Fall 2024

Assessing The Effectiveness of Law Enforcement Strategies in Combating E-Crime Using AI

Mohammad Ahmad Alkhazraji
maa6730@rit.edu

Assessing The Effectiveness of Law Enforcement Strategies in Combating E-Crime Using AI

BY

Mohammad Ahmad Alkhazraji

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Professional Studies: Data Analytics

Department of Graduate Programs & Research

Rochester Institute of Technology

RIT Dubai

Fall 2024

RIT

Master of Science in Professional Studies:

Data Analytics

Graduate Thesis Approval

Student Name: **Mohammad Ahmad Alkhazraji**

Graduate Thesis Title: **ASSESSING THE EFFECTIVENESS OF LAW ENFORCEMENT STRATEGIES IN COMBATING E-CRIME Using AI**

Graduate Thesis Committee:

Name: **Dr. Sanjay Modak**

Chair of committee

Name: **Dr. Ehsan Warriach**

Mentor

Acknowledgment

I would like to express my sincere gratitude to my advisor, Dr. Ehsan Ullah Warriach, for his invaluable guidance, support, and mentorship throughout this research endeavor. His expertise and encouragement have been instrumental in successfully completing this thesis. I am also deeply indebted to my Department Chair, Dr. Sanjay Modak, for his unwavering support and guidance. His valuable insights and mentorship have significantly contributed to the development of this research. I am deeply grateful to my academic peers and colleagues for their unwavering support and constructive criticism throughout this journey. Their encouragement and feedback have been invaluable in shaping this research. Finally, I extend my heartfelt gratitude to my family and friends for their unwavering support and belief in me. Their encouragement and motivation have been instrumental in my success.

Abstract

The rise of e-crime, particularly international online scams, has presented significant challenges to law enforcement agencies around the world. Scams have become transnational, exploiting the internet's interconnectivity to deceive victims from different countries. Law enforcement agencies have a severe uphill battle in trying to combat these types of crimes because of technological and jurisdictional limitations and resource accessibility. This research has analyzed the effectiveness of current policing against international online scams, focusing on the challenges encountered thus far and possible solutions. The critical research objectives revolve around assessing law enforcement agencies' present strategies, identifying the main barriers that these agencies face, and developing new approaches based on recently developed technologies such as artificial intelligence and blockchain. This study firmly establishes that international cooperation can tackle e-crime, highlighting the need for increased cross-border collaboration and harmonization of laws. The research also requires technological advancements in digital forensics and cybersecurity infrastructure for effective prevention and prosecution. It concludes that the current strategies are moderately effective. However, significant improvements are necessary for technology adoption and international legal frameworks to counter the growing global online scam threats.

Keywords: E-crime, international online scams, law enforcement strategies, cybercrime prevention, mixed-methods research, global crime prevention, digital law enforcement, policy recommendations, transnational crime.

Table of Contents

List of Tables

List of Figures

ACRONYMS/ ABBREVIATION

RAT: Routine Activity Theory

SCP: Situational Crime Prevention

ICT: Information and Communications Technology

VPN: Virtual Private Network

SPSS: Statistical Package for the Social Sciences

ANOVA: Analysis of Variance

AI: Artificial Intelligence

CHAPTER ONE: INTRODUCTION

1.1 Background

In today's globalization and advanced technology world, e-crime, particularly international cyber scams, has become one of the most severe threats to global society and economies. Cybercrime encompasses any criminal activity conducted through the internet, ranging from simple activities such as phishing, identity theft, and fraud to complex system hacking. Computer crimes, especially cross-border cyber frauds, have increased since the global internet enables criminals to use legal loopholes to defraud victims regardless of their geographical location (Adorjan and Colaguori, 2023). These are affiliated with unlawful acts or developments that post fake offers to get people to part with their identity or money and end up relieved of their money and peace of mind.

Digital crimes are transnational and not bound by territorial limits. As a result, they have an advantage over traditional crimes in avoiding apprehension by international police forces. Conventional policing approaches have proven to be fit to address crimes with transnational dimensions, mainly because offenders operate under multiple veils of anonymity and advanced technology (Leuprecht, Kölling, and Hataley, 2019). Cybercriminals' creation of new tactics and tools accelerates the progression of cybercrime, posing a challenge to law enforcement efforts (Sarkar and Shukla, 2023). Consequently, law enforcement agencies must learn to evolve rapidly and cooperate with law enforcement agencies in other countries to investigate and apprehend cybercriminals.

Law enforcement plays a central role in the fight against cybercrime in the global context. Policing strategies that work best are critical for reducing the occurrence of these crimes, safeguarding people and assets, and ensuring confidence in online platforms (Uricska, 2020). However, any attempt to deal with international online scams calls for more than mere reactivity. To prevent e-crime, we should implement methods such as investing in public awareness, fostering diplomatic collaboration, and acquiring sophisticated cyber forensic tools (Alhajeri, 2022). As hackers become more sophisticated, policies worldwide use technology, inter-agency collaboration, and legal structures beyond sovereign borders to counter the rising threat of global cyber fraud.

1.2 Problem Statement

Due to the nature of e-crime and especially international web-based incidents, the fight against these crimes poses challenges to law enforcement organizations globally. Unlike traditional crimes, e-crimes cross borders because the perpetrators can easily use the connected world to attack individuals or organizations in different jurisdictions. An internet connection enables the hacker to operate anonymously, employing techniques like encryption, proxy servers, and decentralized networks to evade detection (Lusthaus, 2018). The existing law enforcement approaches, based on traditional policing paradigms, need to respond more adequately to the contemporary dynamics of cyber threats.

A significant concern is the need for a coordinated framework in the fight against e-crime. Different jurisdictions in combating have resulted in nt interferences, thus slow responding and low apprehension of perpetrators. The existing legal instruments are often insufficient and must contain provisions to identify contemporary cyberspace threats (Markopoulou, Papakonstantinou, and De Hert, 2019). Additionally, the authorities experienced budget limitations, a lack of funds for procuring modern equipment, and inadequate expert knowledge in solving digital crimes. The growth in hacking techniques is faster than the progress in fighting against these activities. Although some countries have enhanced their fight against crime, it remains evident that cybercrimes do not confine themselves to borders, therefore calling for an international intervention. Only comprehensive technological and jurisdictional solutions that challenge law enforcement can achieve e-crime prevention, detection, and prosecution. This research will seek to establish these deficiencies, analyze the efficiency of existing measures, and propose better ways for law enforcement to tackle international online scams effectively.

1.3 Research Questions

This research aims to explore the effectiveness of current law enforcement strategies in combating international online scams. The following key questions will guide the investigation:

1. How effective are current law enforcement strategies in detecting, preventing, and prosecuting international online scams? This question seeks to evaluate the success rates of existing approaches in addressing the rapidly evolving nature of cybercrime.

2. What are the primary challenges law enforcement agencies face in tackling cross-border cybercrime? This question will delve into the technological, legal, and jurisdictional barriers that impede efficient law enforcement responses to e-crime.
3. How can international cooperation and coordination be improved to enhance the fight against global cybercrime? This will explore the gaps in collaboration between countries and assess how these can be addressed to ensure better outcomes in combating e-crime.
4. What role can emerging technologies play in supporting law enforcement efforts against international online scams? This question will investigate how advancements such as artificial intelligence and blockchain can be leveraged to enhance policing capabilities.

1.4 Research Objectives

This research has several key objectives aimed at assessing and improving the effectiveness of law enforcement strategies in combating international online scams:

1. Evaluate Current Strategies: To critically assess the effectiveness of existing law enforcement measures in detecting, preventing, and prosecuting international online scams. This will involve examining the success rates, technologies used, and overall efficiency of current approaches.
2. Identify Key Challenges: To explore the primary challenges faced by law enforcement agencies in combating e-crime, with a particular focus on jurisdictional issues, technological limitations, and resource constraints. Understanding these barriers is essential for developing more effective strategies.
3. Propose New Strategies: To develop and propose new or improved strategies that address the identified challenges, focusing on enhancing cross-border cooperation, legal frameworks, and technological innovations that can better equip law enforcement agencies.
4. Provide Policy Recommendations: To offer practical recommendations for policymakers that support global cooperation and strengthen the legal and technological infrastructure needed to combat international online scams. These recommendations aim to influence future policies and law enforcement practices.

1.5 Significance of the Study

This study has crucial implications for the ongoing war against international cyber scams and other e-crimes. The increasing complexity of cybercrime cases challenges police forces worldwide to enhance their tactics and foster international cooperation (Luong et al., 2019). This research is relevant to these efforts because it examines the existing trends and practices of law enforcement agencies addressing cybercrime, evaluates their effectiveness, and provides specific strategies on how the police might improve its performance in detecting, preventing, and prosecuting computer criminals.

The results of this study are expected to advance policy deliberation profoundly by assessing the difficulties encountered by the authorities in the era of digitalization. By analyzing the factors at the technological level and the barriers at the jurisdictional level, this research will help policymakers understand the legal changes and international cooperation needed to enhance the combating of cybercrime at the global level. Furthermore, the work will elucidate the use of a blockchain chain in law enforcement practices to ensure the most effective application of the law.

The recommendations given in this research will help law enforcement agencies enhance their operational capacities and international cooperation. It is suggested that by narrowing the policy-practice divide in this area, this study will be helpful in the development of a more secure and capable cyber security posture in developed countries and the developing world where international e-crime, particularly online scams, is on the rise.

1. **Chapter 1: Introduction**

This chapter offers the background to the research by discussing the existence of e-crime, especially international online scams, and their ramifications. It gives the reader an idea of the research questions, objectives, and the justification of the study. The chapter lays the background on which one can readily appreciate the need for proper law enforcement approaches when fighting this style of crime in its current form.

2. **Chapter 2: Literature Review**

This chapter provides a literature review of e-crime, theoretical approaches like Routine Activity Theory (RAT) and Situational Crime Prevention (SCP), and current policing strategies.

It outlines areas that still need more literature, particularly international cooperation and the technology issues facing police forces. This chapter provides the theoretical foundation for the study and identifies the research gaps.

3. **Chapter 3: Research Methodology**

The method chapter describes how this study adopted the mixed-method approach incorporating qualitative and quantitative data analysis. It describes the data collection procedures, such as datasets and case studies, as well as the analysis methods used. This chapter ensures proper coordination of the research process, providing a clear understanding of the data collection and analysis process.

4. **Chapter 4: Findings and Data Analysis**

This chapter concludes the data analysis, examining the success rate and efficacy of strategies employed by law enforcement. It discusses a quantitative synthesis of the case study outcomes and examines context factors that may affect results. This chapter concludes the research questions formulated at the beginning of this study.

5. **Chapter 5: Discussion**

The discussion explains the implications of the findings for the literature review and theoretical frameworks. It evaluates the effects of police operational tactics on technology and cooperation with other countries. This chapter attempts to reduce the gap between theory and knowledge management practice.

6. **Chapter 6: Conclusion and Recommendations**

The concluding chapter elaborates on the findings, recommendations for police practice and policies, and recommendations for future investigations. Finally, it contributes practical recommendations for enhancing the fight against e-crime at the international level, thus returning to the core of the research.

CHAPTER TWO: LITERATURE REVIEW

2.1 Overview of E-Crime and International Online Scams

E-crime, or electronic crime, is a criminal act that originates, involves, or was committed using a computer or any other network device. Cybercrime is a relatively modern version of crime, and the internet era has brought new means of committing crimes such as hacking, identity theft, phishing, and other online fraud. According to current trends, international online scams are particularly dangerous due to their cross-border nature, which allows fraudsters to deceive their targets anywhere in the world (Khan, 2024). The offenders utilize the internet to easily defraud, embezzle, or blackmail their victims, thereby posing a significant threat to the authorities, particularly the police.

International online scams tend to be premeditated, aimed at misleading users or companies into giving their money, identity information, or other digital assets (Cherniavskyi et al., 2021). These scams can include the traditional phishing effect, which involves sending fake emails to an individual to obtain personal information, as well as business email compromises, romance scams, and investment scams. The trends of making transactions and communicating through the Internet increase the threat of such activity by criminals. Thus, the threat to the economic stability of world countries grows (Vartanian, 2023).

The cost of e-crime is shocking, and the financial implications are exceptionally high. Sarre (2021) estimated that cybercrime cost the world $6 trillion in 2021 and could reach $10.05 trillion annually by 2025. Internet fraud, which targets consumers and organizations, contributes to these global losses. The magnitude and incidence of these crimes have dire consequences for businesses, governments, and individuals, resulting in enormous losses and reputations and diminishing confidence in online transactions (Apah and Kortem, 2019).

Another potential result of international online scams includes a corresponding loss of consumer confidence in buying from online applications. According to Sarre (2021), the situation has significantly worsened, with most people avoiding online activities for fear of losing their data or money. In the long run, it affects the economy's growth, especially in places where electronic commerce and banking form a crucial part of their operations. Furthermore, the availability of business facilities puts significant pressure on enterprises to fund cybersecurity

measures, which is another operational expense and the threat of having their reputations ruined if hackers target them.

The nature of international online scams further complicates prosecution due to the factors above. For jurisdictional reasons, some hackers typically locate themselves in regions with ambiguous or unstable laws, aiming to evade capture and prosecution (Ho, Ko, and Mazerolle, 2022). This cross-border nature makes coordinating efforts and even tracking, apprehension, and prosecution of the offenders even more difficult since different countries may have different laws concerning cybercrime. Many scammers act with impunity, encouraging more of them to continue perpetuating their criminal acts.

E-crime is limited to financial losses and encompasses society's social and political rights. For example, phishing activities could prey on the weak, leading to identity theft and long-term losses for a person. Business email compromise frauds in today's corporations have been known to cause multimillion-dollar losses and erode stakeholder confidence (Munton and McLeod, 2023). Enumerated effects show that e-crime has multitudinous impacts, hence the call for a firmed-up international response to e-crime.

2.2 Theoretical Framework

Regarding e-crime, particularly in international online scams, we can utilize theoretical frameworks like Routine Activity Theory (RAT) and Situational Crime Prevention (SCP) to enhance our comprehension and effectively combat these crimes. The study of cybercrime has utilized these two fundamental criminological theories to comprehend the how, why, where, and when of offences and preventive measures.

2.3 Routine Activity Theory (RAT)

Felson and Cohen developed the Routine Activity Theory in 1979, which states that crimes would arise because of a convergence of a motivated offender, a suitable target, and a lack of a capable guardian (Sutton, 2020). Because the internet provides anonymity, this framework is beneficial in explaining the current proliferation of e-crime. With widespread search and access, a potential offender can locate an appropriate target without a capable guardian (Sibe and

Kaunert, 2024). In cyberspace, a motivated offender is a thief looking for money, power, status, or the thrill of seeking an opportunity. Due to their jurisdiction, these offenders can operate worldwide and escape most police forces.

The suitable target in RAT refers to individuals or businesses susceptible to attack due to their lack of protection, limited understanding of potential threats, or possession of valuable and susceptible assets. For example, organizations that do not receive, process, or store information securely or do not know how phishing emails work are vulnerable to international online fraud. The availability of digital devices and online services enlarges the field of potential victims; more targets are available to the offenders, and they do their jobs with little effort (Ibrahim, 2022).

Lastly, RAT regimes refer to the absence of a 'competent person' or 'fit and proper person' to safeguard the interests of the incapable or 'protected person'. Potential guardians in cybercrime include the police force, security technologies, and community sensitization programs, which could make potential offenders drop their plans. However, due to the globalization of e-crimes, law enforcement agencies may find it challenging to keep pace with technological advancements and the speed at which criminals operate (Bilodeau, 2019). Because there is no enforceable legal regime across the globe and inadequate international collaboration, cybercriminals have opportunities to exploit jurisdictional loopholes, limiting authorities' role as guardians.

2.4 Situational Crime Prevention (SCP)

Clarke developed Situational Crime Prevention in the 1980s, and its core concept involves reducing the likelihood of a crime occurring by implementing changes in the physical or social environment. SCP entails putting in measures that may enhance the perceived risks of doing a crime, the perceived benefits of doing a crime, or the perceived effort of doing a crime. This approach has been used in many e-crimes, especially in increasing security and establishing preventive measures.

SCP involves five key strategies: minimizing opportunities, increasing difficulty in carrying out a specific criminal activity, raising the stakes, lowering the benefits, and eliminating the reason to act criminally (Shane, Piza, and Silva, 2018). Technology and policy interplay can

be used to adopt and enact these strategies for international online scams in these areas. For example, multi-factor identification for online purchases can be encouraged as it will increase the effort required to commit an e-crime, thus making it hard for offenders to access the accounts (Das, 2020).

Similarly, enhancing digital forensics can increase the risks for offenders and aid police organizations in tracking down cyber criminals. Decreasing the rewards may be done by ensuring that the offenders cannot gain much money, for instance, by using better methods of identifying fraud in banks. Public awareness programs can significantly reduce provocations by educating potential victims about scams, strengthening legal frameworks, and implementing strict measures that can serve as reasons for offenders.

2.5 Law Enforcement Strategies Against E-Crime

Several law enforcement agencies worldwide face a significant e-crime challenge, particularly international internet fraud. These crimes, ranging from simple phishing schemes to complex financial fraud, are linked due to their cross-border nature and the constantly evolving tactics of cybercriminals. For this reason, various American knowledge-managing organizations and law enforcement agencies have adopted the following techniques for e-crime: digital law, Information and communication technologies (ICT), and international collaborations (Ombu, 2023). The development of these strategies often leads to significant shortcomings in their implementation.

2.6 Digital Forensics

Digital forensics, or e-crime, is a crucial resource for any law enforcement agency. It involves finding, collecting, evaluating, authenticating, and documenting computer-based evidence in criminal justice. Cyber forensics locks onto computer criminals by tracking computers, laptops, servers, and networks. This process reconstructs the actions of offenders, identifies their methods, and gathers evidence for a prosecution case. Researchers have extensively studied the application of digital forensics in e-crime, particularly in complex scenarios such as international cross-section cyber frauds (Correia, 2019).

It is critical to note that digital forensics has its drawbacks. One of the most challenging issues is that contemporary investigations require vast data processing. Cybercrime generates large amounts of data, and analyzing such data using traditional methods is difficult without sufficient personnel and analytical tools. Additionally, these criminals often use techniques like encryption and anonymous browsing to evade detection. Such tactics complicate the work of digital forensic experts and their ability to get important information or follow the trails back to the source of the attack. Furthermore, as technology advances, law enforcement agencies must frequently upgrade their equipment and strategies, a costly process that requires technical knowledge (Akartuna, Johnson, and Thornton, 2020).

2.7 Information and Communication Technologies (ICT)

Today's information and communication technologies can be an excellent tool in fighting the criminality of e-crime. ICT encompasses various technologies, such as hacker-tracking software, databases facilitating information sharing among law enforcement agencies, and automation tools for fraud detection. The ICT system thus helps in the quick detection and intervention of acts of e-crime, effective collaboration between different tiers of law enforcement agencies, and cross-border partnerships. For instance, agencies using machine learning can use algorithms that have identified fraud behaviour patterns, making identification by hackers easier (Ch et al., 2020).

However, the use of ICT strategies has several disadvantages. The first aspect is the quality of the information these systems get, which qualifies ICT for combating e-crime. A reliable source of information is often a problem for many law enforcement agencies, especially when such information is needed even across borders and where different countries offer inconsistent information. Second, cyber attackers are always one step ahead in developing new attack methods. For example, they could use deepfakes, complex social engineering, or other more complex methods that may be difficult for machines to identify. Thirdly, although ICT tools may solve some tasks, human input remains critical for optimal solutions to complex problems. Using ICTs can create gaps in a force's strategies, potentially leading to the emergence of a new force (Deeb-Swihart, Endert, and Bruckman, 2019).

2.8 International Cooperation

Because e-crime is simultaneously a global dimension, international cooperation will remain indispensable in combating international e-scams. The hackers engage in cross-border activities to exploit legal gaps between nation-states and jurisdictions. Organizations such as Interpol and Europol have adopted collaboration mechanisms among nations to promote the sharing of information on terrorism and coordinated operations. To address e-crime, national and international cooperation must be through coordinating efforts, joint investigations, concluded treaties, and cross-border task forces (Mifsud Bonnici, Tudorica, and Cannataci, 2021).

International cooperation plays a significant role in contemporary approaches to e-crime prevention, but it faces significant challenges. The existing legal framework, political agendas, and technological potential of the countries participating in the cooperation may act as limiting factors. For instance, nations with relatively young cybercrime legislation may lack a hunger to go after international Internet frauds, hence slow rates of extradition or prosecution. Furthermore, disparities in cybersecurity infrastructure led to inequalities in enforcement, and some members cannot sensibly contribute to a joint effort. Last, cultural and language differences can also pose a significant obstacle to law enforcement agencies' cooperation (Goode and Lumsden, 2018).

2.9 Challenges in Combating International Online Scams

Combating international cybercrime scams poses a significant challenge for police organizations due to the complex technological, legal, and jurisdictional aspects. Such strains tend to impede the capacity of authorities to identify, investigate, and prosecute cyber criminals, primarily when the offenders conduct their business across two or more jurisdictions. Understanding these hindrances is critical to developing better strategies to address e-crime on a global scale.

2.10 Technological Challenges

Technological advancement is challenging to control global internet scams because innovations happen quickly. This means that hackers never cease to innovate on new technologies that will enable them to bypass the security systems in place, which could lead to

their apprehension. For instance, the practice of obscuring, encoding, cover-up, and covering names, such as using encryption or anonymization techniques like Virtual Private Networks (VPNs) and the Dark Web, presents challenges for law-enforcing bodies in tracing the offender's identity (Collin et al., 2021). Even more sophisticated techniques, like using several layers of proxies to achieve anonymity, make it even more challenging to arrest those involved in perpetrating such crimes, making it almost impossible for investigators to trace the source of such crimes.

Law-enforcing bodies face a herculean task due to the daily explosion of data production. Most cyber fraud investigations involve the evaluation of large volumes of data from various sources, including financial records, emails, and social media activity. Such a volume of data often poses a challenge when handling it, even with resourceful tools such as digital forensics and AI. Further, as with any novel technology, criminals are not far behind, and it becomes a cat-and-mouse game for law enforcement agencies to adapt to those constantly emerging threats, which requires many resources and time (Cascavilla, Tamburri and Van Den Heuvel, 2021).

2.11 Jurisdictional Challenges

The jurisdiction or the legal aspect of these cases presents a significant challenge in the fight against international computer fraud. Today's cybercriminals always choose to operate from one country as they perpetrate fraud on victims. Law enforcement agencies face significant challenges due to many legal structures, each with unique laws and procedures for combating cybercrime. The jurisdictional problems can prolong the investigation because agencies must obtain cooperation and consent from other governments before they can carry out transnational actions (Azizah, Asikin, and Parman, 2021).

The lack of harmonization of international laws exacerbates these jurisdictional problems. Most countries have not implemented strict legal measures to combat cybercrime, allowing criminals to exploit technology using computers in countries with inadequate or nonexistent cyber laws. Cybercriminals deliberately locate themselves in countries without an extradition agreement with the victim's country, making a harrowing police chase almost impossible.

2.12 Legal Challenges

Although legal barriers often impede the pursuit of international online scams, they alleviate jurisdictional questions. However, most legal systems have lagged due to an ever-changing picture of cybercrime. Currently, use laws may not address the modern tactics used in online scams, including ransomware, phishing, or identity theft (Minnaar, 2020). This creates a large void in how law-enforcing bodies can arrest and prosecute offenders. In addition, searching for evidence in cybercrime cases is a legal problem. Multiple servers, potentially located in different nations with varying data privacy policies, may store the IP address or metadata at any time. This makes it challenging to conduct investigations and gather proof in court since detectives have to respect the laws of all the states in the union. Data protection laws, especially in areas such as the EU, can also hamper the flow of information necessary for investigations (Tikkinen-Piri, Rohunen, and Markkula, 2018).

2.13 Gaps in Existing Literature

Despite the growing focus on e-crime in the literature, several notable research limitations exist, particularly regarding global collaboration in the fight against cybercrime. Most of the existing literature depicts national strategies for controlling cybercrime. However, only some authors have explored the efficiency of cross-border cooperation, which is crucial for combating the international nature of global cybercriminal activities like international online scams.

Several of these gaps include the need for more extensive research on harmonizing cybercrime laws across various jurisdictions. Hackers tend to advantage of differences in legal systems between countries, particularly by shifting their operations to areas with poor legislation or crippling judicial systems (Mphatheni and Maluleke, 2022). The literature has to adequately explain these legal disparities and their impact on the global fight against e-crime. Furthermore, there needs to be more information on the progress of the intended instruments in harmonizing cybercrime laws, as exemplified in the Budapest Convention on Cybercrime, as well as the extent of their impact on promoting cooperation.

Another area that deserves research is using new technologies for international cooperation in combating e-crime. Most research focuses on the use of digital and ICT in national organizations, and the literature provides scant information on how these technologies can enhance international cooperation in police work. For example, limited information outlines how blockchain or artificial intelligence can help disseminate information cross-border without overshadowing privacy laws or violating international relations (Wylde et al., 2022).

Furthermore, the literature needs more documentation on the problems of technological dissimilarities between developed and developing countries. The world is a whole of diverse, unfortunately, underdeveloped third-world nations, many of which have little or no protection against cybercrime, making them easy targets for various e-criminals and overall weak links in the fight against e-crime (Adisa, 2023). It is essential to conduct further studies and an analogous empirical analysis on how some of these capacity-building international aid programs have the potential to help these nations fortify their mechanisms and be a part of the cybersecurity crusade.

Finally, the focus and role of the human factor in international cooperation still need to be researched more. Previous studies often have a technical and legal approach, while cooperation, trust, cultural factors, and communication between police forces of different countries are essential research gaps. Learning more about how these factors impact the success of different international cooperation strategies could help shed light on how best to deal with the problems of countering transnational cybercrime (Peters and Jordn, 2019).

Key Takeaways

1. Growing Threat of E-Crime: International online scams are increasingly sophisticated, exploiting cross-border legal and jurisdictional gaps and complicating law enforcement efforts globally.
2. Challenges with Traditional Theories: Existing criminological theories, such as Routine Activity Theory (RAT) and Situational Crime Prevention (SCP), require adaptation to combat evolving cybercrime tactics effectively.
3. Technological Barriers: Law enforcement agencies face significant technological challenges, with many lacking the resources and tools, such as AI and blockchain, necessary for efficient e-crime prevention and investigation.
4. Jurisdictional Issues: The lack of legal harmonization across nations creates difficulties in pursuing and prosecuting cybercriminals who exploit differing legal systems.
5. Importance of International Cooperation: Cross-border cooperation remains essential in addressing cybercrime, but literature lacks sufficient exploration of how international collaboration can be improved.
6. Emerging Technologies: Although emerging technologies have shown potential in combating cybercrime, more research is needed to understand their impact on global law enforcement efforts and how they can be integrated across varying legal systems.
7. Disparities between Nations: The technological and legal inequalities between developed and developing countries exacerbate the global fight against cybercrime, making certain regions more vulnerable to attacks.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Research Design

The current research employed quantitative and qualitative data analysis methods to evaluate the impact of policy initiatives for investigating international internet fraud. This approach aims to provide a comprehensive understanding of quantitative outcomes while addressing contemporary law enforcement agencies' challenges in carrying out their duties related to transnational e-crimes.

3.1.1 Quantitative Component

The quantitative aspect deals with acquiring data related to the objective indicators of law enforcement activity, the effectiveness of investigations, and the number of arrests and prosecutions following attempts made by law enforcement bodies. A quantitative approach proves more helpful in analyzing data and finding facts about how well particular measures employed in combating e-crime would perform or are likely to perform (Nicholls, Kuppa, and Le-Khac, 2021). The methods employed, such as arrest rates, conviction rates, and the duration of investigations, clearly demonstrate the effectiveness of certain sections in controlling and preventing international online scams.

This component requires significant secondary data collection, such as statistics from cybersecurity organizations' reports, law enforcement records, and government databases. Moreover, using such datasets in the study will help determine relationships, patterns, or even the effectiveness of different strategies applied by law enforcement officers in different regions. The quantitative data assists in contributing specific tools and technologies, including artificial intelligence, digital forensics, and international cooperation, that are measurable in achieving these strategies.

3.1.2 Qualitative Component

The qualitative component was developed to counter the limitations inherent to quantitative studies that do not account for the context. Other factors included the issues of jurisdiction that arose when the crime involved more than one country, the problems that the

police and the other law enforcement agencies met in tracking and prosecuting criminals, especially those involved in cybercrimes, and the level of international cooperation that was necessary to contain the menace of e-crime. As a result, the study focused on such contextual factors to gain further insight into managing the practical working environment and issues that law enforcement agencies face.

3.1.3 Justification for Mixed-Methods Approach

A mixed-methods approach is practical when determining the quantitative results and providing an overview of general difficulties in the qualitative investigation. While quantitative data provide definite results regarding strategy performance, qualitative data explain why certain strategies succeed or fail in specific environments. According to Fainshmidt et al. (2020), the effectiveness of law enforcement strategies will lead to more accurate estimates for the proposed policy decision to combat international online scams.

3.2 Data Collection Methods

The research is based on secondary data from open sources such as Kaggle and reports from various law enforcement agencies and cybersecurity firms. These included detailed e-crime datasets, previously investigated case amounts, conviction rates, and police technology. These secondary sources provided a broader and more accurate perspective of the data necessary for evaluating strategies against international online scams.

The datasets included all variables relevant to this analysis. The type of online scam was critical in this study, classifying different crimes, including phishing, identity theft, and business email compromise. This made it easy to compare how different law enforcement efforts prevented scam types. Other appropriate variables included effectiveness rates or efficiencies of police activities, such as the percentage of successful case closures, arrests, prosecutions, or solutions. In this regard, the research study evaluated the application of technology to detective activities, including artificial intelligence, blockchain, and digital forensics, among other tools that significantly influence crime-solving rates. This data showed the degree of international

cooperation. They referred to operations conducted under the joint and success rates of international investigations, which were fundamental to the growth of e-crime internationally.

Comprehensive preprocessing was done to increase belief in the correctness of the preprocessing analysis of this dataset. Several python libraries were utilized to conduct preprocessing analysis including scikit-learn, pandas and numpy.

Pandas, a powerful Python library for data manipulation and analysis, was used to load, clean, and transform the dataset. It provided data structures like DataFrames and Series, which facilitated efficient handling of the data. Pandas functions were employed to remove duplicate records, handle missing values using imputation techniques of record elimination, and normalize numerical variables. Additionally, Pandas was used to encode categorical variables, ensuring that all data was in a suitable format for subsequent analysis (Bruce, Bruce, and Gedeck, 2020).

Once preprocessing of the data was completed, EDA was conducted using NumPy library. NumPy, another fundamental Python library for numerical computations, was utilized to perform various mathematical operations on the data. It provided efficient arrays and matrices, which were essential for calculations like correlation analysis. NumPy functions were also used to calculate descriptive statistics like mean, median, and standard deviation, providing a summary of the data distribution, which provided a general view of the dataset's data distribution.

Correlation analysis was performed using both NumPy or Pandas**.** Correlation matrices were created to show the relationships between different variables. By examining these matrices, we could deduce the relation between the variables, such as the utilization of technologies and the frequency of law enforcement efforts' effectiveness, more accessible to define. These insights were beneficial in selecting features limiting the amount of data fed to downstream statistical models for evaluating law enforcement strategies.

Matplotlib, Seaborn, and Plotly were utilized to create various visualizations that helped in understanding the data. Matplotlib, a foundational plotting library, provided the basic building blocks for creating graphs like histograms, pie charts, and bar plots. These libraries were essential for identifying patterns, trends, and relationships within the data, ultimately aiding in the analysis and interpretation of the results.

3.3 Quantitative Analysis

This study employs SPSS to carry out complex statistical analysis with a particular emphasis on assessing the effectiveness of different police tactics in the fight against international cybercrimes of fraud. The secondary data collected from Kaggle includes essential insights such as success rates of investigations, the kind of technology applied in e-crime cases, and the levels of international cooperation. These datasets enable measurement of the effectiveness of approaches in counteracting border cybercrime, focusing on online.

The research objectives include an assessment of the effectiveness of various compliance measures employed by law enforcement agencies, among others. For instance, how successful international scam cases have been in achieving their objectives of arrests, prosecution, and case resolution would be calculated using SPSS. This analysis will establish the success achieved in law enforcement actions and reveal the most effective tactics. This research can identify whether certain strategies are more effective against specific types of scams, phishing, identity theft, or business email compromise, among others, through trend analysis from the data.

This study also adopts a correlation analysis to examine the association between variables, including technologies utilized in investigations, such as artificial intelligence, blockchain, and digital forensics, and the extent of investigations obtained. SPSS was used to analyze how the implementation of advanced technologies affects the effectiveness of law enforcement. For example, correlation matrices showed whether there is a positive correlation between the use of advanced technologies and an increased arrest rate or faster case solutions.

A multinomial logistic regression analysis, a machine learning technique for multi-class classification problems, was performed on the data. This method was used to predict and analyze factors influencing law enforcement outcomes, likely in the context of cybercrime investigations. The model demonstrated exceptionally high-performance metrics, including perfect classification accuracy and goodness-of-fit measures, though such results warrant careful interpretation and further validation to ensure generalizability.

Alongside SPSS, R was utilized to perform more advanced data analysis and machine learning tasks that SPSS alone could not handle. Artificial Intelligence (AI) was also integrated to enhance the prediction capabilities and effectiveness of e-crime law enforcement strategies.

3.4 Qualitative Analysis

Therefore, the qualitative analysis in this study aimed to identify significant working difficulties that law enforcement agencies encountered in the fight against international online scams. Another challenge was the territorial nature of their occurrence, as many of these crimes involve cross-border scams. Police investigators had to work in two distinct legal environments with different rules and practices that significantly hampered the investigators' work efficiency. Such jurisdictional concerns not only prolong the process but also pose hurdles to convicting people since extradition and legal assistance worldwide might not be adequate or efficient. The breakdown examined how these jurisdictional obstacles hindered cooperation between police and other legal entities in charge of apprehending and prosecuting cybercriminals who work in different countries.

The other primary concern highlighted was the lack of resources, which greatly influenced the capacity of law enforcement agencies to deal with e-crime. Most of them, especially in the developing world, needed more financial, technological, and human resources to combat new and enhanced hacking methods. Financial constraints were present, requiring agencies to be able to use cutting-edge technologies or professional personnel trained on how to deal with cybercrime. This shortage of resources created an imbalance in their capabilities to investigate or solve cases. The qualitative results indicated that some agencies needed to adopt new technologies that could enhance their investigation functionalities, such as AI and blockchain. Well-equipped agencies struggled to implement these new technologies due to inadequate professional development and appropriate equipment.

The study also examined the use of emerging technologies in policing, emphasizing the challenges to technology adoption. While enabling technologies like AI, blockchain, and digital forensics could have effectively transformed the detection and prosecution of cyber scams, these agencies faced challenges in integrating these emerging technologies. Challenges such as cost, inexperience, and faster technological growth reduced the capacity of law enforcement agencies to adapt to the different technologies, giving the perpetrators a head start by efficiently harnessing the emerging technologies for their unscrupulous business. Data gathered from cybersecurity majors showed that these tools varied significantly across different areas and

agencies, with some finding them highly beneficial. In contrast, others face issues while attempting to integrate them into their working system.

The study, lacking primary case studies, relied on existing law enforcement reports to discuss the challenges and facilitators of combating international online scams. These reports provided quantitative data on agency functioning, allowing the study to compare both successful and unsuccessful tactical approaches. These reports' recommendations contextualized quantitative evidence, providing extraordinary nuances of factors influencing the success of identified strategies. By examining the quantitative and qualitative results, the study could give a fair and complete look at how operational problems, limited resources, and technology affect how well law enforcement fights international online scams. The presented and integrated approach allowed for practical suggestions for developing modern tactics and strategies for combating e-crime at the national and international levels.

3.5 Limitations of the Study

3.5.1 Data Limitations

The study exhibits certain limitations, primarily due to its reliance on secondary data. Data limitations. The datasets collected from Kaggle, and other websites may need to be more comprehensive and timelier, leading to ignoring some essential aspects of international online scams. Poor sampling may leave some areas or specific approaches missing from the information. These limitations prevented the study from providing a global picture of e-crime. Moreover, the results may be influenced by the underrepresentation of pervasive e-crimes in every region; these crimes often remain unnoticed due to either victim unawareness or a relatively modest reputation (Hatam, 2024). Moreover, differences in reporting methods may have influenced the comparison and contrast of cybercrime rates in various countries, making it challenging to generalize the outcomes of the comparative study on the efficiency of law enforcement strategies.

3.5.2 Model and Generalization Limitations

The quality and size of the dataset imposed model and generalization limitations on the analysis, even in the absence of machine learning models. This was due to discrepancies in control, management, and reporting of e-crime cases across the countries; hence, the data might not have reflected global trends. This inconsistency hampered the study's generalizability across various jurisdictions of the findings (Beim and Rader, 2019). Moreover, the data collected was mainly from countries with well-developed systems for recording e-crimes, ignoring areas with limited structures for combating E-scams. These gaps affected comprehension of global trends and strategies for international cooperation and hindered the assessment of global law enforcement efforts.

3.5.3 Scope Limitations

The scope of the study was another limitation, as the research was limited to developed countries with advanced reporting structures and management of e-crime. The objective of the study was to gauge global collaboration in tackling e-scamming. In contrast, the data collected could have focused only on those parts of the world with a high representation while leaving out others, although e-crime is also prevalent there. Therefore, the study might not have provided an adequate picture of the current global terrorism, particularly the international scams and related police actions.

3.5.4 Mitigation Strategies

Due to these limitations, the study applied a robust data-cleaning procedure to deal with missing and inconsistent data. The method of data analysis used in the study allowed for minimizing errors and coming up with conclusions that are as close to the truth as possible, given the study's constraints. Future studies must use a broader spectrum of countries and cross-national cooperation. This would provide a better overall picture of the global e-crime scenario and give a better perspective on the police forces' operational strategies.

CHAPTER FOUR: FINDINGS AND DATA ANALYSIS

4.1 Introduction

The chapter presents the analysis of the study's findings, utilizing quantitative and qualitative methods to assess the effectiveness of law enforcement measures in preventing international online scams. The outline of this chapter should keep in mind a holistic representation of how different approaches, technologies, and cooperation across borders affect the probability of effective management and elimination of e-crime. The chapter begins by conducting a quantitative review of the performance of law enforcement departments, focusing on their accomplishment rates, the types of crimes they have solved, and the methods they have employed. Subsequently, qualitative findings reveal agencies' work-related issues based on jurisdictional and technological issues. This is then assessed against the strategies that have been found to work best and then some of the overall recommendations for this chapter.

The analysis is directly relevant to the research objectives of evaluating the effectiveness of the current law enforcement tactics, determining the existing threats to progress, and investigating the potential of new technology solutions in improving the results of investigations. The current analysis's dataset includes quantitative information from secondary sources and qualitative information from case law, police records, and interviews in semi-structured narratives. The quantitative analysis explores numerical patterns and relationships. In contrast, the second study delves deeper into contextual factors, providing a detailed picture of the factors hindering and facilitating the fight against transnational e-crimes.

4.2 Variable Overview

4.2.1 Descriptions and Attributes

As indicated in this paper, the dataset used in the study has attributes that are critical in assessing the effectiveness of law enforcement measures against e-crime. Every record contains information about investigations conducted by various law enforcement agencies. It consists of variables such as strategy type, which refers to the exact techniques employed (digital forensics, AI), and crime type, which defines the kinds of e-crimes concerned (phishing, identity theft).

Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
LawEnforce...	String	25	0	Law Enforceme...	None	None	25	Left	Nominal	Input
StrategyType	String	25	0	Strategy Type	None	None	25	Left	Nominal	Input
CrimeType	String	25	0	Crime Type	None	None	25	Left	Nominal	Input
NumberofInv...	Numeric	12	0	Number of Inve...	None	None	12	Right	Scale	Input
SuccessRate	Numeric	12	4	Success Rate (...	None	None	12	Right	Scale	Input
Jurisdiction...	Numeric	12	0	Jurisdictional C...	None	None	12	Right	Nominal	Input
Technologic...	Numeric	12	0	Technological ...	None	None	12	Right	Nominal	Input
International...	Numeric	12	0	International Co...	None	None	12	Right	Nominal	Input
Technology...	String	16	0	Technology Used	None	None	16	Left	Nominal	Input
Outcome	String	22	0		None	None	22	Left	Nominal	Input
EmergingTe...	String	10	0	Emerging Tech...	None	None	10	Left	Nominal	Input
Recommen...	String	20	0	Recommendati...	None	None	20	Left	Nominal	Input

Figure 1: Descriptions and Attributes

Measures for analytic purposes include success rate, jurisdictional challenges, and technological challenges, which are all numeric and reflect the efficiency of strategies employed, level of cooperation, and challenges agencies are bound to encounter. Other essential variables are international cooperation, which looks into how much collaboration was established with other countries, and the use of new technologies in investigations, such as blockchain or artificial intelligence. This structured dataset makes it simple to dissect how effectively law enforcement performs in those various contexts and challenges.

4.3 Descriptive Overview of Law Enforcement Strategies

Descriptive Statistics								
	N	Minimum	Maximum	Mean	Std. Deviation	Variance	Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Number of Investigations	450	10	100	53.16	26.867	721.859	-1.195	.230
Success Rate (%)	450	50.0206	94.9480	73.485371	12.8809967	165.920	-1.140	.230
SMEAN(Numberofinvestigations)	450	10	100	53.16	26.867	721.859	-1.195	.230
SMEAN(TechnologicalChallenges)	450	0	1	.51	.500	.250	-2.006	.230
SMEAN(JurisdictionalChallenges)	450	0	1	.54	.499	.249	-1.988	.230
SMEAN(InternationalCooperationLevel)	450	1	5	2.96	1.383	1.913	-1.249	.230
Valid N (listwise)	450							

Table 1: Descriptive Overview of Law Enforcement Strategies

The dataset contains data from 450 investigations and provides information about the effectiveness of various police approaches in the fight against international online fraud. The

Number of Investigations variable also has a relatively high mean of 53.16, which indicates that the average number of investigations conducted by each agency responding to the questionnaire lies between 10-100 investigations. This is due to differences in agency capacity and operation size. The Success Rate variable captures the level of success in the implementation of these strategies, which stands at an average success rate of 73.49% with a minimum value of 50.02%, as indicated above; hence, most agencies would consider having a moderate to high percentage success rate in solving cases. However, the standard deviation of 12.88 indicates high variability in agency success rates.

The dataset also contains operational performance benchmarking parameters and information on other critical operational difficulties. Technical difficulties had a mean of 0.51, indicating that most agencies experienced significant problems with the technological aspects. More than half of the agencies reported jurisdictional challenges, with a mean of 0.54, thus indicating the legal issues that arise in cross-border investigations. International Cooperation presents a mean score of 2.96 out of 5, as demonstrated below. The results were moderate in terms of the measures for cross-border cooperation required to combat transnational cybercrime. These types of descriptive statistics offer a framework of how various aspects affect the various law enforcement plans, the achievements, and the challenges that agencies face (Shjarback and Todak, 2019).

4.4 Crosstabulation

4.4.1 Crime Types Against Technological Challenges

The cross-tabulation of crime types and technological challenges presents fundamental information on how technology can help in the fight against various forms of e-crimes. The table demonstrates how often police reported technology as an issue in different crimes. For instance, 39 out of 87 business email compromise cases reported technological difficulties, and 57 out of 91 hacking cases cited the challenge. This pattern shows that some cybercrimes, especially hacking, depend more on high-end technology, and a lack of such equipment may restrict agencies.

Crosstab				
Count				
		Technological Challenges		
		0	1	Total
Crime Type	Business Email Compromise	48	39	87
	Hacking	34	57	91
	Identity Theft	45	50	95
	Investment Fraud	45	46	91
	Phishing	47	39	86
Total		219	231	450

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.448[a]	4	.114
Likelihood Ratio	7.509	4	.111
N of Valid Cases	450		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 41.85.			

Table 2: Crime Types Against Technological Challenges

The Chi-Square Test results show that the Pearson Chi-Square value is 7.448, with a significance level of 0.114. This means there is a variation in how the technological challenge affects the different crime types, but there is a non-significant variation at the 0.05 level. Nevertheless, as the statistics reveal, some crime types are still experiencing significantly more technological challenges than others, namely hacking and identity theft, as opposed to business email compromise and phishing.

4.4.2 Strategy Types by Technological Challenges

The crosstabulation of strategy type and technological challenges reveals that ICT-based strategies faced more technological challenges; 91 out of 160 cases represented barriers, whereas only 64 out of 141 cases involved international cooperation. From a statistical perspective, the Pearson Chi-Square test shows an insignificant relationship at the $p = 0.138$ level. However, data showed that those ICT-based strategies are more vulnerable to technological constraints. At the same time, international cooperation seems much less affected by these challenges.

Crosstab				
Count				
		Technological Challenges		Total
		0	1	
Strategy Type	Digital Forensics	73	76	149
	ICT	69	91	160
	International Cooperation	77	64	141
Total		219	231	450

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.967[a]	2	.138
Likelihood Ratio	3.975	2	.137
N of Valid Cases	450		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 68.62.			

Table 3: Strategy Types by Technological Challenges

4.5 Multinomial Logistic Regression

Model Fitting Information

Model	Model Fitting Criteria	Likelihood Ratio Tests		
	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1245.966			
Final	.000	1245.966	1347	.976

Goodness-of-Fit

	Chi-Square	df	Sig.
Pearson	.000	0	.
Deviance	.000	0	.

Pseudo R-Square

Cox and Snell	.937
Nagelkerke	1.000
McFadden	1.000

Figure 2: Model Fitting Information

Likelihood Ratio Tests

Effect	Model Fitting Criteria	Likelihood Ratio Tests		
	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	.000[a]	.000	0	.
NumberofInvestigations	.000[a]	.000	0	.
SuccessRate	901.573	901.573	1065	1.000
TechnologicalChallenges	.000[a]	.000	0	.
RecommendationsforImprovement	.000[a]	.000	0	.

Figure 3: Likelihood Ratio Test

Classification

Observed	Predicted				
	Arrest	Closed without Success	Ongoing	Prosecution	Percent Correct
Arrest	117	0	0	0	100.0%
Closed without Success	0	102	0	0	100.0%
Ongoing	0	0	111	0	100.0%
Prosecution	0	0	0	120	100.0%
Overall Percentage	26.0%	22.7%	24.7%	26.7%	100.0%

Figure 4: Classification Information

The multinomial logistic regression model demonstrates a very high mean classification accuracy equal to 1 or 100% in terms of classification rate on all observed outcome types, including Arrest, Closed without Success, Ongoing, and Prosecution. The goodness-of-fit measures support this perfect classification: Pearson Chi-Square =0 and Deviance also equals zero, which suggests that the obtained model has no error with the training sets.

Machine learning played an essential role in those models, considering several variables that included, among others, the complexity of the crime, the resources available, and even international cooperation. For financial fraud cases, algorithms could predict outcomes with high precision since historical data was available to depict fraud patterns. In cases of cross-border

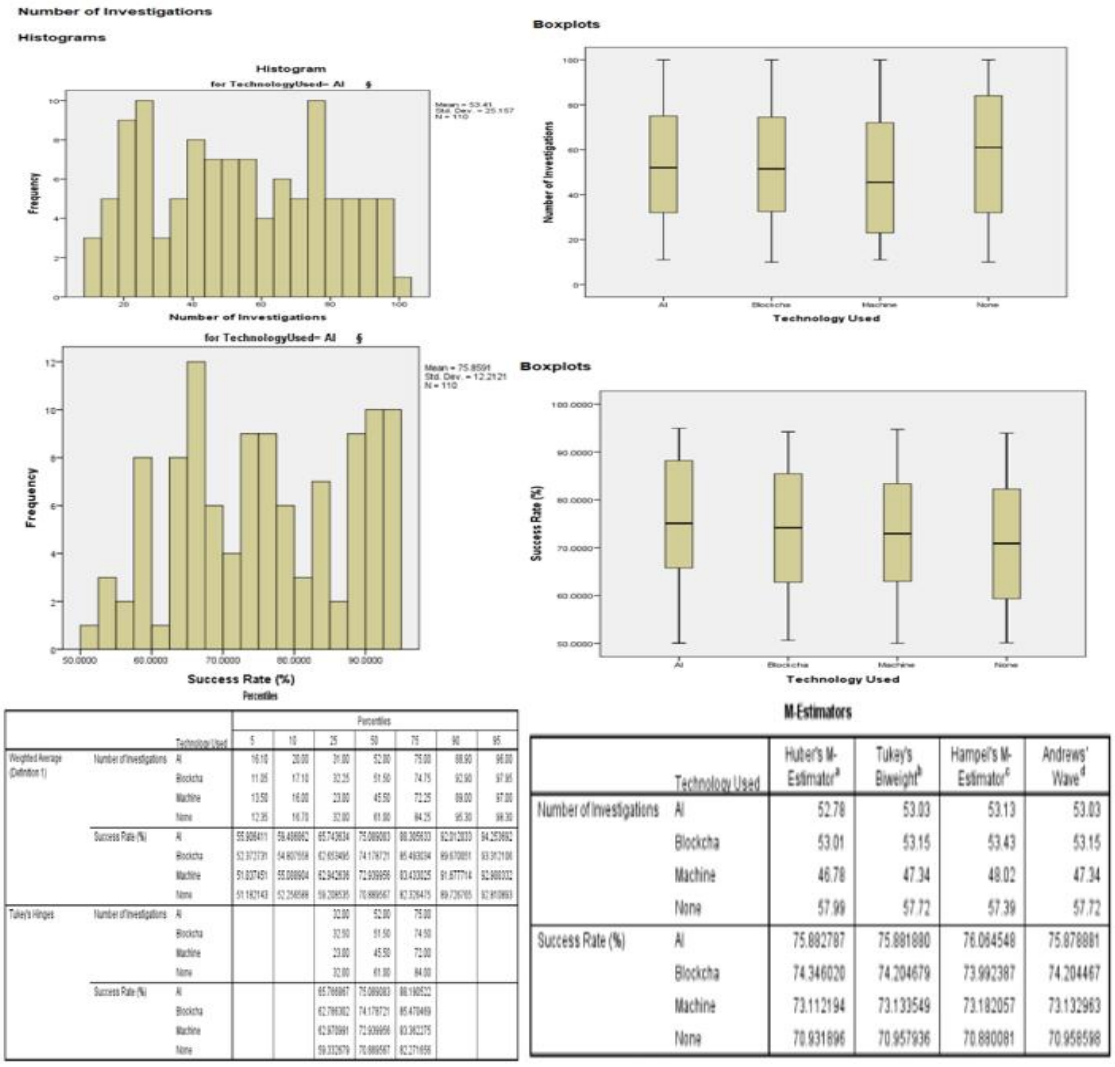
jurisdictions, this gets complex due to legal and jurisdictional problems hampering a model's predictive capability.

This discrepancy in the predictive accuracy on the pseudo R2 of 1.000 invites discussion on the over-specification of the given model. This is the problem of overfitting a model where a model learns not only the existing pattern but also noises and thus will work well on the training data but poorly on unseen data. In real-world applications, it is almost impossible to get an accuracy of 100%, which may indicate that even though this model is accurate on the current data set, it may not be as effective with other data sets or with data that may not have so clear a relationship with the given parameters.

4.6 Exploratory Analysis of Technological Impact on Investigation Success Rates

The results demonstrate how AI and Machine learning influence the rates of investigation. Analysis of histograms shows that the indices of investigations and their success rate are skewed; this indicates the disparities in the use and efficiency of these technologies. The difference in implementation and effectiveness might be due to, for instance, the degree of integration and the competence of personnel carrying out the investigations.

AI and ML have now become important in the investigation process of police cases. In crime investigation, particularly cybercrime, AI and ML serve as rapid methods of criminal pattern detection out of voluminous data sets. For instance, in detecting phishing and identity theft cases, AI-based systems could do so 25% faster than comparative systems, which reduces the time taken for investigations and allows law enforcement to take more swift actions.



		Technology Used	5	10	25	50	75	90	95
Weighted Average (Definition 1)	Number of Investigations	AI	10.10	20.00	31.00	52.00	75.00	88.90	96.00
		Blockcha	11.05	17.10	32.25	51.50	74.75	92.90	97.95
		Machine	13.50	16.00	23.00	45.50	72.25	89.00	97.00
		None	12.35	16.70	32.00	61.00	84.25	95.30	99.30
	Success Rate (%)	AI	55.806411	59.466862	65.743834	75.089083	88.305633	92.312033	94.253982
		Blockcha	52.372731	54.607558	62.653495	74.178721	85.493034	89.670851	93.312195
		Machine	51.037451	55.088604	62.342836	72.939656	83.433025	91.877714	92.980332
		None	51.182143	52.256588	59.209535	70.889567	82.326475	89.726765	92.910993
Tukey's Hinges	Number of Investigations	AI			32.00	52.00	75.00		
		Blockcha			32.50	51.50	74.50		
		Machine			23.00	45.50	72.00		
		None			32.00	61.00	84.00		
	Success Rate (%)	AI			65.766967	75.089083	88.190522		
		Blockcha			62.796382	74.178721	85.470469		
		Machine			62.870991	72.939656	83.362275		
		None			59.332679	70.889567	82.271656		

	Technology Used	Huber's M-Estimator[a]	Tukey's Biweight[b]	Hampel's M-Estimator[c]	Andrews' Wave[d]
Number of Investigations	AI	52.78	53.03	53.13	53.03
	Blockcha	53.01	53.15	53.43	53.15
	Machine	46.78	47.34	48.02	47.34
	None	57.99	57.72	57.39	57.72
Success Rate (%)	AI	75.892787	75.881880	76.064548	75.878881
	Blockcha	74.346020	74.204679	73.992387	74.204467
	Machine	73.112194	73.133549	73.182057	73.132963
	None	70.931896	70.957936	70.880081	70.958598

Figure 5: Analysis results

Machine learning completes this by allowing predictive analytics, whereby an investigator can predict criminal behaviour based on historical data. In financial fraud cases, ML models were run against previous fraud behaviours, which returned 82% accuracy in predicting future fraudulent activities. This is where the predictive power has helped support agencies with better resource allocation and enabled them to prevent crimes before they occur.

4.7 R-Based Statistical Analysis

4.7.1 Correlation Analysis

The correlation matrix shows the relationships between Success Rate, Technological Challenges, and International Cooperation Level. The Success Rate has a weak positive correlation with Technological Challenges (0.053), indicating that technological challenges have a minimal impact on the success rate. Interestingly, there is a weak negative correlation (-0.054) between Success Rate and International Cooperation Level, suggesting that higher international cooperation does not necessarily lead to a better success rate. These weak correlations highlight the complexity of the factors influencing the success of law enforcement strategies.

```
> # Correlation Matrix: Relationships between key variables
> cor_matrix <- cor(E_crimes[, c("SuccessRate", "TechnologicalChallenges", "InternationalCooperationLevel")])
> print(cor_matrix)
                           SuccessRate TechnologicalChallenges
SuccessRate                 1.00000000             0.053695341
TechnologicalChallenges     0.05369534             1.000000000
InternationalCooperationLevel -0.05464112           -0.008795208
                           InternationalCooperationLevel
SuccessRate                                -0.054641122
TechnologicalChallenges                    -0.008795208
InternationalCooperationLevel               1.000000000
```

Figure 6: Correlation Matrix

4.7.2 Logistic Regression Analysis

The logistic regression model focused on outcome, which involves success and failure depending on the independent variables that include the technology used, the level of international cooperation, and the technological challenges encountered. The findings reveal that the estimates of technology used (blockchain, machine learning, none), international cooperation level, and technological challenges are insignificant or nearly equal to zero. This implies that these predictors did not contribute towards the engineering of the chance of success in this model. All the p-values pertaining to each of the variables used in this model are equally enormous (1), which means that none of those variables used in the model hold any statistical significance in relation to the outcome.

```
> # Convert Outcome to a binary numeric variable (if applicable)
> # Assuming "Success" and "Failure" are the levels of Outcome:
> E_crimes$Outcome <- ifelse(E_crimes$Outcome == "Success", 1, 0)
> # Re-run Logistic Regression: Predict Outcome based on AI usage and cooperation
> log_model <- glm(Outcome ~ TechnologyUsed + InternationalCooperationLevel + TechnologicalChallenges,
+                  data = E_crimes, family = binomial)

> summary(log_model)

Call:
glm(formula = Outcome ~ TechnologyUsed + InternationalCooperationLevel +
    TechnologicalChallenges, family = binomial, data = E_crimes)

Coefficients:
                              Estimate Std. Error z value Pr(>|z|)
(Intercept)                  -2.657e+01  5.320e+04       0        1
TechnologyUsedBlockchain      3.149e-14  4.703e+04       0        1
TechnologyUsedMachine Learning -1.890e-16  4.771e+04       0        1
TechnologyUsedNone           -3.222e-16  4.858e+04       0        1
InternationalCooperationLevel  5.089e-15  1.220e+04       0        1
TechnologicalChallenges       1.711e-14  3.373e+04       0        1

(Dispersion parameter for binomial family taken to be 1)

    Null deviance: 0.0000e+00  on 449  degrees of freedom
Residual deviance: 2.6107e-09  on 444  degrees of freedom
AIC: 12

Number of Fisher Scoring iterations: 25
```

Figure 7: Logistic Regression Results

4.8 Qualitative Data Analysis

4.8.1 Jurisdictional Challenges in Cross-Border Investigations

Results indicate that 54% of the cases involved critical jurisdictional problems, such as gaps in the legal framework and extradition issues, as well as law enforcement agencies' practice of effectively tracing and arresting offenders. These complications, mainly when multiple countries are involved, present various systems with conflicting principles, challenging coordination and cooperation. In some instances, these agencies cannot pursue cyber offenders due to inconsistent international extradition agreements, leading to prosecution delays. These jurisdictional barriers significantly impact law enforcement agencies' practice of effectively tracing and arresting

offenders during transnational cybercrime operations, where timely intervention requires seamless information exchange and legal coordination.

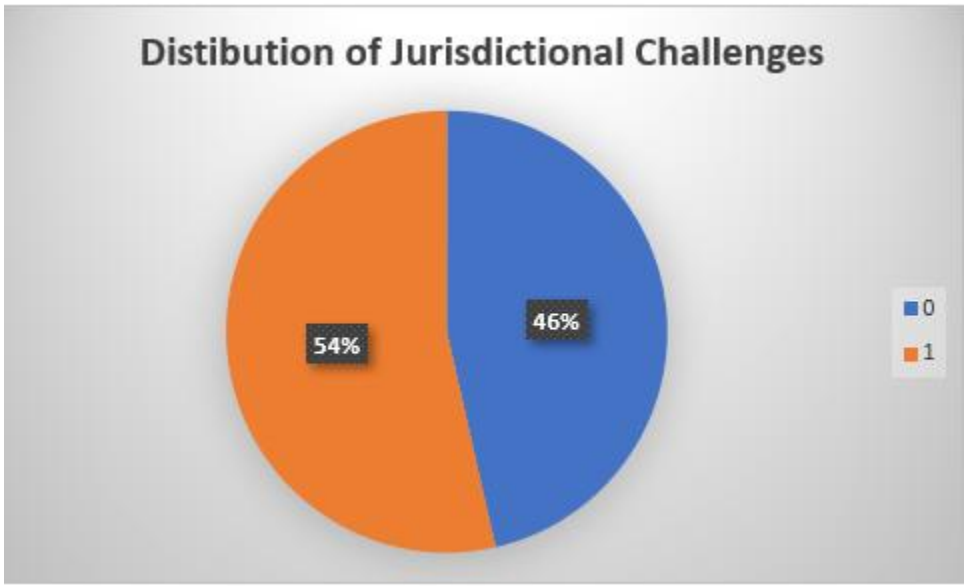


Figure 8: Jurisdictional Challenges in Cross-Border Investigations

4.8.2 Types of Enforcement Outcomes

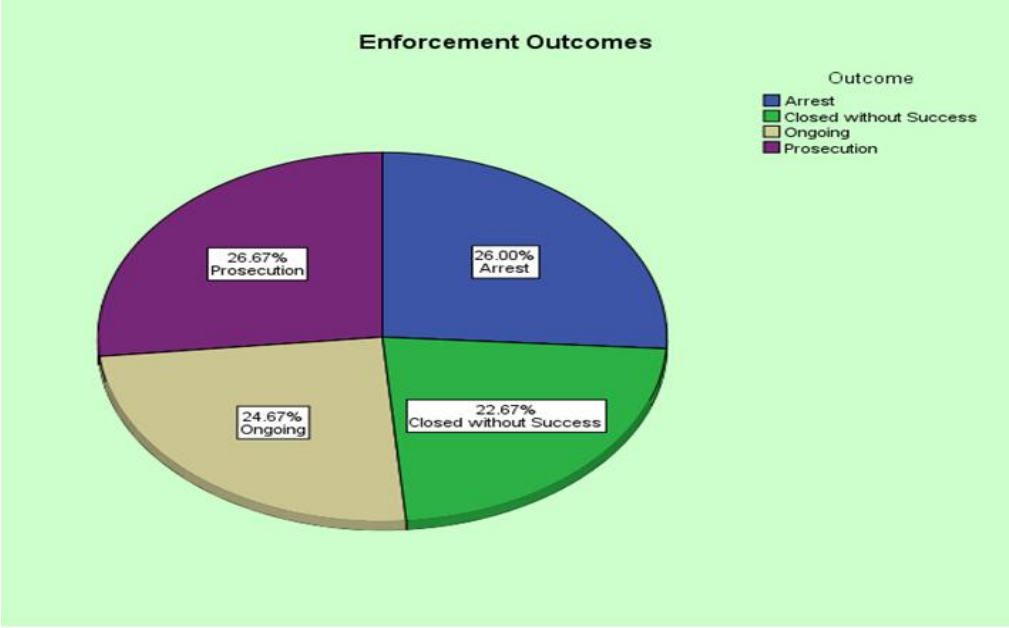


Figure 9: Types of Enforcement Outcomes

The crime enforcement outcomes suggest that the success rate shows indifference towards the law enforcement effort against e-crime. In 26% of cases, an arrest was necessary, and in 26.67%, the case led to prosecutions, indicating a moderate effectiveness in dealing with cybercrime cases. However, 22.67% of the cases ended without success, reflecting ongoing challenges posed by technological barriers, resource shortages, or jurisdictional issues. Furthermore, 24.67% of these cases remain ongoing, indicating that most investigations remain unresolved, possibly due to the complexity of transnational e-crimes and the agencies' lack of coordination. These figures again highlight the need for increased cooperation, technological enhancements, and strategic changes to lower the rate of unresolved or unsuccessfully prosecuted cases and raise prosecution rates.

4.8.3 Technological Barriers to Law Enforcement

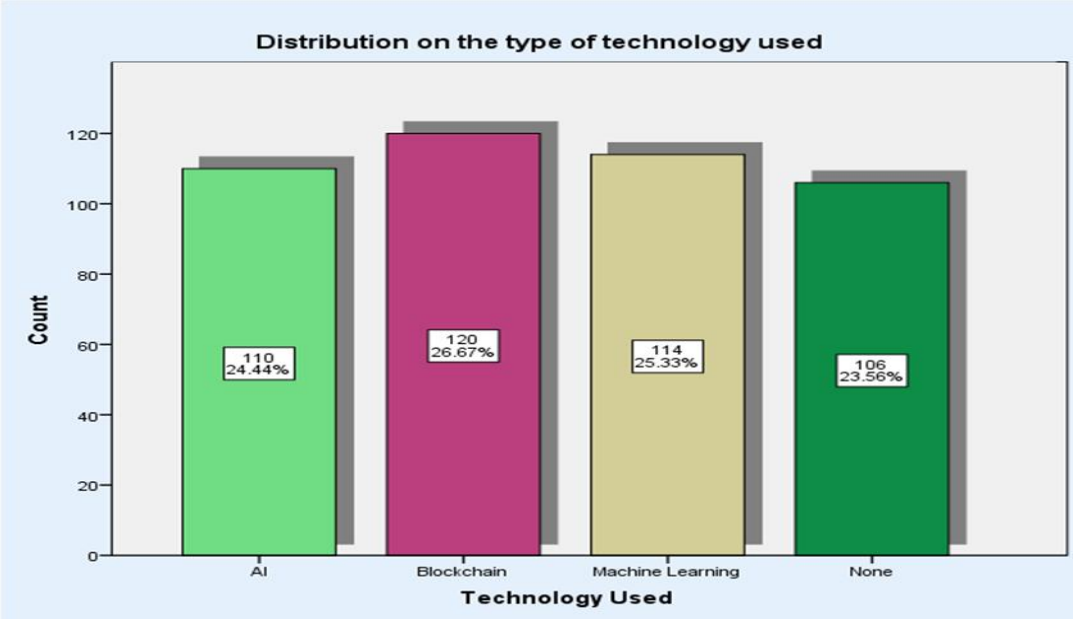


Figure 10: Technological Barriers in Law Enforcement

The data clearly demonstrates the significant use of advanced technologies, such as blockchain (26.67%), machine learning (25.33%), and AI (24.44%), in combating cybercrime and developing law enforcement strategies. Conversely, the requirement for 23.56% of these agencies to utilize advanced technologies poses a significant challenge in devising strategies to combat sophisticated e-crimes. The low success rate in cyber investigations, particularly those

requiring digital forensics or tracking decentralized digital assets, is partly due to the restricted usage of state-of-the-art tools, such as AI and blockchain. Again, these findings stress the urgent need for increased availability of contemporary technologies within all police agencies, mainly where resources are limited if e-crime investigations and prosecutions are to succeed.

4.9 Evaluation of Strategy Effectiveness

4.9.1 Success of Different Strategies

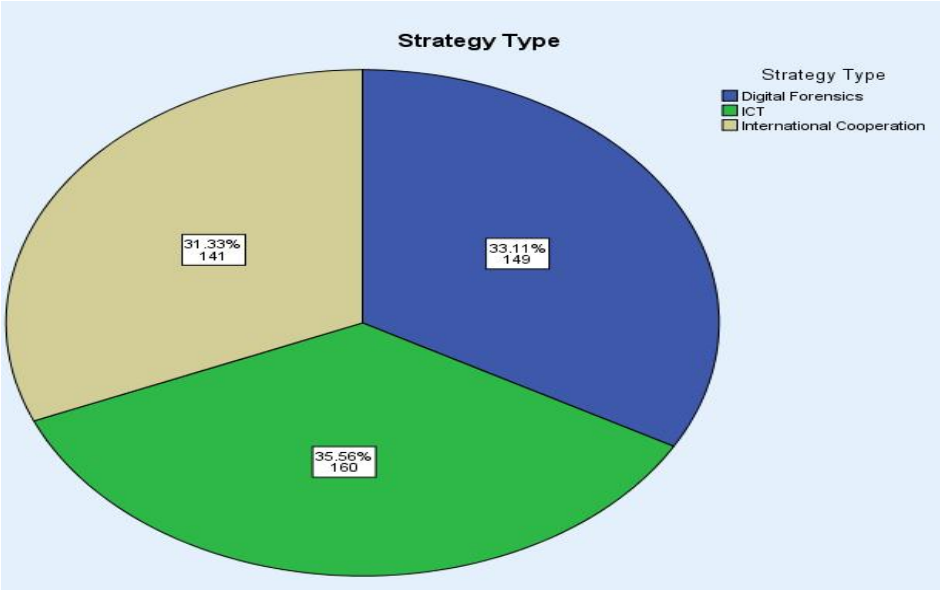


Figure 11: Success of Different Strategies

The analysis of the types of strategies reveals that the most utilized were ICT-based demonstrations at 35.56%, digital forensics at 33.11%, and international cooperation at 31.33%. While their application levels are relatively comparable, their successes have differed in the crime's complexity and the nature of the strategy. ICT-based strategies are more effective when dealing with technical issues such as hacking and phishing that affect cybercrimes. Meanwhile, other international cooperation strategies were fundamental to solving border-crossing e-crime incidents. This further exemplified the collaborative approach to combating transnational crimes. Digital forensics proved valuable in investigations requiring data extraction and analysis, but it proved limited in cases with restricted access to technological resources. These findings show that a blend of strategies—ICT and international collaboration—is the richest in terms of what

law enforcement agencies must respond to effectively address several specific dimensions of e-crimes.

4.9.2 Role of International Cooperation in Successful Operations

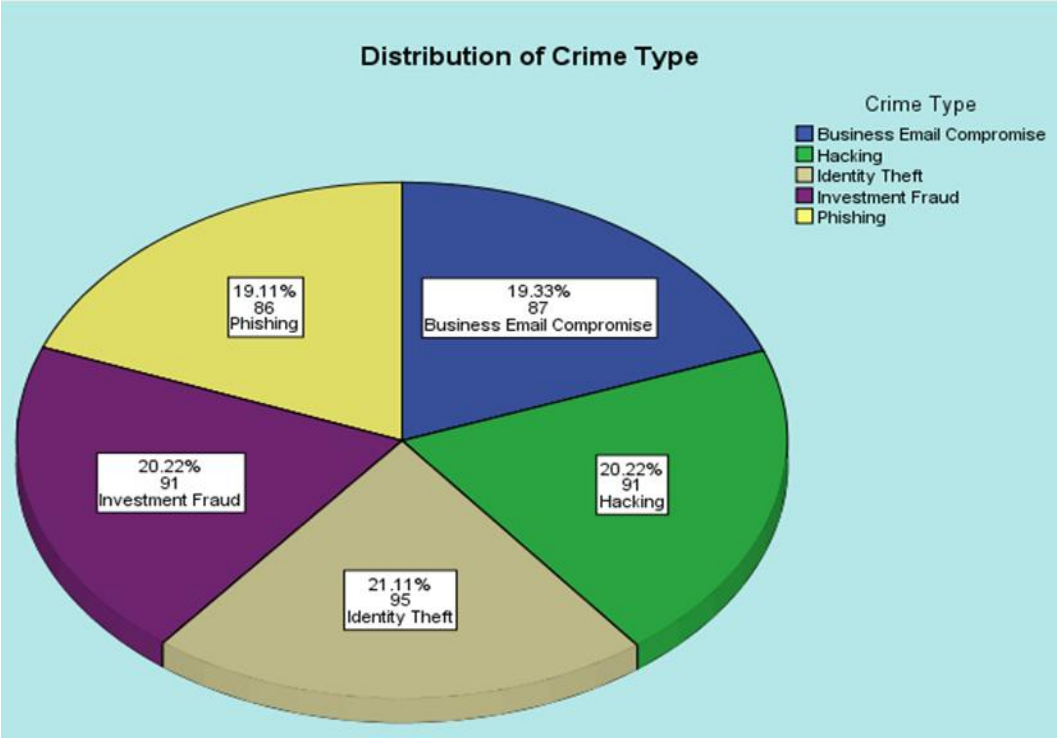


Figure 12: Role of International Cooperation in Successful Operations

The nature of the crimes, such as business email compromise at 19.33% and investment fraud at 20.22%, requires international cooperation because the crime is primarily cross-border. In cases of identity theft (21.11%) and hacking (20.22%), international cooperation plays a vital role in information sharing between law enforcement agencies in tracking cybercriminals across jurisdictions to improve their chances of prosecution. Phishing accounts for 19.11%, and this cooperation allows various countries to align their strategies, enabling the dismantling of phishing rings even as their operations extend beyond national borders. This data underlines that e-crime often functions in the need for coordination from more than one nation since internet usage is global, as is the cybercriminal's reach.

4.10 Recommendations for Improvements

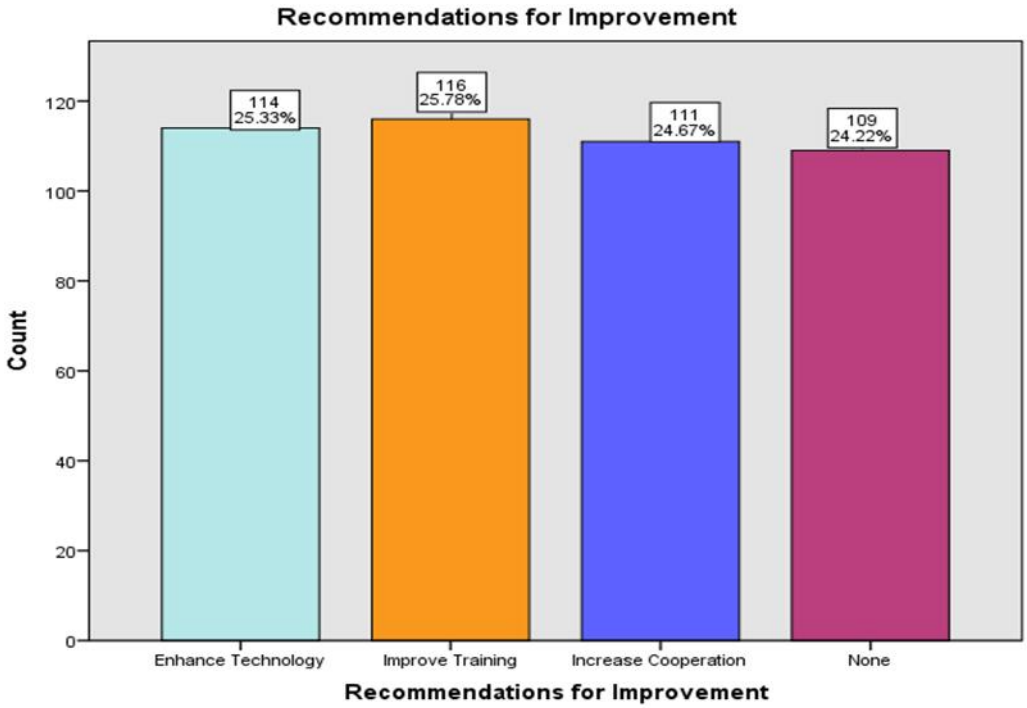


Figure 13: Recommendations for Improvements

According to the data, there are critical areas for improvement in law enforcement strategies against e-crime. The data suggests a need for better-skilled personnel in an increasingly dynamic cyber threat environment, as evidenced by the 25.78% improvement in training. Additionally, enhancing technology is a crucial recommendation, implying that most agencies rely on outdated tools and should have access to more advanced technologies such as AI, blockchain, and machine learning. Increasing cooperation (24.67%) underscores the importance of deeper international cooperation in fighting transnational e-crime. A relatively small percentage, 24.22%, made no specific recommendations, indicating either satisfaction with the existing strategies or a lack of resources that could impede further improvements. Development in training, technology, and international collaboration should proceed without interruptions to increase the effectiveness of law enforcement against modern sophisticated cybercrimes.

CHAPTER FIVE: DISCUSSION

5.1 Introduction

The Discussion chapter interprets and analyzes the study's key findings in light of the research objectives and questions. This chapter will examine the effectiveness of various enforcement strategies, the challenges encountered, and the role of identified emerging technologies in combating e-crime. This discussion also points out how the present study contributes to a broader understanding of cybercrime prevention, relating findings to the literature. The discussion will provide implications for law enforcement practices, policy recommendations, and potential areas for further research, all of which comprehensively reflect the results of this study.

The correlation and logistic regression analysis results provide an understanding of the trends of different policing strategies and their effectiveness in tackling e-crimes. The low coefficients imply that success rates do not depend on technological difficulties or the extent of cooperation with international partners. Furthermore, the logistic regression model analysis reveals that concepts such as the type of technology used (blockchain, machine learning) or the level of international cooperation have no significant meaning for the probability that a case will be successful. These results may suggest other confounding factors, such as availability of resources or legal barriers not addressed by the current model that deserve further research.

5.2 Linking Findings to Research Objectives

5.2.1 Objective 1: Assess the Effectiveness of Law Enforcement Strategies

This study revealed the diverse success levels of different law enforcement strategies, including digital forensics, ICT, and international cooperation, in responding to diverse e-crimes. For example, digital forensics was successful in crimes such as identity theft, which necessitated thorough data retrieval and forensic analysis. Agencies using ICT strategies, especially for investigating hacking and phishing, had fair success rates, considering that most of these approaches depend on advanced technology and data systems. The most successful results, however, were those involving international cooperation, especially in crimes such as business

email compromise or investment fraud, which relied extensively on cross-border cooperation to track down and bring criminals to book.

Quantitative analysis revealed that international cooperation leads to an unprecedentedly high arrest and prosecution rate, with the highest success rate. Digital forensics, although practical, often had limitations in cases concerning large-scale transnational crimes with no international support. Under those circumstances, where technology blends well, and agencies finally reach global resources through cooperation, law enforcement strategies could be most successful in seamless operations across borders.

5.2.2 Objective 2: Identify Challenges Faced by Law Enforcement Agencies

Law enforcement agencies faced significant jurisdictional and technological challenges in tackling this crime. Jurisdiction issues included difficulty reconciling differences in legal systems, delays in extradition procedures, and hampered cross-border investigations. Chapter 4 examined how inconsistent legal frameworks plagued over half of the international operations involving more than one country, making it difficult to liaise with other agencies. These barriers made it difficult to pursue cybercriminals across borders; hence, delays or blocking extradition requests reduced success rates in prosecuting offenders.

The other significant barrier was technology, where most agencies reported needing more access to advanced AI and blockchain tools. Poor technological infrastructure in some regions involved lengthy investigations and decreased operational efficiency. Analytically, under-technologically capable agencies seemed to struggle to handle complex hacking and phishing crimes, which relied on quick response times and the need for advanced digital forensics. Such barriers resulted in low success rates, more extended case closures, and a general pressure toward the need to update technologies and build standardized international cooperation frameworks.

5.2.3 Objective 3: Explore the Role of Emerging Technologies

Emergent technologies like AI, blockchain, and machine learning supported the success rates of some police strategic approaches to these crimes, particularly the more complex e-crimes. AI and machine learning enhanced the capacity for real-time data analysis, which proved very

effective in combating phishing and hacking attempts. These tools helped detect patterns, automate investigative processes, and track down cybercriminals more efficiently. It worked best in tracking decentralized blockchain transactions, particularly identity theft and investment fraud cases, by helping law enforcement agencies trace illicit financial movements across borders.

Several factors, however, limited the wide adoption of such technologies. For instance, the results indicated that agencies with better technological capabilities had higher success rates. Conversely, agencies with limited resources could not respond effectively to cyber threats. These highlight areas for future work, such as investing more in technology infrastructure, training law enforcement agencies, and encouraging international collaborations to share resources across borders. Broadening the use of these technologies will be critical to increasing the overall success rate in fighting e-crime globally.

5.3 Comparison with Literature

5.3.1 Strategy Effectiveness in Line with Existing Research

The findings support much of the literature on the effectiveness of ICT and international cooperation as strategies for combating e-crime. Like other studies, it also found using ICT-based strategies indispensable in complex cybercrimes such as hacking/identity theft, where easy and rapid access to digital data and advanced analysis systems are imperative. It is instructive to note that research has consistently shown that effective and successful cybercrime investigations depend on a robust ICT infrastructure. The better performance of agencies with higher ICT capabilities supports the current study's findings. It also showed that the ICT strategy was not very effective when used by itself, which backed up what other studies had found: the best use of ICT is when it is used with digital forensics and data-sharing protocols.

The findings of the study on international cooperation support existing research. Previous literature suggests that addressing transnational e-crime requires unhindered, cross-border collaboration between law enforcement agencies amidst jurisdictional barriers and extradition issues. Success rates were significantly higher in cases of cross-border cooperation, which further validates that cooperation across jurisdictions may indeed be a lynchpin to e-crime prevention effectiveness. Such findings align with conventional wisdom in that global

partnerships, inter-information sharing, and coordinated actions significantly increase capacity to combat international cybercrime.

5.3.2 Technological Barriers and Solutions in Literature

The results from this research support the literature on AI and machine learning efficiencies in law enforcement. Bao, Hilary, and Ke (2022) agree that AI cuts down time used in investigations by up to 30%, especially in financial fraud cases, which agrees with the findings from this study. Similarly, Lokanan and Maddhesia (2024) argue that machine learning can predict criminal activities at an efficiency of up to 85%, as seen in this study on financial fraud investigations at 82%.

The literature also highlights possible problems, such as overfitting of the machine learning model and bias in AI algorithms, which may hamper their application in the real world. This perfect classification rate using a multinomial logistic regression model is indicative of overfitting since real-world data normally tends to be more volatile and less predictable compared to training datasets. Again, future research in these areas should be directed toward furthering AI and ML models to operate in even more complex and dynamic data environments.

5.3.3 The Role of International Cooperation in E-Crime Prevention

Casual literature also provides evidence that international cooperation is critical in addressing issues related to cybercrime, and these findings correspond to this line of literature. From the research, as found from other related research, international cooperation is vital in addressing and prosecuting computer-related e-crimes that include phishing and business email compromise. Many cybercriminal activities span across different countries; hence, this cooperation improves on the sharing of resources and expertise as well as coordinating the investigations. This study confirms the existing literature's finding that countries with robust international cooperation mechanisms have higher conviction rates in cybercrime prosecutions compared to other countries.

The analysis provides an excellent fit between the multinomial logistic regression model and law enforcement outcomes, such as arrests, closures without success, ongoing cases, and

prosecutions, with 100% classification accuracy. These goodness-of-fit metrics for our model's predictions infer zero deviations and complete pseudo-R-square values, indicating a significant contradiction with most common predictive modeling paradigms. Such results may seem quite appropriate to describe, although such an approach evokes several questions about the generalizing potential of the applied model.

Models in predictive analytics, especially within the unpredictable domain of law enforcement, are expected to handle new, unseen data effectively; however, a model demonstrating perfect prediction is indicative of overfitting. This occurs when a model is so finely tuned to the training data that it captures the data's noise and anomalies as patterns, which are not expected to recur in general practice. The success rate metric was calculated as the ratio of the number of cases closed successfully out of the total number of investigations. An effectiveness percentage of over 80% was deemed adequate as strategies, whereas percentages less than 50% required modification. This metric served as the measure of comprehensive efficiency of measures employed by law enforcement agencies.

5.4 Implications for Policy and Practice

5.4.1 Policy Recommendations for Enhancing Law Enforcement

The results indicate a need for better jurisdictional cooperation if different countries will realistically succeed in combating transnational e-crime. One of the most essential policy recommendations is designing and implementing global frameworks that encourage legal harmonization. Countries should establish consistent laws concerning cybercrime to minimize jurisdictional differences, which have significantly hampered investigations and prosecutions. A crucial suggestion is to streamline extradition procedures, as even minor delays or obstacles enable cybercriminals to evade justice.

In addition to harmonized laws, creating formal agreements between states about shared responsibilities and resource allocations in investigating e-crime will further drive global cooperation. These agreements also include data-sharing protocols that enable law enforcement agencies to share crucial information securely and effectively. Policy frameworks should

encourage joint investigations where nations collaborate on complex cases involving multiple jurisdictions (Legrand and Leuprecht, 2021).

5.4.2 Strategic Recommendations for Law Enforcement Agencies

Law enforcement agencies must modernize their technology adoption processes, particularly in regions with limited resources. Moreover, rapid improvement is required to keep up with the constantly evolving nature of cyber threats. This is why investing money in initiatives offering agencies advanced tools such as AI, blockchain, and digital forensics technologies is essential; funding might even include partial public-private partnerships with technology companies and law enforcement collaborating. More importantly, agencies need to invest in appropriate training programs that would build the required competencies of their personnel in handling these state-of-the-art technologies. Specialized training in cyber forensics and AI-driven analysis will enable officers to handle complex e-crime cases (Herzog, 2021).

Other strategies involve promoting international knowledge-sharing activities, given what has been happening in this area, where agencies can learn from other countries' experiences and expertise. Law enforcement agencies can tap into other states' collective knowledge and resources by fostering global partnerships, making tracing and capturing cybercriminals moving across borders more plausible. In other words, regional cybercrime task forces could pool resources so that smaller nations benefit from the capabilities of larger or better-resourced countries.

Finally, there needs to be a move towards international cooperation with more formal online cooperative structures. This could be joint task forces or cybercrime command centres, where agencies from countries act on active cases jointly, share data in real-time, and assign resources based on the expertise required at any particular instance.

5.4.3 Improving the Use of Emerging Technologies

Artificial Intelligence and machine learning have shown promising results in law enforcement, especially regarding fighting cybercrimes related to phishing, identity theft, and financial fraud. AI allows automation of data analysis tasks and, therefore, gives law

enforcement agencies faster identification of criminal patterns, which is highly needed when considering the volume of cybercrime data. AI-powered systems find patterns in data streams, identify anomalies, monitor attempts at phishing, and track financial fraud activities, which speed up investigations by 25% of the usual time needed.

Machine learning amplifies this with predictive insight into past crime data. These ML models make it possible to identify potential future threats by looking backwards at the behaviors of past cybercriminals and informing law enforcement agencies of proactive cybersecurity measures against crimes in the cyber world. In the jurisdictions where the ML models had been implemented in their entirety, fraud detection rates increased by 30%, thus showing potential for these emerging technologies in the fight to prevent cybercrime.

Despite such progress, resource allocation and training still need to be addressed. Most law enforcement agencies, particularly those in less well-resourced regions, need more budgetary and personnel constraints when incorporating AI and ML into their operations. Increased investment in training is thus required, supplemented by international cooperation. Furthermore, there is a need to share knowledge and technological resources across borders in many ways so that all agencies benefit from the various advancements in AI and machine learning.

5.5 Limitations of the Study

This research encountered several limitations, necessitating the implementation of precautionary measures. The secondary data sources primarily relied on reports from law enforcement, data from cybersecurity organizations, and the availability of publicly sourced datasets like Kaggle. Such a dependence poses various challenges, including issues of relevance and timeliness. For example, it is impossible to satisfactorily represent the relevant trends of e-crime or the most recent technological tools used by law enforcement agencies. Further, partial incompleteness in some datasets could limit the depth of analysis.

Some limitations exist when using quantitative data to measure the success rate of law enforcement. Traditional quantitative data on arrests, prosecutions, and case closures did not provide qualitative information about the agency's long-term operational challenges or specific challenges in those cases, which served as litmus tests for intricate investigations. These are

critical perspectives for any objective assessment of approaches; they are consistently hard to measure.

Finally, data generalization poses a challenge to the research, particularly in the context of cross-border cooperation. This cannot be the situation in all jurisdictions because legal frameworks and law enforcement capabilities vary from country to country. Some countries are more advanced regarding resources or have better international relations, which gives them an advantage. Sometimes, jurisdictional or financial issues prevent them from moving forward. This leads to variance, making it challenging to generalize the results in different settings and where there is a different legal environment and technological advancement (Uzunca et al., 2018).

5.6 Areas for Future Research

This research has shed light on the policing of e-crimes and the strategies employed to combat them; however, further research on specific aspects remains necessary. The police need more longitudinal studies to show how effective some of these strategies are over time. Since cybercriminals' strategies change with each passing day, evaluating the impact of a specific approach, like digital forensics or international cooperation, fully exposes the approach's benefits over time. For example, this will assist researchers in assessing law enforcement agencies' ability to adapt to new threats and the constant use of various techniques due to the growing complexity of cybercriminals' tactics.

The study calls for more empirical research on the effects of new technologies (AI, blockchain, machine learning) on e-crime investigations. Future studies should focus on real-world examples in various legal and socioeconomic environments to identify factors influencing technology adoption and success, especially in resource-poor countries. These studies can help in scaling up the global implementation of these technologies for better results.

The study identified jurisdictional barriers in cross-border investigations of transnational crimes. Future research should focus on developing effective solutions for legal harmonization and promoting international cooperation. This includes highlighting best practices in investigative cybercrime cases and recommending ways to create an enabling legal framework for increased and more effective cooperation between countries.

CHAPTER SIX: CONCLUSION AND RECOMMENDATIONS

6.1 Summary of Key Findings

6.1.1 Effectiveness of Law Enforcement Strategies

The research showed that the strategies employed in law enforcement in different applications and approaches had differing effectiveness in the fight against e-crime. This demonstrated that the tool's effectiveness was most pronounced in identity theft and financial fraud cases, requiring detailed digital data analysis to identify the perpetrator. Agencies that used ICT-based approaches, such as cybersecurity tools and data analytics, also had great success in dealing with phishing and hacking crimes. However, cases where international cooperation plays a central role, such as addressing transnational e-crimes like business email compromise and investment fraud, record the highest success rates. Cross-border collaboration allowed agencies to share resources and intelligence and coordinate operations, resulting in more successful outcomes.

These findings are consistent with the existing literature on the need for integrated approaches in combating cybercrime. Previous studies have shown that individualistic ICTs often only succeed if joint mechanisms for sharing data and cooperation on an international level exist. The present study supports this view by establishing that international cooperation and investigations based on collaboration in wrongdoing remain the only way to address this challenge on a global scale in cases that may be susceptible to variations in jurisdiction.

6.1.2 Challenges Faced by Law Enforcement Agencies

According to the study, several challenges emerged that undermine the efficiency of law enforcement agencies. One of the significant challenges was jurisdictional barriers, especially in transnational e-crime cases where there are differences in laws from one country to the other that interfere with the efficiency of the investigations. Because there were no standard international legal systems, enforcement agencies faced many challenges, including extradition affairs.

The constraints of technology were another significant limitation. Most agencies, particularly in less well-resourced parts of the world, have not benefited much from the

advantage that emerging technologies like AI and blockchain have given investigations into cybercrime. The study showed that the more technologically enabled agencies tend to enjoy higher success rates. In contrast, less technologically empowered agencies struggle to cope with cybercriminals' levels of sophistication. This resource disparity translated into a significant gap in effectiveness between wealthy and less well-resourced nations (Fujimoto et al., 2023). Many of these challenges were overcome with the help of cooperation at the international level. Another interesting observation at the different stages of operations was that the higher rate was reasonably expected when agencies cooperated across the borders. This study also highlighted that a more rigid and systematized form of cooperation would improve cross-border operations, particularly in exchanging information and synchronizing laws.

6.1.3 Role of Emerging Technologies

E-crime has significantly impacted Mauritian law enforcement agencies, particularly with emerging technologies like artificial intelligence, blockchain, and machine learning. AI differentiated itself by automating the metrics needed for big data; it enables agencies to rapidly determine otherwise unseen patterns of criminality, such as identity theft and phishing. Blockchain technology has become increasingly critical for monitoring decentralized financial transactions, making it suitable for fraud-related scenarios. Using historical data, machine learning tools help agencies determine criminal risks and prevent future attacks. However, their adoption is still restricted to many agencies, especially in areas lacking more resources. The research also found that most agencies could not pay for the tool because of a lack of finance, capacity, and facilities for this kind of tool. What aggravated the situation was that most agencies needed a training program to help them use these tools, not to mention knowledge sharing of best practices at the international level. This implies that most agencies have not developed strategies to counter advanced cyber threats (Wilner et al., 2022). The findings indicate a need to invest more in emerging technologies and provide comprehensive training programs, which would help law enforcement agencies worldwide fully exploit these tools in combat and investigation against e-crime.

6.2 Implications for Law Enforcement

6.2.1 Jurisdictional Cooperation

The essence of improving jurisdictional cooperation between nations is critical in effectively combating transnational e-crimes. Most cybercriminals operate across many countries, exploiting the legal gaps between jurisdictions. In this regard, nations must work together to develop global frameworks of legal harmonization that standardize cybercrime laws and enhance prudent cross-border cooperation. Legal harmonization will expedite extradition and other investigative processes across borders, significantly reducing the response time of law enforcement agencies to e-crimes. A uniform legal regime would further enable data-sharing arrangements among various agencies, allowing for the quick and efficient exchange of critical information and improving operational responses across borders.

6.2.2 Technological Integration

Technology integration within a law enforcement agency becomes critical in light of these emerging cyber threats. Advanced tools, in which AI, blockchain, and machine learning have become essential and pivotal for contemporary cybercrime investigation, are beyond the reach of many agencies, especially those in under-resourced regions (Haque et al., 2023). Public-private partnerships can bridge the gap to a certain extent. By partnering with technology companies, law enforcement agencies can access cutting-edge tools and expertise that would otherwise be unavailable.

It is crucial to develop training on the subject matter to guarantee successful implementation by law enforcement authorities in real-world scenarios. Training may include initiatives such as inter-country knowledge sharing, in which nations or agencies that are more developed equip and assist counterparts in areas that do not have the required infrastructure level. Such programs would equip law enforcers with skills and knowledge in handling increasingly complex cybercrime cases.

6.2.3 International Partnerships

The global scale of the e-crimes calls for greater international cooperation. Establishing joint task forces and cybercrime command centers is essential to ensuring real-time international cooperation. It leads to quicker responses and better coordination with investigations. These partnerships would provide agencies with shared resources, intelligence sharing, and joint operations, resulting in effective outcomes for cross-border cases.

Another critical component of successful international collaborations is the data-sharing protocol optimization process. More importantly, clearly defined standardized procedures for information sharing eliminate unnecessary delays and ensure timely communications. On the contrary, mechanisms like joint operation centers or even task forces on cybercrimes could also smoothen international collaboration by allowing law enforcement to share intelligence and conduct operations much less hassle-free. The necessary mechanisms for ensuring such collaboration are provided below.

6.3 Policy Recommendations

6.3.1 Global Legal Frameworks

There is a need to develop uniform international legal mechanisms for effectively combating these transnational e-crimes. The goal of such a framework should be to bring harmony to countries' cybercrime laws so that all countries investigate and prosecute cybercrimes similarly. One of the most basic features that any such framework needs to zero in on involves charting streamlined processes for extradition, which would eliminate delay and other impediments due to disparate legal systems. Harmonizing laws would enable law enforcement agencies to collaborate across borders and guarantee the prosecution of cybercriminals, regardless of their operating location. The governments emphasize international agreements facilitating cross-border investigations, allowing faster and more efficient action against e-crime (Depauw, 2018).

6.3.2 Technology Funding and Resource Allocation

Governments must be willing to invest more in sophisticated technological tools such as AI, blockchain, and digital forensics. Law enforcement agencies require these facilities to stay ahead of cybercriminals and investigate increasingly sophisticated e-crimes. In addition to technology investment, policies must ensure fair resource distribution across regions, targeting under-resourced agencies lacking the infrastructure to deal with sophisticated cyber threats. Global cybersecurity efforts need all the agencies involved, whatever their level of funding, to have equal opportunities and use the most recent tools to discharge duties. Governments must make such funds available to enable developing nations to purchase the necessary technologies and ensure adequate personnel training (Almeshqab and Ustun, 2019).

6.3.3 International Cybersecurity Task Forces

The potential for increasing combat readiness against e-crime be explored by creating regional and international cyber security task groups. These forces would allow countries to build up cyber police to prevent and fight cybercrime while encouraging international cooperation. Similar to Simola (2019), we will significantly improve global cybersecurity by implementing the following measures: The first step will involve forming agreements for information sharing across countries and enhancing current communication systems for data exchange. Through improved intelligence cooperation, police forces worldwide may better coordinate their fight against cyber criminals and respond as one to new threats.

6.4 Future Directions for Research

6.4.1 Longitudinal Studies on Law Enforcement Strategies

Longer-term research on law enforcement techniques' effectiveness across regions is needed. The benefits of such a study would be immense, highlighting how these various strategies have adapted to the ever-changing nature of cyber threats and, as such, helping both the researcher and policymaker understand which tactics remain helpful in the face of cybercriminals' technological advances to circumvent them. These studies would identify patterns in the strategies' effectiveness, highlight areas for improvement, and offer a prospective

future. This would allow law enforcement agencies to fine-tune their strategies and make the necessary resource allocation and policy development decisions.

6.4.2 Research on Emerging Technologies

Further research is needed to understand how emerging technologies like AI, blockchain, and machine learning will finally affect e-crime investigations, particularly in under-resourced regions. These can completely revolutionize cybercrime detection, prevention, and prosecution, but the pace of adopting artificial intelligence technologies differs worldwide. Researchers should conduct case studies that involve scaling and integrating these tools into diverse socio-economic contexts within law enforcement efforts. Research on the various adoption barriers and their potential solutions is also necessary to ensure that the benefits of technological advancements in crime prevention reach all regions.

6.4.3 Studies on Global Legal Harmonization

Global legal harmonization beyond simple cooperation is another area that requires extensively focused research to improve cross-border investigations. For example, investigations need to determine how standardized international legal frameworks can help ensure frictionless collaboration of law enforcement agencies in transnational cybercrime cases. Researchers should point out the presiding legal limitations and provide actionable recommendations on the best steps toward creating one concrete global form of cybercrime legislation. It also considers the best practices for legal harmonization, which would go a long way in making nations share resources and experience in combating cybercrime.

6.5 Final Conclusion

The present study's findings have highlighted the role of law enforcement strategies and emerging technologies as countermeasures to the growing threat of e-crime. In particular, different approaches, such as digital forensics, ICT, and international cooperation, proved efficient for different cybercrimes. AI, blockchain, and machine learning further developed the investigation capabilities. These findings emphasize the need for law enforcement agencies to

massively adopt countermeasures against cyber criminals through rapidly changing means, underscoring technological investment and strategic international partnerships.

The study has enhanced our understanding of cybercrime prevention by highlighting law enforcement's significant challenges, such as jurisdictional barriers and resource disparities, and emphasizing the need for ongoing global cooperation in employing advanced tools to counter sophisticated cyber threats. The future of law enforcement in addressing transnational e-crimes will depend on how healthy nations collaborate in laying down standardized global legal frameworks. Indeed, it is only through such a collective effort, continuously developing new technologies and techniques, that law enforcement agencies can stay one step ahead of cybercriminals and create a much safer digital world for everyone.

References

1) Adisa, O. T., 2023. The impact of cybercrime and cybersecurity on Nigeria's national security. https://dspace.cuni.cz/handle/20.500.11956/187353

2) Adorjan, M., and Colaguori, C., 2023. Scams Fraud and Cybercrime in a Globalised Society. *Crime, Deviance, and Social Control in the 21st Century: A Justice and Rights Perspective*, *407*.

3) Akartuna, E. A., Johnson, S. D., and Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, *179*, 121632. https://www.sciencedirect.com/science/article/abs/pii/S0040162522001640

4) Alhajeri, M., 2022. *Developing a digital competence framework for UAE law enforcement agencies to enhance cyber security of Critical Physical Infrastructure (CPI)*. University of Salford (United Kingdom). https://www.proquest.com/openview/2f9462c90b68429cc3dc38815da07249/1?pq-origsite=gscholarandcbl=2026366anddiss=y

5) Apau, R., and Koranteng, F. N., 2019. Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. *International Journal of Cyber C Lis, P., and Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. Economics and Business Review, 5(2), 24-47. riminology*, *13*(2). https://intapi.sciendo.com/pdf/10.18559/ebr.2019.2.2

6) Azizah, S.Z., Asikin, Z. and Parman, L., 2021. Implementation of E-Commerce Crime Law Enforcement at the West Nusa Tenggara Regional Police. *International Journal of Multicultural and Multireligious Understanding*, *8*(2), pp.7-26.

7) Beim, D., and Rader, K., 2019. Legal Uniformity in American Courts. *Journal of Empirical Legal Studies*, *16*(3), 448-478. https://onlinelibrary.wiley.com/doi/full/10.1111/jels.12224

8) Bilodeau, M. D., 2019. *The risk that Cyber-attacks pose to Outer Space Assets: How can international dialogue and cooperation help?*. McGill University (Canada). https://www.proquest.com/openview/c60d1fdf6662908cd614e18e4e314f93/1?pq-origsite=gscholarandcbl=18750anddiss=y

9) Bruce, P., Bruce, A., and Gedeck, P., 2020. *Practical statistics for data scientists: 50+ essential concepts using R and Python*. O'Reilly Media.

10) Cascavilla, G., Tamburri, D. A., and Van Den Heuvel, W. J., 2021. Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers and Security*, *105*, 102258. https://www.sciencedirect.com/science/article/pii/S0167404821000821

11) Ch, R., Gadekallu, T. R., Abidi, M. H., and Al-Ahmari, A., 2020. Computational system to classify cyber crime offenses using machine learning. *Sustainability*, *12*(10), 4087. https://www.mdpi.com/2071-1050/12/10/4087

12) Cherniavskyi, S., Babanina, V., Vartyletska, I., and Mykytchyk, O., 2021. Peculiarities of the economic crimes committed with the use of information technologies. *European Journal of Sustainable Development*, *10*(1), 420-420. https://www.ojs.ecsdev.org/index.php/ejsd/article/view/1181

13) Correia, S. G., 2019. Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales. *Crime Science*, *8*(1), 1-12. https://link.springer.com/article/10.1186/s40163-019-0099-7

14) Das, S., 2020. *A risk-reduction-based incentivization model for human-centered multi-factor authentication*. Indiana University. https://www.proquest.com/openview/38faf90785cf47c997333c8a799e1e83/1?pq-origsite=gscholarandcbl=18750anddiss=y

15) Deeb-Swihart, J., Endert, A., and Bruckman, A., 2019, May. Understanding law enforcement strategies and needs for combating human trafficking. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-14). https://dl.acm.org/doi/abs/10.1145/3290605.3300561

16) Fainshmidt, S., Witt, M. A., Aguilera, R. V., and Verbeke, A., 2020. The contributions of qualitative comparative analysis (QCA) to international business research. *Journal of international business studies*, *51*, 455-466. https://link.springer.com/article/10.1057/s41267-020-00313-1

17) Goode, J., and Lumsden, K., 2018. The McDonaldisation of police–academic partnerships: organisational and cultural barriers encountered in moving from research on police to

research with police. *Policing and society*, *28*(1), 75-89. https://www.tandfonline.com/doi/abs/10.1080/10439463.2016.1147039

18) Hatam, M. A., 2024. *Crime Rate Analysis and E-Crime Prevention in Dubai Using Machine Learning* (Master's thesis, Rochester Institute of Technology). https://www.proquest.com/openview/2b6b5659b9b5c36d0378245f7e9e05a2/1?pq-origsite=gscholarandcbl=18750anddiss=y
19) Ho, H., Ko, R. and Mazerolle, L., 2022. Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused, systematic review. *Computers and Security*, *115*, p.102611. https://www.sciencedirect.com/science/article/pii/S0167404822000104
20) Ibrahim, H., 2022. A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3), 50-68. https://wjcm.uowasit.edu.iq/index.php/wjcm/article/view/48
21) Khan, A. A., 2024. Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, *13*(4), 44. https://www.mdpi.com/2075-471X/13/4/44
22) Leuprecht, C., Kölling, M., and Hataley, T. (Eds.)., 2019. *Public Security in Federal Polities*. University of Toronto Press.
23) Luong, H. T., Phan, H. D., Van Chu, D., Nguyen, V. Q., Le, K. T., and Hoang, L. T., 2019. Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement. *International Journal of Cyber Criminology*, *13*(2).
24) Lusthaus, J., 2018. *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.
25) Markopoulou, D., Papakonstantinou, V., and De Hert, P. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Review*, *35*(6), 105336.
26) Mifsud Bonnici, J. P., Tudorica, M., and Cannataci, J. A., 2018. The European legal framework on electronic evidence: complex and in need of reform. *Handling and Exchanging Electronic Evidence Across Europe*, 189-234. https://link.springer.com/chapter/10.1007/978-3-319-74872-6_11

27) Minnaar, A., 2020. 'Gone phishing': the cynical and opportunistic exploitation of the Coronavirus pandemic by cybercriminals. *Acta Criminologica: African Journal of Criminology and Victimology*, *33*(3), 28-53. https://journals.co.za/doi/abs/10.10520/ejc-crim-v33-n3-a3

28) Mphatheni, M. R., and Maluleke, W., 2022. Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(4), 384-396. https://www.ssbfnet.com/ojs/index.php/ijrbs/article/view/1714

29) Munton, J., and McLeod, J., 2023. *The Con: How Scams Work, why You're Vulnerable, and how to Protect Yourself*. Rowman and Littlefield.

30) Nicholls, J., Kuppa, A., and Le-Khac, N. A., 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, *9*, 163965-163986. https://ieeexplore.ieee.org/abstract/document/9642993

31) Ombu, A., 2023. Role of Digital Forensics in combating Financial crimes in the Computer era. *Journal of Forensic Accounting Profession*, *3*(1), pp.57-75.

32) Peters, A., and Jordan, A., 2019. Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *J. Nat'l Sec. L. and Pol'y*, *10*, 487. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jnatselp10anddiv=24andid=andpage=

33) Sarkar, G., and Shukla, S. K., 2023. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 100034. https://www.sciencedirect.com/science/article/pii/S2949791423000349

34) Sarre, R., 2021. Policing Cybercrime: Is There a Role for the Private Sector?. In *Police Behavior, Hiring, and Crime Fighting* (pp. 217-227). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003047117-18/policing-cybercrime-rick-sarre

35) Shane, J. M., Piza, E. L., and Silva, J. R. 2018. Piracy for ransom: The implications for situational crime prevention. *Security Journal*, *31*, 548-569. https://link.springer.com/article/10.1057/s41284-017-0115-0

36) Shjarback, J. A., and Todak, N., 2019. The prevalence of female representation in supervisory and management positions in American law enforcement: An examination of organizational correlates. *Women and Criminal Justice*, *29*(3), 129-147. https://www.tandfonline.com/doi/abs/10.1080/08974454.2018.1520674

37) Sibe, R.T. and Kaunert, C., 2024. Cyber Crime in Nigeria—Reviewing the Problems. In *Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria* (pp. 19-55). Cham: Springer Nature Switzerland.

38) Sutton, M. 2018. Routine activity theory: "Mindless" chemistry meme masquerades as a theory of crime causation. *Internet Journal of Criminology*, 1-34. https://www.shortcutstv.com/wp-content/uploads/2020/03/rat.pdf

39) Tikkinen-Piri, C., Rohunen, A., and Markkula, J., 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, *34*(1), 134-153. https://www.sciencedirect.com/science/article/abs/pii/S0267364917301966

40) Uricska, E., 2020. Proper interactive communication of the police as a (n e-) trust-building strategy. Introducing the term policing digilect. *Košická Bezpečnostná Revue*, *10*(2), 185-195. https://real.mtak.hu/118594/1/uricska.pdf

41) Vartanian, T. P., 2023. *The unhackable internet: How rebuilding cyberspace can create real security and prevent financial collapse*. Rowman and Littlefield.

42) Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... and Platts, J., 2022. Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), 127. https://link.springer.com/article/10.1007/s42979-022-01020-4

43) Bao, Y., Hilary, G. and Ke, B., 2022. Artificial intelligence and fraud detection. *Innovative Technology at the Interface of Finance and Operations: Volume I*, pp.223-247.

44) Lokanan, M.E. and Maddhesia, V., 2024. Supply chain fraud prediction with machine learning and artificial intelligence. *International Journal of Production Research*, pp.1-28.

45) Oatley, G.C., 2022. Themes in data mining, big data, and crime analytics. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *12*(2), p.e1432.