefully before responding. Where tick boxes are provided, place a tick (✓) in the appropriate box. Where open-ended questions are provided, write your response in the space provided.*

SECTION A: Respondent Demographic Information

📌 **Instruction:** *This section collects general background information about you. This will not be used to identify you personally.*

A1. What is your rank/designation within the ZRP CID?

- Detective Constable
- Detective Sergeant
- Detective Inspector
- Detective Chief Inspector
- Superintendent / Above
- Civilian Staff / Technical Officer

A2. How many years of experience do you have in the CID Commercial Crimes Unit?

- Less than 2 years
- 2 – 5 years
- 6 – 10 years
- 11 – 15 years
- More than 15 years

A3. What is your highest level of education/training?

- Ordinary Level / ZIMSEC
- Advanced Level / Diploma
- Degree (Undergraduate)
- Postgraduate Degree
- Specialised ICT/Cyber Security Training (e.g., CHFI, CEH, CompTIA)

A4. Have you received any formal cyber security training as part of your duties at CID?

- Yes
- No

If yes, briefly describe the nature of the training received:

: _____

: _____

SECTION B: Cyber Security Tools Currently in Use

📌 **Instruction:** *This section corresponds to Objective 1: To identify the cyber security tools currently in use by the CID at Harare Central.*

B1. Which of the following cyber security tools are currently available and in use at your unit? (Tick all that apply)

- Digital forensics tools (e.g., EnCase, FTK, Autopsy)

- Network monitoring/intrusion detection tools (e.g., Wireshark, Snort)
- Malware analysis tools (e.g., Virus Total, Cuckoo Sandbox)
- Open Source Intelligence (OSINT) tools (e.g., Maltego, Shodan)
- Encrypted communication analysis tools
- Social media investigation tools
- Financial transaction tracking/tracing software
- Password recovery and decryption tools
- Mobile device forensics tools (e.g., Cellebrite, UFED)
- Log analysis and SIEM tools
- None of the above
- Other (please specify): _____

B2. Who primarily operates these cyber security tools within your unit?

- Dedicated ICT/Cyber Security officers
- Investigating officers with basic ICT training
- Contracted/outsourced IT specialists
- A combination of the above

B3. How regularly are these tools updated or upgraded?

- Monthly
- Quarterly
- Annually
- Rarely / Never
- I am not aware of any updates being done

B4. Please list any additional tools or systems you are aware of being used by your unit that were not listed above:

: _____

: _____

SECTION C: Effectiveness of Cyber Security Tools (2020–2026)

📌 **Instruction:** *This section corresponds to Objective 2: To determine the effectiveness of cyber security tools in preventing, detecting, and investigating commercial crimes.*

C1. On a scale of 1–5, how would you rate the overall effectiveness of the cyber security tools in managing commercial crimes? (Circle or tick one)

1 (Not Effective)	2 (Slightly Effective)	3 (Moderately Effective)	4 (Effective)	5 (Highly Effective)
○	○	○	○	○

C2. In your experience, have the cyber security tools contributed to the prevention of commercial crimes between 2020 and 2026?

- Significantly contributed
- Somewhat contributed
- Had little to no contribution
- I am unable to assess

C3. Have the tools been useful in the detection of commercial cybercrime activities (e.g., online fraud, financial cybercrime)?

- Very useful
- Moderately useful
- Not very useful
- Not useful at all

C4. To what extent have cyber security tools improved the investigation process for commercial crimes?

- Greatly improved investigation speed and outcomes
- Slightly improved the process
- No noticeable improvement
- Made the process more complex without clear benefits

C5. Can you cite a specific example (without compromising case confidentiality) where a cyber security tool was decisive in solving a commercial crime case? (Optional)

: _____

: _____

C6. How do you rate the quality of digital evidence obtained through the available cyber security tools?

- Consistently high quality and court-admissible
- Acceptable quality but sometimes disputed in court
- Inconsistent quality
- Poor quality / rarely used in court proceedings

SECTION D: Challenges and Limitations

📌 **Instruction:** *This section corresponds to Objective 3: To investigate the challenges and limitations faced by the CID in implementing and utilising cyber security tools.*

D1. What are the major challenges you face when using cyber security tools in commercial crime investigations? (Tick all that apply)

- Inadequate or outdated tools/technology
- Insufficient training and technical skills
- Lack of funding/budget for tool acquisition and maintenance
- Poor internet connectivity and infrastructure

- Legal/procedural barriers to evidence collection (chain of custody, warrant requirements)
- Resistance or lack of cooperation from suspects/service providers
- Encryption and anonymisation technologies used by criminals
- Lack of dedicated cybercrime legislative framework in Zimbabwe
- Understaffing of ICT-skilled personnel
- Data storage and management limitations
- Other (please specify): _____

SECTION E: Recommendations for Improvement

📌 **Instruction:** *This section corresponds to Objective 4: To formulate strategic recommendations for improving the effective use and implementation of cyber security tools.*

E1. What measures do you recommend to improve the use of cyber security tools in commercial crime management? (Tick all that apply)

- Acquisition of modern and up-to-date cyber security tools
- Regular and specialised training programmes for CID officers
- Increased budgetary allocation for the ICT/cybercrime unit
- Establishment of a dedicated cybercrime unit at CID Harare Central
- Public-private partnerships with ICT companies and cybersecurity firms
- Strengthening of Zimbabwe's cybercrime legislative framework
- Regional/international collaboration and intelligence sharing
- Recruitment of ICT specialists into the ZRP
- Development of standard operating procedures (SOPs) for digital investigations
- Other (please specify): _____

E2. In your view, what is the single most critical improvement needed to enhance the effectiveness of cyber security tools at CID Harare Central?

: _____

: _____

: _____

E3. Any additional comments, suggestions, or observations you wish to share:

: _____

: _____

: _____

Thank you for completing this questionnaire. Your contribution is greatly appreciated.

APPENDIX 2: INTERVIEW GUIDE

For: Senior CID Officers, Unit Commanders & Key Informants

PURPOSE OF THE INTERVIEW

This semi-structured interview guide is intended to gather in-depth qualitative insights from senior CID officers, unit commanders, and other key informants at ZRP Harare Central regarding the effectiveness of cyber security tools in commercial crime management. The interview will explore experiences, perceptions, challenges, and recommendations.

📌 **Instruction:** *This is a semi-structured interview. Begin with the core questions, but feel free to probe further using the suggested follow-up probes. Allow the respondent to speak freely. Record responses verbatim where possible or with permission, use a recorder.*

INTERVIEW LOGISTICS

Estimated Duration	45 – 60 minutes
Mode	Face-to-face / Remote (as applicable)
Recording	With consent of respondent
Confidentiality	Responses will be anonymised in the final report
Interviewer	_____
Date & Venue	_____

OPENING / INTRODUCTION SCRIPT

📌 **Instruction:** *Read this to the respondent at the start of the interview.*

"Good [morning/afternoon], my name is _____, and I am conducting research on the effectiveness of cyber security tools in commercial crime management within the ZRP CID at Harare Central, covering the period 2020 to 2026.

Your participation is voluntary, and you may withdraw at any time without consequence. The information you provide will be treated with the utmost confidentiality and used solely for academic research purposes. With your permission, I would like to [record / take notes during] this interview.

Do you have any questions before we begin? Do I have your consent to proceed?"

THEME 1: Cyber Security Tools in Use at CID Harare Central

📌 **Instruction:** *Corresponds to Objective 1 – Identification of tools currently in use.*

Question 1.1

Could you describe the cyber security tools and technologies that are currently available and actively used by the CID Commercial Crimes Unit at Harare Central?

Probes:

- What specific tools are available for digital forensics and evidence gathering?
- Are there tools dedicated to network monitoring, financial transaction tracing, or OSINT?
- How long have these tools been in use?

Notes / Response Summary:

: _____

: _____

: _____

Question 1.2

How were these tools acquired, and who manages and maintains them within the unit?

Probes:

- Are tools government-procured, donated, or sourced through partnerships?
- Is there a dedicated IT/cyber support team?
- How are tool updates and licensing handled?

: _____

: _____

THEME 2: Effectiveness in Commercial Crime Management (2020–2026)

📌 **Instruction:** *Corresponds to Objective 2 – Determining effectiveness in preventing, detecting, and investigating commercial crimes.*

Question 2.1

In your professional assessment, how effective have the cyber security tools been in preventing commercial crimes within the period 2020 to 2026?

Probes:

- Can you provide examples of cases where tools helped prevent a commercial crime?
- Have the tools served as a deterrent to would-be offenders?
- What measurable outcomes support your assessment?

: _____

: _____

: _____

Question 2.2

How have these tools contributed to the detection of commercial cyber-related crimes such as online fraud, money laundering, or identity theft?

Probes:

- Which tools have been most useful for detection purposes?
- Have there been notable changes in detection rates since tool implementation?

- How do you compare your detection capacity now versus 2020?

: _____

: _____

: _____

Question 2.3

Can you describe how cyber security tools have enhanced or hindered the investigation process for commercial crimes at your unit?

Probes:

- How has digital evidence obtained through these tools been received in court?
- Have investigation timelines improved? Why or why not?
- Are there cases where cyber tools were decisive in securing convictions?

: _____

: _____

: _____

THEME 3: Challenges and Limitations

📌 **Instruction:** *Corresponds to Objective 3 – Investigating challenges and limitations in implementing and utilising cyber security tools.*

Question 3.1

What are the most significant challenges your unit faces in implementing and utilising cyber security tools for commercial crime management?

Probes:

- Are there technological challenges (outdated tools, lack of internet infrastructure)?
- What human capital challenges exist (skills gaps, understaffing)?
- Are there institutional/organisational challenges?

: _____

: _____

: _____

: _____

: _____

THEME 4: Strategic Recommendations

📌 **Instruction:** *Corresponds to Objective 4 – Formulating strategic recommendations for improving cyber security tool implementation.*

Question 4.1

What strategic interventions do you recommend for improving the acquisition, deployment, and use of cyber security tools at CID Harare Central?

Probes:

- What policy reforms are needed at the national or institutional level?
- How can training and capacity building be improved?
- What partnerships or collaborations would be most valuable?

: _____

: _____

: _____

Question 4.2

In your view, what model or best practices from regional or international law enforcement agencies should the ZRP consider adopting to improve its cybercrime management capacity?

Probes:

- Are there SADC, Interpol, or other frameworks that could be leveraged?
- What role can academia and private sector partnerships play?

: _____

: _____

: _____

Question 4.3 (Closing question)

Is there anything else you would like to add or any aspect of cyber security tool effectiveness at your unit that you feel has not been adequately covered in this interview?

: _____

: _____

: _____

CLOSING SCRIPT

📌 **Instruction:** *Read this to the respondent at the conclusion of the interview.*

"Thank you very much for your time and valuable insights. Your contribution to this research is greatly appreciated. As mentioned, all information shared will remain confidential and your identity will be protected in the final report.

If you have any follow-up thoughts or wish to review your responses, please do not hesitate to contact me at _____. Once again, thank you."

END OF RESEARCH INSTRUMENTS