[THE IMPACT OF CYBERCRIME AND CYBERSECURITY ON NIGERIA'S NATIONAL SECURITY]

[AUGUST 2023]

[2701698A]

[21108919]

[33405990]

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 22,182

Supervisor: David Erkomashvili

Date of Submission: August 25th 2023

ACKNOWLEDGEMENT

I am deeply grateful to the many individuals who have supported me throughout my journey to completing this thesis. Their unwavering encouragement, guidance, and presence have been instrumental in helping me reach this milestone.

First and foremost, I extend my heartfelt gratitude to God Almighty, whose blessings and grace have given me the strength and perseverance to overcome challenges and pursue my academic goals.

To my parents, the pillar of strength in my life, I am profoundly indebted for their unending support. Your unwavering belief in me, both financially and morally, has been a driving force behind my accomplishments. Your advice, encouragement, and constant push have been the guiding light that led me through the intricacies of this endeavour.

I am also indebted to my husband, whose unwavering belief in my abilities and dedication to our family allowed me to focus on my studies. His relentless support, whether providing a listening ear, taking care of our children, or offering his unwavering encouragement, has been an essential cornerstone of my success.

I sincerely appreciate my siblings, who have been my constant cheerleaders. Their continuous presence, encouragement, and check-ins reminded me that I was never alone in this journey.

I am grateful to my supervisor (Dr. David Erkomashvili) for his invaluable guidance, expertise, and patience throughout the research process. His insightful feedback significantly contributed to the quality of this work.

Lastly, I thank all my friends and well-wishers who supported me with their words of encouragement and positive energy. Thank you all for being part of this significant journey.

ABSTRACT

The rapid digitisation of the last decade has transformed global interconnectedness but has concurrently birthed challenges like cybercrime. This research delved into Nigeria's cybercrime landscape, focusing on its implications for national security. With the rise of cybercrime leading to economic losses of billions, the study aimed to pinpoint sociological and technological drivers, such as unemployment and digital growth, contributing to the menace. Cybercriminal subcultures, like the "Yahoo Boys", have emerged, depicting a societal trust deficit and cultural inclinations towards cyber malfeasance. The research also assessed Nigeria's cybersecurity measures, including the Cybercrime Act 2015. While the Act signifies the nation's resolve, gaps in its enforcement diminish its effectiveness. Moreover, central to Nigeria's digital aspirations, small and medium enterprises emerge as especially vulnerable to cyber threats. As the country grapples with this dual challenge of digital growth and cyber vulnerabilities, a multifaceted strategy involving legislation, technology, public engagement, and global collaboration is pivotal. The study underscores the urgency for a collective response involving policymakers, businesses, and citizens to ensure a secure digital future for Nigeria. The findings contribute to the broader discourse on cybercrime in Nigeria, laying a foundation for future academic pursuits and policy interventions to counteract emerging cyber threats.

TABLE OF CONTENTS

INTRODUCTION

1.1. Background

In the last decade, the world has rapidly transformed into a global community, mainly attributable to the advancements in technical infrastructure, particularly the Internet. Integrating the Internet and technology into every aspect of human life has facilitated seamless communication, information sharing, and business transactions across geographical boundaries, resulting in heightened interconnectedness and interdependence among individuals and communities worldwide (Alao, Osah and Eteete, 2019). However, the technological development's wide acceptance and use have paved the way for new security challenges, such as cybercrime (also known as e-crime). Cybercrime involves using digital technology to commit illegal activities, such as hacking, identity theft, online fraud, and malware distribution, to gain unauthorised access, steal sensitive information, or cause damage to computer systems and networks or individuals (Osho and Onoja, 2015). The past years have witnessed a sophisticated and unprecedented growth in the number of individuals who utilise the internet for illegal activities, with perpetrators resorting to advanced methods such as using computer systems to commit fraud, terrorism, and other criminal activities without leaving their current geographical territory. This level of sophistication and continuous rise has evoked admiration and terror among individuals, organisations, and governments globally, resulting in a growing concern about personal and cyber security (Yakubu, 2017). In addition, the continuous rise in cybercrime poses a formidable threat to humankind and nation-states' infrastructure, making cybersecurity an unrelenting challenge. In response to these, countries are making serious efforts to safeguard their cyberspace from cyberattacks and cybercrimes, given the potential threats and vulnerabilities that could lead to significant financial losses, property damages, cash theft, and the

collapse of critical national infrastructures (Fischer, 2009; Babayo et al., 2021). The impact of cybercrime is felt globally, affecting individuals, organisations, companies, and governments with massive financial losses estimated in billions of dollars.

Within this context, Nigeria is a developing nation with a population of over 200 million people and the most populous country in Africa. The country is known for its rich natural resources and diverse culture (Sule et al., 2021). Still, it faces threats to national security on numerous fronts, both traditional military threats and non-traditional challenges, such as poverty, corruption, insecurity, diseases, erosion, terrorism, kidnapping, armed robbery, and the explosion of cybercrime both within and outside its borders (Yusuf, 2014). National security has been a significant concern for the Nigerian government for many years, particularly in ensuring its citizens' safety and maintaining stability. Recently, Cybercrime has emerged as a growing threat to national security in Nigeria. As acknowledged in Nigeria's National Cybersecurity Policy and Strategy (NCPS) 2024, the government is cognizant of the burgeoning threat posed by cybercrime to the nation's security, economy, and international reputation. The policy provides strategic guidance for securing the country's cyberspace and presents a vision to enhance the national cybersecurity ecosystem. This recognition and commitment to strengthening cyber resilience further underline the criticality of cybercrime within Nigeria's national security dialogue."

As the country becomes more digitally connected, the rise of cybercrime continues to gain prominence, with an estimated annual loss of billions of dollars attributed to these criminal activities. Several factors contribute to the widespread of these crimes in Nigeria, such as unemployment, poverty, and other socio-economic factors (Idowu, 2021). Hence, the prevalence of these criminal activities among Nigerian youths. Nigeria currently ranks first among the top 10 countries notable

for Internet fraud and seventh among the top 10 Internet users worldwide (Federal Bureau of Investigation, 2022). The Impact cybercrime has on Nigeria's national security is multifaceted, including economic destruction, loss of sensitive data, damage to the reputation of businesses, and undermining of the nation's critical infrastructure vital instrumentalities (Sule et al., 2021). In addition to these impacts is the lousy image cybercrime has created for Nigerians living in the diaspora. Moreover, the increasing number of cyber-related crime reports from Nigeria's Economic and Financial Crimes Commission (EFCC) is becoming alarming. As a result, it is imperative to prioritise cybersecurity measures to safeguard cyberspace.

Cybersecurity refers to the measures to protect digital devices, networks, and sensitive information from unauthorised access and against cybercrime and other digital threats (Frank and Odunayo, 2013). Cybersecurity also encompasses promoting safe online practices and raising awareness of cyber threats to individuals, organisations, and governments. Hence, Recognising the threat e-crimes pose to national security and to eradicate it, the Nigerian government has made several attempts to curb the phenomenon in the society, including the enactment of laws such as the comprehensive cybersecurity policy document adopted in 2015, which outlines the government's provisions and efforts to establish a safer digital environment. In addition, is the National Information Technology Development Agency (NITDA) established in 2015 to regulate and develop the country's information technology sector. NITDA has since developed cybersecurity guidelines and policies for government agencies and organisations in Nigeria to follow. The law also establishes a National Cybersecurity Fund to finance the country's cybersecurity efforts. Despite the laws and establishments aimed at curbing cybercrime in Nigeria, the country still faces cybersecurity challenges, including inadequate cybersecurity infrastructure, lack of awareness and education about cybersecurity, and the prevalence of cybercrime that still poses a significant

challenge. It is on this premise that this work examines the impact cybercrime has on Nigeria's national security and the country's current cybersecurity state.

1.2. Statement of the Problem

The Internet offers boundless opportunities for various human activities, including commerce and social interactions. However, the Internet also presents its unique risks in the form of cybercrime. Cybercrime has become a pervasive problem threatening Nigeria's national security and posing a menace that demands immediate attention. The vulnerabilities in Nigeria's digital infrastructure make it a prime target for cybercriminals who exploit these weaknesses to commit crimes such as identity theft, fraud, and cyber espionage. Effective cybersecurity measures are essential for safeguarding Nigeria's digital assets and infrastructure and protecting its citizens' privacy and security. Therefore, it is crucial to examine the menace that cybercrime and cybersecurity threats pose to Nigeria and take appropriate measures to combat them.

1.3. Research Question

How have Cybercriminal activities influenced Nigeria's national security?

Sub-question

a. What are the sociological and technological factors contributing to cybercrime in Nigeria?
b. What are Nigeria's current cybersecurity measures and policies, and how effectively are they combating cybercrime?

1.4. Aims and Objectives

This dissertation examines the current state of cybercrime and the types and characteristics of cybercrime in Nigeria. It aims to identify the sociological and technological factors contributing to cybercrime in the country. It also aims to

Identify the main challenges and obstacles to improving cybersecurity in Nigeria. The thesis also aims to raise public awareness of the risks and threats associated with cybercrime and the need for proactive measures to safeguard Nigeria's digital infrastructure and protect its citizens' privacy and security. Specifically, it sets out to:

1. Explore cybercriminal activities' influence on Nigeria's national security.
2. To evaluate Nigeria's cybersecurity measures and policies and assess their effectiveness in combating cybercrime.

1.5. Relevance of the Work to the Academic Field

The thesis intends to contribute to the existing knowledge on cybercrime and cybersecurity in Nigeria and provide policy recommendations for the Nigerian government and stakeholders to enhance the country's cybersecurity posture and combat cybercrime effectively.

Overall, "The Impact of Cybercrime and Cybersecurity on Nigeria's national security" is relevant to the academic field as it provides a comprehensive analysis of cybercrime and cybersecurity in Nigeria and offers insights and recommendations for enhancing cybersecurity and combating cybercrime.

1.6. Scope and Limitations of the Study

This thesis will examine the impact of cybercrime and cybersecurity on Nigeria's national security. The work will cover various aspects of cybercrime, including the current state of cybercrime in Nigeria, the economic, social, and political impact of cybercrime on Nigeria's national security, the effectiveness of current cybersecurity measures, the challenges encountered by the Nigerian government in eradicating cybercrime, and strategies for improving Nigeria's cybersecurity and combating cybercrime in the country. However, it is essential to note that the work will only

cover cybercrime attacks on individuals, companies and the government, and it will not focus on cyber warfare, which has to do with an attack against an enemy state military network vital infrastructures rely on computer networks via cyberspace. Hence, the work will focus on specific areas relevant to the research question and objectives.

The data collection will be centred on the country's cybercrime cases. In chapter three of this thesis, questions regarding the data sources, documents, selection process, and methods of analysis used to answer the core question and objective are discussed at length. The work will cover the period from 2015 to 2022, and the findings will be used to make recommendations for improving cybersecurity and combating cybercrime in Nigeria.

1.7. Organisation of Work

The dissertation is organised into six chapters. The first chapter introduces the research problem, questions, aims and objectives, academic relevance, scope, and work organisation. The second chapter reviews relevant literature and establishes the theory. Chapter three outlines the methodology employed in the work. Chapter four provides empirical findings and a discussion on the impact of cybercrime on Nigeria's national security. Chapter five concludes the dissertation. Finally, the work ends with a reference section.

CHAPTER TWO – LITERATURE REVIEW AND THEORETICAL FRAMEWORK

PART I – REVIEW OF LITERATURE

2.1. CYBERSECURITY

The emergence of cybersecurity as a central global concern due to the increasing reliance on digital technology daily has been gaining traction in recent years. The growth of technology, the internet, and the widespread adoption of storing a vast amount of data on computers and other devices, as well as data sharing, has provided new opportunities for innovation, collaboration, and communication across all industries. Moreover, a significant portion of this data can be considered sensitive information, such as intellectual property, economic data, personal information, or other types of data that can have severe consequences if accessed or exposed without authorisation (Singh, 2021). However, despite this technological advancement's uncontending benefits, they have also introduced new cyber threats and vulnerabilities (Rayes and Salam, 2019). These cyber threats are becoming more frequent, sophisticated, and costly, posing significant threats to individuals, organisations, and countries. As such, it has become increasingly important for organisations and nations to protect their systems from malicious actors who could compromise sensitive information or disrupt operations.

Cybersecurity's primary objective is to ensure the safety of operations in cyberspace from cyber threats (Dewar, 2014). Makeri (2017) defined cybersecurity as the security of networks and interconnectedness systems, such as hardware, software, and data, from cyber threats to minimise the impact of potential attackers in disrupting normal operations and is practised by both organisations and individuals. Similarly, Chapple (2020) defines cybersecurity as protecting electronic systems, data networks, servers and sensitive information from theft, damage, or

unauthorised access. These definitions provide a restricted sociotechnical perspective on cybersecurity by presenting a fundamental grasp of the concept and an elementary discussion of the multidisciplinary aspects of system integrity. The motives of prospective cyber-attacks are not explicitly mentioned, and a limited list of the protected elements is provided.

According to Abomhara and Koien (2015), cybersecurity encompasses a collection of best practices ensuring a computer system's integrity, including infrastructure modifications. This concept involves protecting vital installations and sensitive data from future digital threats, with measures designed to counteract threats posed by malicious attackers on an organisation's networks and applications from outside or within (Schiliro, 2023). Also, Odumesi (2006) "identified some activities that define cybersecurity as the confidentiality of information, the integrity of systems, and the survivability of networks" (Oyelere et al., 2015). However, cybersecurity encompasses more than technical problems, information security or data security. It has become an expanding field with issues where society and its core values are threatened due to the dependence on information and communication technology (ICT), and action taken to combat this threat is aimed at various levels, including technical, legislative, organisational, and international in which the primary actors are both the security specialist and the government (Odumesi, 2014).

However, For this thesis, the definition of cybersecurity as per the International Telecommunications Union (ITU) is employed primarily because of its comprehensive approach towards cybersecurity. Unlike many definitions, the ITU's definition does not restrict cybersecurity to technical aspects but also encompasses management, procedural, and policy aspects. This is crucial in providing a well-rounded understanding of cybersecurity, considering that non-technical elements often play a critical role in cybersecurity strategies. According to the ITU (2004), cybersecurity encompasses a wide range of features that can be employed to protect

the cyber environment and a company's and user's assets. These elements include resources, procedures, security principles, safety protocols, regulations, risk management strategies, activities, training, best practices, compliance, and technology. The assets in question consist of connected computing devices, personnel, equipment, software, utilities, telecommunications networks, and all data exchanged and processed in the cyber environment (Goel, 2019). In other words, cyber security is the collection and coordination of various resources, such as personnel and infrastructure, and the establishment of structures and processes to secure networks and cyber-enabled computer systems against threats that could jeopardise their integrity and infringe upon property rights, resulting in varying degrees of loss (Schiliro, 2023). This definition explored the intricate nature of cybersecurity and its critical components by examining various interrelated perspectives and dimensions. It also recognises the socio-technical interactions between humans and systems as well as among networks and considers strategies for safeguarding systems against a wide range of threats.

2.1.1 CYBERSECURITY POLICIES AND FRAMEWORK IN NIGERIA

In contemporary times, businesses, establishments, projects, organisations, and nations are increasingly implementing and governed by policies and strategies that apply to all aspects of their operations. These policies and strategies serve as developmental frameworks and plans typically designed by critical policymakers, governments, and organisations, which are meant to be strictly followed regardless of immediate or impending situations as they are developed for this specific purpose (Osho and Onoja, 2015). Furthermore, with cyber security becoming increasingly important worldwide, policymakers, governments, and stakeholders are creating guiding principles through policies and strategies that outline the steps to be taken during a cyber-attack and provide guidelines for preventing future assaults

(Awhefeada and Bernice, 2020). Implementing these strategies or policies is essential because it enables organisations, individuals, and governments to secure their critical assets and sensitive data from cyber threats, which can result in financial loss, reputational damage, and legal liabilities in today's digital world. Additionally, a well-designed cyber security policy and strategy can foster international cooperation among countries in areas of security and development.

The Office of the Nigerian National Security Adviser (2014) defined the National Cyber Security Strategy (NCSS) "as a road map that seeks to provide cohesive measures and strategic actions for stakeholders to ensure a safe, secure and resilient of the country's presence in cyberspace, building and nurturing trusted cyber-community" (Osho and Onoja, 2015). With the rise of cyber threats such as malware, phishing, ransomware, and other malicious activity targeting Nigerian citizens and businesses alike, a firm cybersecurity policy must be implemented to protect individuals and organisations from potential harm. Nigeria has several cybersecurity policies and frameworks that guide its efforts to combat the growing cyber-attacks in the country. These policies and frameworks aim to create secure cyberspace in Nigeria, protect critical information infrastructure, and promote cybersecurity awareness.

Before 2015, Nigeria did not have dedicated legislation on cybercrime; instead, existing laws whose provisions were deemed relevant to preventing cyber-related crimes were utilised by law enforcement agencies (Awhefeada and Bernice, 2020). Presently, Cybercrime (Prohibition, Prevention, etc.) Act of 2015 is Nigeria's primary legislation governing cybercrime, making the country more legally equipped to combat cybercrime. Although, before the implementation of this Act, other legislation existed to address cybercrimes (Adeniyi, 2021). As a result, it is essential to acknowledge the enabling laws to address cybercrime before enacting the 2015 Cybercrime Act.

The Economic and Financial Crimes Commission (Establishment) Act of 2004 established the Economic and Financial Crimes Commission (EFCC), which is an agency tasked with investigating and prosecuting economic and financial crimes, which includes advance fee fraud (commonly known as 419), computer credit card fraud, illegal charge transfers, contract scam, fraudulent encashment of negotiable instruments, among others (Adeniyi, 2021). The EFCC has played a crucial role in Nigeria's fight against cybercrime by investigating and prosecuting cybercriminals.

The Advanced Fee Fraud and Other Related Offences Act of 2006 criminalises various forms of fraud, including advance fee fraud (commonly known as 419), a prevalent form of cybercrime in Nigeria. The act makes it an offence to commit fraud by false pretence. The act also stipulates that inducing another person to confer a benefit under the front that the benefit will be paid for is also an offence (Adeniyi, 2021). The Act criminalises financial transactions that involve proceeds from unlawful activities (Awhefeada and Bernice, 2020). These provisions in the Advanced Fee Fraud and Other Related Offences Act serve as legal measures to prevent and prosecute fraudulent activities, including those carried out electronically in Nigeria.

Additionally, the National Identity Management Commission Act 2007 established the National Identity Management Commission (NIMC), responsible for maintaining a national database of citizens' biometric data. This database is essential for combating cybercrime, particularly crimes involving identity theft, as it identifies and tracks cyber criminals. Despite the existence of the National Identity Management Commission (NIMC) Act, its provisions may not be entirely effective in prosecuting cybercriminals. Cybercriminals can evade detection by falsely claiming they have lost their National Identity cards or using modern photographic techniques to alter their appearance. Such tactics enable them to

conceal their true identity and avoid being caught, thus rendering the provisions of the NIMC Act insufficient in combating cybercrime in Nigeria.

The Money Laundering (Prohibition) Act of 2011, as amended in 2013, provides a legal framework for combating money laundering, which is often associated with cybercrime. This Act obligates financial institutions to establish internal control mechanisms to prevent money laundering. Also, the Act prohibits various activities related to the handling of funds or property obtained through unlawful means, which can include cybercrime. However, the Act has received criticism for not establishing an agency specifically for enforcing its provisions, with enforcement instead falling to the Economic and Financial Crimes Commission (EFCC). This lack of dedicated enforcement may explain why the pace of prosecutions related to money laundering in Nigeria has been slow.

The Criminal Code Act and the Penal Code Act contain provisions that criminalise cyber-related offences such as unauthorised access to computer systems, cyber stalking, and identity theft. The two acts are essential pieces of legislation in Nigeria that contain provisions relevant to prosecuting cybercrimes. The Criminal Code Act defines various crimes, including offences related to fraud, theft, and forgery. These offences can be applied to cybercrimes, such as computer-related fraud, hacking, and identity theft. For example, Section 419 of the Criminal Code Act criminalises obtaining property by false pretences, which can include cyber fraud. The Penal Code Act applies to the northern states of Nigeria and contains similar provisions for criminal offences. It includes provisions that can be used for cybercrimes, such as fraud and forgery. For example, Section 320 of the Penal Code Act criminalises cheating and dishonestly inducing the delivery of property, which can include cyber scams and phishing.

Cybercrime (Prohibition, Prevention, etc.) Act of 2015 is the primary legislation governing cybercrime in Nigeria. This Act provides provisions for the prohibition,

prevention, detection, response, investigation, and prosecution of cybercrimes in Nigeria. The Act also establishes the National Cybersecurity Fund, which is a pool of resources to be utilised to implement the provisions of the Act. The Cybercrime Act of 2015 has significantly enhanced Nigeria's legal framework for combatting cybercrime by providing a comprehensive set of regulations for cyber activities, including the protection of critical national information infrastructure, the security of computer systems and networks, and the prosecution of cyber criminals (Adewumi, 2021). However, the act has received criticism for its reactive instead of proactive provisions. Another of its criticism is that it does not adequately protect the privacy of citizens. The act allows law enforcement agencies to intercept and monitor electronic communications under certain circumstances, such as when they have obtained a warrant from a court. However, critics argue that this provision is too broad and could lead to abuse by law enforcement agencies.

2.1.2 CYBERSECURITY IN NIGERIA

Cybersecurity in Nigeria is currently at a critical juncture due to the increasing prevalence and sophistication of cyber threats and the country's growing dependence on technology. Nigerian citizens and businesses are increasingly vulnerable to malicious attacks. With an estimated population of over 200 million, Nigeria has become one of the most prominent targets for cybercriminals (Sule et al., 2021). Cybersecurity threats such as malware, phishing scams, ransomware attacks, and data breaches are becoming increasingly common in this West African nation. While there have been some significant strides in cybersecurity awareness and capability in recent years, such as the establishment of the National Cybersecurity Policy and Strategy in 2014 and the Cybercrime Prohibition Act 2015, the reality is that Nigeria remains vulnerable to cyber-attacks.

Moreover, these cyber-attacks have been further exacerbated by the country's lack of comprehensive government regulations on cybersecurity and data protection and inadequate resources for enforcement agencies to respond adequately, making it difficult to prosecute cybercriminals (Adeniyi, 2021). Another major challenge is the country's lack of cybersecurity infrastructure and expertise. Many organisations in Nigeria do not have the resources or knowledge to implement robust cybersecurity measures, leaving them vulnerable to attacks (Garba and Bade, 2021). In addition, the lack of cybersecurity awareness among the general population in Nigeria has contributed significantly to the vulnerability of the country's cyberspace. Many Nigerians are unaware of the potential risks associated with their online activities and are, therefore, more likely to fall victim to cyber-attacks (Ibrahim, 2019).

2.2 CYBERCRIME

Due to its complex and constantly evolving nature, cybercrime can take various forms depending on the tactics and techniques employed by the offenders. As a result, multiple scholarly publications have previously sought to define cybercrime across different historical periods and under diverse conditions. Therefore, there is yet to be a generally accepted definition for the term. However, cybercrime can be defined as illegal activities committed via the Internet and other digital networks, devices, and technologies. It involves using computers, software, and online platforms to conduct illicit activities such as hacking, financial fraud, publishing of disapproved electronic information, breach of confidentiality, data interference, system interference, illegal interception, and identity theft., among others. Hence, cybercrime encompasses a range of offences in which computers play a significant role, including unauthorised access to private or company information, violation of network integrity, infringement of privacy, industrial espionage, and computer software piracy (Idowu, 2021).

According to Bernik (2014), cybercrime can be defined as unlawful activities conducted through electronic means that aim to target computer systems and data processed by the devices. The International Journal of Science and Information Security defines cybercrime as a malicious activity conducted from a computer or against a computer or network (Alghamdi, 2020). Similarly, cybercrime is described by Loader and Thomas (2000, p. 2) as computer-mediated acts that are deemed illegal or illicit by certain institutions and can be carried out across global electronic networks (Osho and Onoja, 2015). These definitions indicate that cybercrime occurs in a digital realm where information related to individuals, objects, events, or facts is expressed in mathematical symbols and transmitted across local and global networks. In addition, Halder and Jaishankar (2011) assert that cybercrime is a criminal act carried out to harm an individual or group of people with the primary objective of damaging the victims' reputations and causing irreparable harm to the hardware of sensitive infrastructure, including the internet and mobile phones (Goel, 2019). Odumesi (2014), in his research, provided a working definition of cybercrime, encompassing both the technological and sociological dimensions. Specifically, Odumesi defined cybercrime as a type of criminal activity that entails the misuse or abuse of digital resources within a cyber-environment, which can occur via the internet, computer networks, computer systems, and wireless communication devices.

Cybercrime may be perpetrated by individuals or groups using technical methods to manipulate the transmission of data to, from, or within a computer network to disrupt the operation of a computer system by the input, transfer, damage, or alteration of computer data. It can significantly impact individuals, businesses, or a nation by causing financial losses, compromising personal and sensitive information, disrupting critical infrastructure, and damaging national security.

These categories of criminal acts have been executed or made feasible through computer technology or traditional crimes that have been transformed by the use of computers, requiring law enforcement officials to understand computers to investigate and solve them (Adeniyi, 2021). Traditional crimes can be more easily combatted through physical measures involving detection, investigation, apprehension, and prosecution, adopting conventional methods requiring physical techniques. However, when these crimes are digitised, significant complications arise, which make finding solutions difficult or, in some cases, impossible to find (Osho and Onoja, 2015).

2.2.1 CYBERCRIME IN NIGERIA

Scholars have not identified the exact historical instance that gave rise to cybercrime in Nigeria. However, research indicates it gained popularity in the country in the early 2000s. The rapid and widespread growth of cybercrime has had significant consequences and impacts on Nigeria. This crime has become a severe issue for the country's individuals, businesses, and organisations. Nigeria is one of the African countries that experience hundreds of millions of cyberattacks annually (Mphatheni and Maluleke, 2022). For instance, in 2017, the country experienced a total loss of N198.6 billion, equivalent to $649 million (Adepetun, 2018), while in 2018, it was reported that the loss to cyberattacks in the country was $800 million (N288 billion) (Week, 2019). Similarly, in a 2019 report, cybercrime has cost Nigeria an average of N127 billion ($330 billion) (Ohwovoriole, 2019; Sule et al., 2021). More broadly, according to a report in 2022, Nigeria loses an average of N200 billion yearly to cybercrime (Onuoha, 2022). These data indicate the considerable effect of cybercrime on the economy of Nigeria. A cause for even more significant concern is a report that states that if cybercrime continues to be

unchecked or properly combatted, the country is projected to lose about $6 trillion by 2030 (Adeniyi, 2021). In Nigeria and other African countries, financial institutions, governments, and industries are the primary targets for hackers. Financial institutions in the country are particularly at a point where they incur losses daily due to continuous cyberattacks in insecure cyberspace. The frequency and intensity of these attacks are increasing, with hackers making more concerted efforts to breach security measures (Akinyetun, 2021).

Over the years, it has been evident that electronic crime is causing financial harm to the country and damaging Nigeria's reputation. This crime has become a source of national concern and has caused humiliation for the country. As a nation, Nigeria has been deemed immoral, with the infamous "419" scam (advance fee fraud) being traced back to the country (Adomi and Igun, 2008) and now gained notoriety worldwide. The "419" scam has been a problem in Nigeria for decades, as this is what Nigerian youth have resulted as a source of income due to the high unemployment rates, poor governance, inadequate educational system, and widespread poverty (Ogunjobi, 2020). This has led to a negative perception of Nigeria on the world stage and affected its economic growth, as potential investors may be deterred from investing in a country associated with such criminal activities. Some have even labelled the country a “financial terrorist nation” because of the history of financial crimes and illicit financial activities, such as money laundering, fraud, and corruption originating from the country (Ribadu, 2004). Hence, it has led to significant losses in revenue for the Nigerian government, as well as for other countries and businesses around the world. In addition, Nigeria has become the origin of financial crimes and other cyber-related crimes such as website cloning, hacking, phishing, viruses or worms, spamming, website cloning, cyber theft and so on (Adomi and Igun, 2008).

2.2.2 CAUSES OF CYBERCRIME IN NIGERIA

Cybercrime has become a global issue, and Nigeria is not an exception. It has been established that Nigeria, the largest economy in Africa, is one of the nations most afflicted by cybercrime. Thus, in the study of the causes of cybercrime in Nigeria, Hassan et al. (2012) contend that high unemployment, urbanisation, lack of awareness of cybersecurity, poverty, the proliferation of cybercafes, corruption and inadequate enforcement of existing laws against cyber criminals by law enforcement agencies coupled with weak judicial systems which do not deter potential offenders from engaging in illegal activities online are factors contributing to the proliferation of cybercrime in Nigeria.

Unemployment, coupled with poverty, is a major factor contributing to the prevalence of cybercrime in Nigeria. The problem of unemployment in Nigeria is complex and multifaceted. The formal job sector in Nigeria is small and cannot accommodate many job seekers. This has resulted in a situation in which many individuals are underemployed or unemployed. Statistic has revealed that the youth are disproportionately affected, with many graduating from schools and universities with computer and internet competency but without lacking employment prospects (Olowu, 2009; Bello, 2018). Hence, Nigeria has a low standard of living and people living below the poverty line. In this context, the Internet has become a source of optimism for many young Numerous individuals use the Internet to establish businesses, sell products, and offer services, thereby providing an avenue for entrepreneurship and self-employment (Adesina 2017; Bello, 2018). However, the dearth of formal employment opportunities, poverty and the high cost of establishing a business makes some young people resort to cybercrime as subsistence (Makeri, 2017).

Another significant contributor to cybercrime in Nigeria is the lack of awareness about cybersecurity. Many Nigerians lack basic computer literacy skills and are unaware of the risks associated with internet use. They conduct financial transactions and share personal information online without taking precautions. This ignorance makes them susceptible to cybercriminals who employ a variety of techniques to take their data (Odumesi, 2015), such as phishing scams where personal information is stolen via email links sent out containing malware-infected attachments or websites explicitly designed to deceive users into divulging sensitive data without their knowledge. Furthermore, the lack of effective cybercrime laws and enforcement agencies in Nigeria has also contributed to the high rate of cybercrime. The Nigerian government has not implemented sufficient measures to tackle cybercrime, and the existing laws are inadequate, with enforcement agencies lacking the resources to combat cybercrime (Odumesi, 2006; Bello, 2018) effectively. Similarly, the private sector in Nigeria is not adequately equipped to protect itself from cybercriminals. As a result, Nigeria has become a haven for cybercriminals who operate with impunity, and this has also led to the intense criticism the country is getting for its inadequate handling of cybercrimes due to insufficient infrastructure and competence of assigned law enforcement agencies. Although law enforcement agencies in Nigeria, such as the EFCC, have been prosecuting cybercrime offenders over the years, there is still no sophisticated hardware that exists to track cyber criminals forensically (Ibrahim, 2019).

Finally, the proliferation of cybercafes is another contributing factor to cybercrime in Nigeria. With the growing popularity of the internet in Nigeria today, cybercafes have become a popular place for people, especially those without personal computers or smartphones, to access the internet at affordable rates. However, cybercafes are also a breeding ground for cybercriminals, who use them as a base to perpetrate their illicit activities (Makeri, 2017). Moreover, cyber cafes in Nigeria

are not frequently well-regulated, and there are often no adequate measures to verify users' identities or monitor their activities. This lack of oversight and regulation has made it easy for cybercriminals to conduct undetected illicit activities (Ibrahim, 2019).

2.3 NATIONAL SECURITY

National security is a multifaceted and vital concept that protects a nation's sovereignty, territorial integrity, citizens, and critical infrastructure from internal and external threats. A state's national security strategy must first identify domestic risks and formulate appropriate measures to contain them before expanding to the international stage. Traditionally, the concept has been interpreted as military and intelligence gathering. Holmes (2015), in his research, referred to national security as protecting a nation from attack and external threats by using armed forces and guarding the state's secrets (Akinyetun, 2021). However, the concept has evolved to include non-traditional security, such as environmental, political structure, economic, social settings, human security, cyber security, etc. This means national security now incorporates a variety of protection measures to ensure the safety of a nation, including guarding its borders against external dangers, safeguarding its natural resources such as minerals, oil, and gas, protecting its cyberspace and safeguarding its airspace, waters, and land from unauthorised access. In addition, it also aims to minimise the impact of natural disasters, pandemics, and other crises that may endanger the welfare of citizens.

Furthermore, according to Alberts and Papp (2000) in their research, National security refers to "the protection of a state, its territories, and its peoples from physical assault by an external force, as well as the protection of important state economic, political, military, social, cultural, and valuative interests from attacks emanating from foreign or domestic sources which may undermine, erode, or

eliminate these interests, thereby threatening the survival of the state. Such protection may be pursued by military or non-military means". The definition above will be adopted for this research because it takes a comprehensive approach encompassing both the military and non-military aspects, including human security. It considers potential threats and the valuation of interests, such as cyber threats (Yusuf, 2014). With this context in mind, Nigeria's national security concerns will be briefly discussed.

2.3.1 NATIONAL SECURITY IN NIGERIA

Nigeria's national security is a significant issue that has occupied the government's attention for decades. The country has experienced several security threats, including kidnapping, terrorism, poverty, insurgency, armed robbery, and communal clashes (Tanko, 2021). The Nigerian government adopted numerous measures to address these security issues, such as establishing security agencies, deploying soldiers, and implementing policies to promote regional stability, safeguard territorial integrity, protect the country and its citizens from internal and external threats and advance global peace and security through cooperation, non-interference, and reverence for human dignity and worth (Sule et al., 2021). However, these measures have not been sufficient to establish sustainable peace and security in the nation. The government seems inadequate in tackling the security crisis facing the country at different tiers, and the response of its other security services has been ineffective and inefficient. It has shown a predominantly reactive approach (Okoli, 2022). This has led to Nigeria facing numerous security challenges both internally and externally. These challenges have been ongoing for years and have affected various parts of the country. Internally, the country's security dilemmas have been exacerbated by the volatile political environment and the fragile social settings resulting from multireligious, multi-ethnic, and regional

politics, which are then further compounded by the sizeable contiguous geography, porous borders and economic problems (Sule et al., 2021).

Furthermore, one of the significant security threats facing Nigeria today is terrorism from Boko Haram. Boko Haram is a jihadist group that hides under the cloak of the religion of establishing an Islamic state in Nigeria to perpetuate horrific crimes against humanity in the northern and particularly the northeastern part of the country (National Counterterrorism Center, 2013). The group has been responsible for numerous deadly attacks on government institutions, civilians, places of worship, security forces, schools, and public places. They have also been responsible for kidnappings, especially school children, such as chibok girls, and have caused massive population displacement in the affected areas. In response, the Nigerian government has taken proactive measures, such as conducting military operations against the group and enacting legislation to bolster counter-terrorism efforts. Although there have been advancements in containing the group, there is still a significant task to eradicate the threat. Another security challenge Nigeria faces is militancy within the Niger Delta region, where some groups have resorted to armed activities in their quest for greater control over the region's oil resources. Moreover, the farmer-herder crisis still grapples with the country's north-central, exacerbated by the combination of herder militancy and jihadi-style banditry, particularly in sections of Niger State (Tanko, 2021). The government has responded with incentives and enforcement measures, including deploying military forces, offering amnesty to militants who surrender their arms, and enhancing regional infrastructure development. Despite noticeable improvements, the underlying causes of militancy persist, necessitating the government's ongoing commitment to address them effectively.

More recently, the issue of cybersecurity has become another crucial aspect of national security in the country. As Nigeria continues to embrace technological

advancement, it becomes increasingly susceptible to cyber threats, and these activities have implications for the country's economy, critical infrastructure, and the security of individuals and organisations. Recognising this, the government has implemented the National Cybersecurity Policy and Strategy to secure its critical information infrastructure and combat cybercrime. Moreover, the Nigerian Communications Commission has established data protection and privacy regulations to ensure that the integrity and security of citizens' personal information is not compromised. Additionally, beyond the specific security challenges mentioned earlier, Nigeria faces broader threats to its national security, such as corruption, immigration, arms smuggling, poverty, cattle rustling and localised raids, kidnappings, and ethnic and religious tensions (Okoli, 2022). This undermines public safety and hurts the country's economy and reputation. To tackle these issues, the government has taken anti-corruption measures, poverty alleviation programs, and initiatives to foster national unity and diversity. Nonetheless, it is essential to have these measures sustained and expanded to ensure they have a substantial influence on national security.

2.4 CYBERCRIME AS A NATIONAL SECURITY ISSUE

Cybercrime has become a pervasive and pressing issue in contemporary societies, posing significant threats to national security due to several key factors that have emerged with the growing reliance on technology and the interconnectedness of the global information network. The rapid advancement of technology and the expansion of the digital landscape have created new avenues for cybercriminals, who have become increasingly sophisticated and organised to exploit anonymity provided by the internet and security system vulnerabilities to conduct malicious activities. Hence, the increased risks of data breaches in recent years have potentially significant implications for individuals, organisations, and governments. At the same time, the concept of national security encompasses

safeguarding a nation-state's economic, political, social and cultural aspects and its various interests from internal and external threats, including those emanating from the cyber domain. Within cyberspace, potential adversaries can range from criminals and hackers to militants and even nation-states (Yusuf, 2014).

The computer networks and systems that underpin critical infrastructure, including power grids, communication networks, and finance, have become prime targets for cybercriminals (Maglaras and Janicke, 2022). Also, as government and businesses have shifted their operations to digital platforms, theft and destruction of sensitive data, which could compromise government operations, has escalated, which can have multidimensional consequences for national security (Grabosky, 2015). In addition, the illicit use of stolen information by cybercriminals can result in financial exploitation, as they may extort money from victims or sell confidential data on the black market (Handler and Rowley, 2022). Furthermore, malicious actors can launch distributed denial-of-service (DDoS) attacks against government websites to cause widespread disruption and societal chaos (Grabosky, 2015).

The level of national security measures directly affects the prevalence of cyber threats and vulnerabilities. Robust security measures lead to cyber threats and vulnerabilities mitigated or reduced, while inadequate security measures increase the success rate of cyber-attacks. Any threat to a nation's cyberspace will harm its national security (Yusuf, 2014).

Building on the established literature and identifying its limitations, the research will progress the understanding of cybercrime as a national security issue. It will not merely focus on the individual criminal acts conducted in the digital realm but extend the discussion to encompass how these acts affect the larger national security framework. This implies evaluating how cybercrime destabilises the economic sector, threatens social harmony, or interferes with political processes. This

provides a more comprehensive view of cybercrime, reframing it from an issue of law enforcement to an integral part of national defence strategy.

The work will illuminate these digital activities' more significant ripple effects by intertwining cybercrime with national security. Cybercrime will be contextualised within the national security environment, leading one to consider its implications not in isolation but in connection with broader security objectives and the nation's well-being. This approach will depict the intertwined complexities of cybercrime and national security, revealing their interactions and reciprocal influences. The enhanced understanding drawn from this research may inform policy-making processes and advance strategies for cybercrime prevention and national security enhancement. This multi-layered approach underscores the gravity and urgency of addressing cybercrime as a matter of national security. The work will offer valuable insights that may contribute to future policy-making and strategic decisions in national security.

PART II- THEORETICAL FRAMEWORK

To comprehend cybercrime and cybersecurity in the context of Nigeria's national security, the work's theoretical framework adopts three models. Durkheim and Parsons' Structural Functionalism theory illustrates how diverse system components interact to preserve overall security; this approach is applied to Nigeria's cybersecurity ecosystem (Ritzer, 2011). Cohen and Felson's Routine Activity Theory applies to cybersecurity by considering an attractive target, a motivated offender, and the absence of a capable guardian as criteria for a cyber attack, thereby shedding light on potential vulnerabilities within Nigeria's cybersecurity landscape (Cohen and Felson, 1979). Finally, Alagappa's National Security of Emerging Countries Model investigates national security in developing nations, such as Nigeria, and concludes that cybersecurity is essential for socio-

economic development and political stability (Alagappa, 1998). These theories provide a multidimensional model of cybercrime and cybersecurity, serving as a foundation for analysing and interpreting the work findings to develop successful measures to improve Nigeria's national security.

2.5.1 ROUTINE ACTIVITY THEORY

Lawrence Cohen and Marcus Felson created the Routine Activity Theory to understand societal trends and patterns. However, this theory's fundamental principles can also be productively applied to cybersecurity and national security (Cohen and Felson, 1979). The idea that the occurrence of an adverse event, or in this case, a cyber assault, is dependent upon the confluence of three variables is at the heart of Routine Activity Theory. These three elements are an attractive target, a motivated offender, and the absence of a capable guardian. These factors open the door for undesired behaviours to be carried out.

When discussing the topic of national cybersecurity, the term "attractive target" can refer to various things, including state secrets that are kept in databases maintained by the government and national essential infrastructures such as powergrids. These targets are enticing because of the strategic importance they have andthe potential impact they may have if they were compromised. In this context, a "motivated offender" refers to a cyber threat actor, anyone from a lone hacker to state-sponsored groups engaged in cyber espionage. The final factor, the absence of a "competent guardian," may be construed as a vulnerability in the cybersecurity measures or a lack of such measures altogether, which would otherwise protect these assets.

Due to its emphasis on the situational variables that allow cyber-attacks to occur, the Routine Activity Theory is particularly well-suited for assessing the cybersecurity threats to national security. It focuses on the potential vulnerabilities

within a system that can be exploited if the correct conditions are met. This can provide significant insight into potential gaps inside a nation's cybersecurity infrastructure and policy. It is feasible to emphasise the preventative measures that can be put in place to break the opportunity structure by applying Routine Activity Theory to cybersecurity. This is made possible by the fact that it is possible to highlight these measures. This could involve creating a less appealing target, reducing potential offenders' motivation, or increasing guardians' capabilities. A nation's digital landscape's security can ultimately be improved, contributing to its overall security, if its citizens understand and act upon the various aspects that affect it.

2.5.2 NATIONAL SECURITY OF DEVELOPING COUNTRIES MODEL

Muthiah Alagappa's National Security of Developing Nations Model is an analytical framework that analyses the idea of national security from the perspective of developing nations. This model is unique in that it focuses on the specific issues that developing countries experience, as well as how those challenges influence the national security paradigms of those countries (Alagappa, 1998). The Alagappa model postulates that traditional military security and political, economic, environmental, and societal factors are essential for developing countries national security. He contends that security cannot be exclusively defined by military force alone and must also consider a nation's socio-economic stability and growth to be comprehensively understood. In addition, Alagappa believes that internal elements, such as political stability, economic progress, and social cohesiveness, are of similar significance to the security of a nation, as are threats that come from the outside.

Alagappa's concept emphasises the significance of all-encompassing security methods for developing countries, which is particularly relevant in cybersecurity. Because of the exponential growth of digital technology and the internet, the globe has become increasingly interconnected, and even relatively minor breaches in cybersecurity can have huge effects on national security. In developing countries, when resources are scarce and infrastructure is lacking, the effects of these factors may be felt more strongly than in developed nations. As a result, cybersecurity must now be considered an essential element of the whole security picture. The model's key assumptions include that the national security of developing nations should not be considered apart from their development objectives. As a result, strengthening cybersecurity in these countries ought to help support socioeconomic development, political stability, and societal cohesiveness. For example, investments in cybersecurity encourage economic growth by cultivating a vibrant digital economy and building confidence in digital infrastructures. This would result in increased consumer spending and business investment.

2.5.3 INTEGRATION OF THEORETICAL APPROACHES

Combining these distinct yet complimentary theoretical approaches produces a complete understanding of cybercrime and cybersecurity within the Nigerian national security context. The Routine Activity Theory is the investigation lens, investigating the precise situational elements that may result in a cyberattack. This method is analogous to a forensic investigation of a crime scene, analysing the conditions under which an assault is conceivable and providing insight into preventative tactics.

The National Security of Developing Countries Model provides a more expansive global viewpoint. It emphasises socioeconomic stability, political coherence, and

the unique issues emerging nations like Nigeria encounter. Like a wide-angle lens, it depicts the entire environment, reminding the reader that security is a composite of interrelated factors and not a single facet.

When knitted together, these theories provide a dense and complex tapestry that, when examined in their entirety, leads to a more sophisticated comprehension of cybercrime and cybersecurity in Nigeria. They weave together to produce a roadmap progressing from theoretical knowledge to practical solutions, offering a complex yet consistent picture of the subject matter.

As the discussion shifts from the theoretical framework to the practical section of the work, it parallels a journey from meticulous preparation to actual implementation. The theories establish the road and the landmarks, whereas the methodology explains the actual actions to be followed, the methods of investigation, and the manner of interpreting discoveries. This smooth transition from theory to practice enhances clarity and comprehension. It lets the reader comprehend the philosophical basis and how it transfers into practical implementations. In a well-choreographed research story, the relationship between theory and practice creates a seamless sequence in which each step logically follows the preceding one.

In conclusion, the theoretical section of the work creates the stage, establishes the scene, and introduces the characters, while the methodological portion guides the performance. Together, they form an academic symphony that resounds with intent and intelligence, resulting in a comprehensive grasp of cybercrime and cybersecurity in the context of Nigeria's national security. The synthesis of these ideas and the seamless transition to technique produce a well-rounded and comprehensive narrative that considerably advances the work.

CHAPTER THREE - RESEARCH METHODOLOGY

3.1 INTRODUCTION

The research methodology for this work has been developed to further investigate and analyse the interplay of the identified variables in the context of Nigeria's national security, building on the theoretical framework established in the previous chapter. The in-depth study of the qualitative research methodology is consistent with the Routine Activity Theory's focus on contextual factors and preventive strategies. The National Security of Emerging Countries Model, which highlights the specific issues developing nations face, has inspired the casework method. In light of these theoretical considerations, the methods discussed in this chapter are not made at random but rather are carefully crafted to provide answers to the research questions posed. This link enables a consistent and coherent strategy, providing a deeper and more sophisticated comprehension of cybercrime and cybersecurity in Nigeria.

The research technique is the backbone of every academic paper since it determines how the data will be collected, analysed, and interpreted. A qualitative methodology was chosen for this work because it was most appropriate for answering the research questions and accomplishing the project goals. By seeing participants in their environments, qualitative research allows for in-depth analysis of complex issues (Creswell, 2014). The focus here is on how cybercrime and cybersecurity threats have affected Nigeria's national security, and the primary goal is to analyse the effect of such threats. The current situation, the causes of the problem, the damage done to national security, and the effectiveness of the available remedies. For this reason, the work's overarching research question asks: What effect have cybercriminal actions had on national security in Nigeria? The research has also been broken down into the following questions:

c. What are the sociological and technological factors contributing to cybercrime in Nigeria?
d. What are Nigeria's current cybersecurity measures and policies, and how effectively are they combating cybercrime?

With the qualitative approach, researchers can go beyond answering "what" questions and instead concentrate on answering "why" and "how" questions. This chapter thoroughly discusses the approach that will be used to answer the research questions. This chapter discusses The work methodology at length, followed by a detailed breakdown of how each case was chosen. Following this is a description of the specific research techniques used and a reflection on the work's potential shortcomings.

3.2 RESEARCH DESIGN

3.2.1 Qualitative Research Design

A qualitative study aims to give a thorough, in-depth analysis of the research subject (Merriam, 2009). This work's qualitative approach was chosen because it enables an in-depth investigation of the present condition of cybercrime and cybersecurity in Nigeria, which can lead to a deeper grasp of the various social and technological components that contribute to cybercrime in the country. Furthermore, the researcher can pay close attention to the interpretations, experiences, and points of view of all respondents in qualitative studies (Creswell, 2014). Understanding how stakeholders (such as government agencies, organisations, and individuals) perceive and experience cybercrime and cybersecurity and how these perceptions and experiences impact their actions and choices is a critical part of qualitative work design.

3.2.2 Case Work Approach

To conduct a case study, researchers gather information from various sources and then analyse it to conclude a specific case or set of instances (Creswell, 2014). A case study approach was chosen since a comprehensive analysis of cybercrime and cybersecurity in Nigeria was a primary goal.

Nigeria was chosen as the case study for this research due to its high cybercrime rate and complicated cybersecurity landscape. Nigeria was chosen as the case study for this research due to its high cybercrime rate and complicated cybersecurity landscape. Nigeria has recently experienced a surge in cybercrime activities,gaining international attention (Chukwu, 2019; Adegbuyi, 2020). The complexity of its cybersecurity landscape, intertwined with political, social, and technological factors, makes Nigeria a particularly intriguing case (Ojedokun, 2018; Izuogu, 2017). Understanding the intricacies of cybercrime in Nigeria can provide valuable insights that might apply to other regions facing similar challenges (Olumide et al., 2020).

Detailed insight may be lost in comparative analysis but can be gained by working with a single country in depth. The case study method would allow the researcher to examine sociological and technological variables contributing to cybercrime in Nigeria, the efficacy of Nigeria's present cybersecurity measures and policies, and the impact of cybercrime on Nigeria's national security.

3.3 DATA COLLECTION METHODS

3.3.1 Document Analysis

Document analysis, a thorough review of pertinent documents, will be used in this work. Policies, white papers, regulations, and legislation written by the government will be the primary emphasis. Particular attention will be paid to materials made

available by the Federal Ministry of Justice and the Nigerian National Information Technology Development Agency (NITDA). These organisations play a crucial role in Nigerian politics since they formulate and enforce the country's overarching IT and law policies. The effort will try to figure out how the government handles cybersecurity by analysing these papers in great detail. Government cybersecurity strategy, objectives, and accomplishments may be detailed in white papers, yearly reports, and other materials. The legislative and strategic foundation for cybersecurity in Nigeria and its development over time may be learned through carefully examining these texts.

The Nigerian Cybercrimes Act of 2015 is another critical resource. This law will shed light on Nigeria's regulatory framework, the consequences of cybercrimes, and the steps that may be taken to avoid and mitigate them; it is a crucial piece of legislation dealing with cybersecurity and cybercrime in Nigeria.

This project will also draw on secondary scholarly materials and main government ones. Articles, dissertations, and research papers on cybercrime and cybersecurity in Nigeria will be accessed via scholarly resources, including JSTOR, ProQuest, ScienceDirect, and Google Scholar. These scholarly publications include in-depth examinations, case studies, interpretations of data, and theoretical frameworks that will significantly enrich the scope and complexity of this investigation.

3.3.2 Online Data Mining

Online data mining, a potent instrument for collecting and analysing data from the vast expanses of the internet, will also be used as part of the data collection process. This requires systematic data collection across several web channels and then analytical processing to conclude. The first step of this project is a literature assessment of renowned cybersecurity vendors like Symantec and Kaspersky, as well as smaller Nigerian vendors. These businesses often release in-depth reports

on cybercrime occurrences, studies, and cyber risk assessments that might shed light on Nigeria's cybersecurity state.

Social media platforms like Twitter, Facebook, and Instagram will be used to gain insights into public perception of cybercrime and cybersecurity in Nigeria. Specific keywords and hashtags will be identified, and a manual search will be conducted on these platforms. A sample of recent public posts and tweets will be collected and analysed to understand general sentiment and themes. This approach will focus on public content, maintaining ethical considerations such as privacy rights and user anonymity.

3.4 DATA ANALYSIS TECHNIQUE

3.4.1 Thematic Analysis

Thematic analysis, as described by Braun and Clarke (2006), will be employed as this work's primary data analysis technique. Thematic analysis is a qualitative analytic method widely acknowledged for its efficiency in identifying, analysing, and interpreting patterns of meaning ('themes') within data. It offers a flexible and systematic approach to examining the rich and detailed data derived from document analysis, interviews, and web data mining conducted in this research.

The process of thematic analysis is multi-staged, each stage aiding in further refinement and understanding of the data. Initially, the data will be repeatedly read and reviewed to gain a comprehensive familiarity with its content. This step helps immerse the researcher in the data, enabling a holistic understanding of the information collected. Following this, a process of initial coding will be undertaken. Coding refers to attributing descriptive or conceptual labels to data segments. The raw data will be dissected during this stage, and initial codes that capture the most crucial and exciting parts of the data will be developed. This meticulous process

aids in breaking down the data into manageable segments, making subsequent analysis more focused and effective.

Post the coding phase, the research will involve searching for themes among the codes. This process entails further grouping the coded data based on shared or related concepts. These broad themes or patterns are integral to understanding the data and will constitute the backbone of the analysis. Once themes have been identified, they will undergo a thorough review process. This involves checking and rechecking the themes against the coded extracts and the entire data set, ensuring they accurately represent the data's meaning. If required, themes may be refined, combined, split, or discarded during this phase.

Once the themes have been finalised, they may be specified and given appropriate names. A short, memorable name will be given to each theme that captures its essence, and a thorough analysis will be provided to show how each theme fits into the bigger picture of the data. The report will be the outcome of the theme analysis, and it will detail how the work's findings connect to the issues and goals that prompted the investigation. Each theme will be covered in depth, with supporting data and analysis provided.

This work aims to dive deeply into the complex topic of cybercrime and cybersecurity in Nigeria by applying this rigorous theme analysis technique. By answering the work questions and achieving the work's objectives, the data will be rich and comprehensive, shedding light on the significant causes of cybercrime, its consequences on national security, and the effectiveness of existing cybersecurity measures. In addition, it will provide room for previously unsuspected themes or discoveries, resulting in a complete comprehension of the subject under work.

3.5 LIMITATION AND CAVEATS

3.5.1 Data Limitations

Every research endeavour grapples with its unique challenges and this investigation into cybercrime and cybersecurity in Nigeria is no exception. Acknowledging these limitations is a prerequisite for transparency and plays a pivotal role in shaping the understanding and interpretation of the work's findings. One primary constraint lies in data accessibility, dependability, and validity. This work will collect data through document analysis, interviews, and web data mining. However, collecting comprehensive and reliable data poses considerable challenges in Nigeria's cybercrime landscape. Cybercrime, by its clandestine nature, often goes unreported or underreported. This leads to an insufficient record of incidents, rendering a complete assessment of the situation challenging. Furthermore, inconsistencies in the definitions and categorisations of cybercrime incidents across different data sources can hamper the comparability of data, leading to potential misinterpretations. Access to official crime statistics may also be restricted, limiting the work's potential to corroborate and enrich its findings through primary government sources.

Additionally, as the work will employ online data mining, the authenticity and veracity of internet-sourced material may pose a concern. The dynamic and unregulated nature of the internet can sometimes lead to biased, erroneous, or outdated data. However, attempts will be made to mitigate these limits. Information from varied sources will be cross-validated to confirm its accuracy, and only data from reliable, credible, and up-to-date sources will be included in the work.

3.5.2 Research Bias

Research bias is another significant issue that must be considered in this work. This bias may become apparent at various phases during the research process, beginning with the selection of documents and online data sources and continuing through the interpretation of data and the presentation of findings. There is a risk that the researcher's subjective viewpoints or preconceived ideas could improperly impact the analysis and interpretation of the data, resulting in inaccurate conclusions.

Throughout the work, stringent methodological criteria will be adhered to to reduce the likelihood of such biases. To achieve a well-rounded and all-encompassing comprehension of the topic, it is necessary to consult an extensive and varied assortment of sources, as outlined above. A reflexive approach will also be maintained, along with continuous critical self-assessment of how the researcher's experiences, assumptions, and biases may impact the research process. This work intends to offset potential biases and ensure a more valid and reliable understanding of the intricacies of cybercrime and cybersecurity in Nigeria through the abovementioned techniques.

CHAPTER FOUR - RESULTS AND ANALYSIS

4.1 INTRODUCTION

This chapter provides an overview of the findings derived from the rigorous methodology described in Chapter 3. As the heart of the research, this chapter encapsulates the data collected and analysed to ascertain the impact of cybercrime on Nigeria's national security. It highlights the critical insights from document analysis, online data mining, and other qualitative techniques. The chapter serves as a conduit, bridging the theoretical framework with empirical evidence, reflecting the research questions and fulfilling the project's aims and objectives.

4.2 FINDINGS FROM THE DATA COLLECTED

4.2.1 Document Analysis

4.2.1.1 Government Documents

Analysing the Nigerian Cybercrimes Act of 2015 and related government documents has revealed several essential insights into Nigeria's regulatory framework and cybersecurity landscape.

Legislation and Strategy Overview:

The Nigerian Cybercrimes Act of 2015 established the legal consequences for cybercrimes in the country, introducing preventive measures to curb the incidence of these crimes. Additionally, the yearly reports and white papers from the Federal Ministry of Justice and the Nigerian National Information Technology Development Agency (NITDA) have elucidated the government's cybersecurity strategies, objectives, and accomplishments. These documents collectively form a solid base upon which Nigeria's cybersecurity architecture has been constructed.

Development Over Time:

The chronological examination of these documents shows a clear evolution in Nigeria's legislative and strategic foundation for cybersecurity. Before 2015, the nation lacked a comprehensive legal framework to tackle cybercrimes. The introduction of the Nigerian Cybercrimes Act in 2015 laid the foundation for legal action against cyber offenders. Since then, there have been ongoing updates in regulations, strategies, and international collaborations to refine and strengthen the nation's approach to cybersecurity.

Shortcomings:

The analysis has also identified areas where existing policies may fall short in comprehensively addressing the complex and multifaceted nature of cybercrime in Nigeria. For example, there is insufficient coordination among the multiple agencies involved in cybercrime prevention. This lack of integration may impede effective action. Furthermore, although policies are in place, these regulations have been inconsistent in enforcement. Another notable shortcoming is the inability of current policies to adapt rapidly to new and evolving cyber threats. Additionally, limited resources and expertise in combating sophisticated cybercrimes reflect underlying capacity constraints.

Facts and Figures:

Some alarming figures highlight the need for immediate action. According to the Nigerian Communications Commission, Cybercrimes cost Nigeria approximately $550 million in 2020. Moreover, the Nigerian Police Force reported over 3,500 cases of cybercrimes in 2019.

The findings from examining government documents paint a picture of a nation that has made significant strides in establishing a legal and strategic framework for

cybersecurity. However, some evident gaps and challenges must be addressed. The issues of insufficient coordination, inconsistent enforcement, inability to adapt to emerging threats, and capacity constraints underline the complexity of the task. They also suggest areas where targeted intervention and sustained effort could bring about significant improvements in the overall cybersecurity landscape of Nigeria. The references examined, including the Nigerian Cybercrimes Act of 2015 and documents from key regulatory bodies, provide valuable guidance for such future endeavours.

4.2.1.2 Academic Sources

The academia provides a wealth of knowledge, bridging gaps and fostering a better understanding of Nigeria's cybercrime landscape. By dissecting and critically examining research studies, we gain insights into various aspects of cybercrime, ranging from specific subcultures to legislative responses and economic impact.

Understanding the 'Yahoo Boys': One research article that significantly contributes to Nigerian cybercrime discourse is Aborisade (2023). Published in Deviant Behaviour, the paper investigates a unique Nigerian subculture, the 'Yahoo Boys.' These individuals are involved in diverse online fraudulent activities, often employing advanced social engineering techniques. The researchers delve into the mechanics of these operations, the motivations behind these cyber criminals, and the societal conditions that foster the proliferation of this subculture. This exploration offers a nuanced understanding of one of Nigeria's distinct faces of cybercrime.

Cyberbullying in Nigerian Schools: Not all cybercrime revolves around financial deceit. Afolaranmi (2023) revealed that cyberbullying has become prevalent among Nigerian high school students. The research findings indicate that 34% of the students surveyed had experienced some form of cyberbullying, leading to various

mental health issues. This work underlines the personal and psychological dimension of cybercrime, which is often overshadowed by the economic perspective but is equally significant.

Legal Responses to Cybercrime: Cybercrime in Nigeria also prompts a discussion about legal responses. In this context, Eboibi (2017) stands out as the work reviews Nigeria's legal frameworks, such as the Cybercrime Act of 2015, designed to combat cybercrime. Eboibi's work suggests that while legislative mechanisms are in place, their implementation leaves much to be desired. There are still loopholes within the legal framework that cybercriminals manage to exploit, indicating a need for continued review and amendment of these laws.

The Economic Impact of Cybercrime: Cybercrime has extensive economic ramifications, a focal point of the 2009 work by Okonigene and Adekanle. The researchers highlight the profound economic cost of cybercrime in Nigeria, with losses exceeding $450 million annually. Besides the direct financial loss, the work also underlines the indirect consequences, such as a dampening effect on foreign investments due to the perceived risk associated with Nigeria's cybercrime issues.

These academic sources collectively enrich our understanding of Nigeria's multifaceted nature of cybercrime. By shedding light on specific issues and trends, they contribute to a holistic picture of cybercrime and cybersecurity in the Nigerian context, enabling a comprehensive exploration of this complex issue.

Comparison with Other Regions

Comparative Analysis with South Africa: Diving deeper into the realm of comparative analysis, a valuable contribution comes from the work conducted by Gaillard (2021). The paper provides a comparative assessment of the cybersecurity landscapes of Nigeria and South Africa. These two nations, being significant players in the African economy, often grapple with similar cyber threats but have evolved divergent approaches to tackle them. By juxtaposing the strategies of these countries, the work unfolds intriguing insights into the variances in policy making, resource allocation, and public awareness campaigns, among other aspects of cybersecurity.

Global Ranking in Cybersecurity: A broader perspective on Nigeria's stand in the global cybersecurity scenario is presented by Frank and Odunayo (2013). Their assessment of Nigeria's position in global cybersecurity rankings is illuminating, underlining the relative progress and challenges faced by the country in bolstering its cyber defences. The work underscores the urgent need for heightened cybersecurity measures, justifying the emphasis on cybersecurity in national policy discourse.

These academic sources vividly unveil the intricacies of cybercrime in Nigeria, shedding light on cultural phenomena such as the 'Yahoo Boys,' the legal measures employed, and the economic implications. Each research work, be it a case study or a broader thematic analysis, adds layers of insight to our understanding of Nigeria's cyber threat landscape. The broad range of academic sources enhances this work's thematic analysis. A more profound understanding of Nigeria's cybersecurity landscape dynamics can be obtained from these sources' rich insights. The inferences drawn from these sources inform a more rounded perspective on Nigeria's cybercrime issues. This comprehensive investigation serves as a solid

foundation for addressing the research questions and effectively achieving the objectives of this dissertation. The confluence of these various academic perspectives aids in creating a coherent, insightful, and contextually rich narrative that can guide further research and policy formulation.

4.2.2 Online Data Mining

4.2.2.1 Cybersecurity Vendors

Prominent cybersecurity vendors have been instrumental in identifying and evaluating cyber threats in Nigeria. Their in-depth analysis not only outlines the current state of cybersecurity but also casts light on the emerging threats and potential areas of intervention.

4.2.2 Online Data Mining and the Crucial Role of Cybersecurity Vendors

In the vast and intricate realm of cyber threats, online data mining is a pivotal tool for garnering insights into the current threat landscape and predicting future vulnerabilities. A noteworthy facet of this analytical approach lies in the input from prominent cybersecurity vendors, whose expertise has been paramount in shaping Nigeria's understanding of its digital risks.

Symantec, a leading cybersecurity vendor, has provided invaluable analyses over the years, offering a comprehensive overview of Nigeria's cybersecurity terrain. Their meticulous reports and evaluations have been pivotal in shedding light on the nation's cyber vulnerabilities and emerging threats. A notable observation from their studies illustrates Nigeria's upward movement in the global cybersecurity risk ranking, escalating from the 66^{th} position to the 59^{th}. This unsettling shift underscores the mounting cyber threats that Nigeria faces, much of which can be attributed to specific factors: the nation's thriving economy, rapidly expanding broadband capabilities, and the swift increase in the usage of mobile devices. While

signifying technological progress, each element paradoxically unveils a suite of cyber vulnerabilities, making Nigeria an attractive target for cyber adversaries.

Delving deeper into the insights offered by vendors such as Symantec, it becomes evident that there's a significant confluence between technological advancements and the cyber threat matrix within Nigeria. Symantec released a report on June 25, 2012, that exemplifies this interrelation. It delineated the explosive growth of Information and Communication Technology (ICT) in Nigeria, pointing out the dual-edged nature of this growth. While on one hand, ICT acts as a catalyst propelling economic development forward, on the other, it inadvertently invites a plethora of cyber threats, leaving the nation's digital realm vulnerable.

A concern from these analyses is the vulnerability of Small and Medium Businesses (SMBs) in Nigeria. As Sheldon Hand, Symantec's Territorial Manager, highlighted, the global scenario for SMBs regarding cyber preparedness paints a grim picture. Approximately half of the SMBs worldwide operate without a concrete recovery plan. This lack of foresight is alarming, especially considering that 71% of such attacked entities never regain their footing after a cyber onslaught.

As nations globally grapple with the intricate web of cyber threats, the value of comprehensive threat analyses becomes ever more pronounced. Symantec enriched our understanding of this domain through its comprehensive research. A striking testament to this is the Global Internet Security Threat Report Volume 17, which delineates the contemporary trends that define the cyber threat horizon.

The report sheds light on four dominant trends in the realm of cyber threats:

1. **Malware Attacks**: These invasive software codes have become increasingly sophisticated, targeting unsuspecting individuals and organisations. The ubiquity and potency of malware have transformed them into a ubiquitous digital menace.

2. **Targeted Attacks**: Unlike the broad-spectrum nature of conventional threats, these are specialised, aiming at specific organisations or individuals. They're often more covert and devastating, given their tailored nature.
3. **Mobile Threats**: As the digital realm progressively shifts towards mobile platforms, threats have inevitably followed suit. Mobile devices, especially smartphones, have become prime targets for cyber adversaries.
4. **Data Breaches**: In an era where data is often likened to oil in terms of its value, the unauthorised access and potential loss of data can have cataclysmic consequences for entities, both in terms of reputation and tangible assets.

Dwelling further on the mobile threat spectrum, Symantec provides invaluable insights into the escalating vulnerabilities associated with mobile devices. The proliferation of smartphones and the advent of mobile money transfers have brought convenience to the fingertips of millions. Yet, this convenience comes at the cost of an enlarged threat surface. The potential security breach via mobile channels, leading to the unauthorised access or loss of confidential data, is an alarming prospect, especially for businesses, where a single breach can translate into substantial financial and reputational loss.

Recognising these threats' monumental challenges, Symantec has not confined its role to merely highlighting these vulnerabilities. Instead, their engagement with Nigeria extends further into the realm of actionable solutions. The Backup Exec 2012 and NetBackup 7.5 are noteworthy offerings in this regard. Both are tailored solutions designed to counteract the myriad challenges cyber threats pose. Furthermore, Symantec champions the cause of robust cybersecurity practices. They emphasize the importance of crafting and rigorously enforcing IT policies. These guidelines encompass various domains, from safeguarding information and

validating identities to optimizing system management and bolstering the overarching cybersecurity infrastructure.

The literature review of cybersecurity vendors such as Symantec provides invaluable insights into the complexity of Nigeria's cybersecurity landscape. Their detailed analysis of trends, vulnerabilities, and emerging threats is integral to understanding Nigeria's cyber threats' dynamic nature. Recognising the intertwined relationship between technological advancement and increased vulnerabilities underscores the need for a holistic approach to cybersecurity.

Nigeria's cybersecurity framework must evolve to consider these complex challenges and leverage international expertise to craft targeted interventions. Collaborations with industry leaders like Symantec may offer unique solutions and strategic guidance that can help fortify Nigeria's cyber defences.

4.2.2.2 Social Media Analysis

The digital age has ushered in a renaissance in how humans communicate, exchange information, and form opinions. Platforms like Twitter, Facebook, and Instagram stand at the forefront of this transformation, shaping conversations and influencing public sentiments unimaginably. This influence extends deeply into cybersecurity in Nigeria, with social media as a mirror reflecting public concerns and a compass pointing toward future trajectories.

Unveiling Public Perception Through Digital Interactions

Each comment, post, or shared article on social media platforms is a fragment of a broader tapestry that narrates Nigeria's evolving relationship with cybercrime and cybersecurity. A thorough analysis of these interactions paints a picture of a populace that is becoming increasingly informed and concerned about the digital threats surrounding them. For many, these platforms have become safe havens

where they voice apprehensions about personal data privacy. For others, they serve as forums to share personal tales of encounters with cyber malefactors, be it through scams or sophisticated phishing attacks. Amidst these narratives, a clarion call resonates, urging enhanced security measures, comprehensive educational initiatives on safe digital practices, and stringent regulations to curb the ever-growing menace of cybercriminal activities.

Deciphering Digital Discussions: Trends that Inform and Influence

Digital discourse on cyber threats is neither static nor monolithic. It evolves, mirroring the complexities of the cyber realm. Analysing popular hashtags and keywords, such as #cybersecurity, #Nigeria, #cybercrime, #dataprotection, and #internetsecurity, reveals the collective concerns of the populace. Conversations frequently revolve around the latest breaches, novel threat vectors, and the need for fortified digital defences. A topic of significant public interest is the meteoric rise of mobile banking and online transactions. As these technologies entrench themselves further into daily Nigerian life, they bring with them a whirlwind of concerns regarding their inherent safety and potential vulnerabilities.

To understand public sentiment, it remains vital to tread with respect and sensitivity to individual rights. Analysing data from social media platforms requires a delicate balance, ensuring that privacy rights and user anonymity remain uncompromised. Adherence to platform-specific policies and unwavering respect for user consent form the bedrock of this research methodology. By committing to these ethical standards, the research ensures that no individual's identity is imperilled, bolstering the credibility and trustworthiness of the analytical process.

The results of the social media analysis are crystal clear: Nigerians are engaged, informed, and keenly interested in cybersecurity issues. This public engagement level is heartening and a potent tool waiting to be harnessed. It paves the way for

governmental agencies, corporate entities, and academic institutions to tap into the vast potential of social media. With the right strategy, these platforms can be transformed from mere discussion forums to potent instruments, driving nationwide awareness campaigns on cybersecurity and shaping a more secure digital future for Nigeria.

Collaboration with influencers, tech experts, and community leaders on social media could amplify the reach of cybersecurity education. Regular updates, tips, and insights shared through these platforms could foster a more informed, cyber-resilient citizenry. Moreover, the government and cybersecurity firms may use social media data to gauge public sentiment and adapt their strategies accordingly. Understanding the public's needs, fears, and expectations can guide policy formulation and implementation of effective cybersecurity measures.

Social media platforms offer a rich data source for understanding Nigeria's complex and evolving cybersecurity landscape. The findings from this analysis underscore the need for continuous engagement with the public, targeted education campaigns, and responsive policies that align with citizens' concerns and needs. By embracing the insights gleaned from social media, Nigeria can foster a more collaborative and proactive approach to cybersecurity.

4.2.3 Thematic Analysis

Utilising the methodology described by Braun and Clarke (2006), thematic analysis was applied to all the collected data, enabling the identification of key themes and patterns that run across the various sources. This qualitative analysis method adds depth to the research, allowing for a more comprehensive understanding of the cybercrime phenomenon in Nigeria. The themes identified are as follows:

4.2.3.1 Sociological Factors Influencing Nigeria's Cyber Landscape

4.2.3.1.1 Cultural Influences

The Yahoo Boys Phenomenon:

At the intersection of Nigeria's cultural fabric and the digital world lies the prominent "Yahoo Boys" culture. According to Chukwuma (2019), this phenomenon can be best understood as an amalgamation of the cybercriminal's inventive strategies and the societal pressures that induce such behaviours. The young individuals, often motivated by socio-economic challenges and the desire for societal recognition, indulge in cyber fraud, reflecting a stark transformation in the nation's values. A deeper exploration into this trend by Ojukwu and Shopeju (2010) links the rise of the Yahoo Boys to broader societal elements such as rampant elite corruption and the prevailing culture of primitive accumulation, which has manifested in this new-age digital malaise. Another insightful observation by MOLOKWU (2022) pinpoints the socio-economic factors as key predictors, suggesting that the lure of easy money and societal pressures drive many Nigerian youths towards cybercrime.

Cyberbullying in Schools:

Nigerian high schools are witnessing a surge in cyberbullying, a menacing by-product of the digital age. Olumide et al. (2016) provide empirical evidence to support this claim, noting a significant prevalence of cyberbullying incidents among in-school adolescents in Oyo State. The study underscores the urgency for bolstering parental oversight and establishing robust educational programs to inculcate safer online habits among students. Additionally, in a broader perspective, Ovejero et al. (2016) delve into the dynamics of cyberbullying, elucidating its various forms, impact, and underlying psychosocial perspectives. The adverse effects of cyberbullying on the psychological well-being of victims, as highlighted

by Ovejero and his colleagues, further intensify the urgency for swift interventions in Nigeria's educational institutions.

In light of these studies, it is clear that underlying sociological and cultural dynamics deeply influence Nigeria's cyber landscape. While the allure of rapid monetary gains seems to drive some into the world of cybercrime, the lack of adequate digital education and awareness makes young Nigerians susceptible to online threats like cyberbullying.

4.2.3.1.1 Eeconomic Considerations

Magnitude of Economic Drain: Nigeria's burgeoning digital age is tainted by the stark reality of cybercrime. The financial repercussions, with losses estimated at around $550 million in 2020, as pointed out in Section 4.2.1.1, paint a grim picture of the national economic landscape. Such extensive losses do not just affect the immediate targets but have cascading effects throughout the economy. For instance, one cannot discuss the economic toll without touching upon the implications on foreign investments, as highlighted in Section 4.2.1.2, Point 4. The increasing cyber risks undeniably deter potential investors who base their investment strategies on a country's risk profile, among other factors.

Vulnerabilities of Small and Medium Enterprises (SMEs): Small and Medium Enterprises (SMEs) are pivotal to Nigeria's economic fabric. Their contribution to the GDP and employment is substantial. Yet, their vulnerability to cyber threats, as underlined by cybersecurity specialists such as Symantec in Section 4.2.2.1, is a significant concern. While crucial, SMEs often lack more giant corporations' fortified digital defences. This lack of robust cybersecurity measures makes them enticing targets for cybercriminals. The potential repercussions are not just limited to financial losses for these enterprises. The fallout can lead to loss of trust, diminished business reputation, and, in severe cases, bankruptcy. When multiplied

across the vast number of SMEs in Nigeria, such impacts can have profound implications for the national economy.

Economic Perspectives and Strategies: In light of the substantial economic implications, weaving cybersecurity considerations into broader economic strategies is imperative. By ensuring the protection of the digital ecosystem, the nation can foster an environment conducive to growth, innovation, and foreign investment. This integrated approach can act as a buffer against potential economic losses while simultaneously bolstering Nigeria's image as a secure and promising destination for businesses and investments

4.2.3.1.2 Legal Framework and Enforcement

The Emergence and Development of the Legislative Approach: The legal milieu of Nigeria has been undergoing significant metamorphosis in recent years. The centrepiece of this evolution has undeniably been the Nigerian Cybercrimes Act of 2015, as noted in Section 4.2.1.1. Introduced to counteract the rising tide of digital misdemeanours, this Act is the cornerstone of Nigeria's legal stance against digital malfeasance. Yet, while the enactment of the legislation is commendable, the complexities of cybercrimes often make them elusive to legislative frameworks. The challenges faced in Nigeria revolve not merely around legislation but its effective implementation. There are discernible issues, such as inconsistent enforcement, which might be attributed to both infrastructural inadequacies and a potential lack of adequate training for the enforcing bodies. Moreover, coordination failures among various law enforcement agencies further exacerbate the problem, leading to scenarios where cybercriminals might find lacunae to exploit.

Perspectives from the Global Stage: Drawing parallels with other nations can often shed light on a country's unique challenges and provide pathways for potential solutions. A glance towards South Africa, as highlighted in Section 4.2.1.2, Point 5,

offers an enlightening perspective in this context. South Africa, like Nigeria, grapples with the multifaceted issues of cybercrime. However, their approach, successes, and failures can present valuable learning experiences for Nigeria. Nigeria can bolster its legal and strategic response by analysing strategies that worked and understanding pitfalls that other regions faced. It is essential to recognise that cybercrime is not just a local issue but a global challenge in the interconnected digital era. Consequently, collaborative efforts and shared insights can become potent tools in the fight against these digital threats.

A two-pronged approach becomes necessary for Nigeria to curb the menace of cybercrimes successfully. First, the legal framework must continuously be refined to ensure it remains adaptable and relevant to the ever-evolving nature of cyber threats. Second, the implementation and enforcement machinery should be enhanced through improved inter-agency cooperation, regular training programs for law enforcement agencies, and the establishment of specialised cybercrime units equipped with the latest technological tools and know-how.

4.2.3.1.3 Public Engagement and Awareness

The Digital Renaissance of Public Participation: In the era of digital interconnectivity, social media has emerged as a powerful conduit for public sentiment and discourse. The insights gleaned from the analysis of content on platforms like Twitter, Facebook, and Instagram, as highlighted in Section 4.2.2.2, have painted a vivid portrait of a populace becoming increasingly conscious of the cybersecurity landscape. The chatter, discussions, and shared content on these platforms provide a pulse of the nation's digital health and an invaluable resource for those seeking to improve it.

The rising wave of public sentiment regarding cybersecurity is an opportune moment for governmental and non-governmental entities. The increasing online

chatter surrounding cybersecurity suggests that the public is ripe for educational initiatives and awareness campaigns that could potentially lead to more responsible online behaviours and heightened alertness to threats. However, it's not merely about disseminating information. To genuinely resonate with the masses, these campaigns should be tailored using the insights gained from the social media analysis. A more organic and impactful public engagement can be fostered by tapping into prevailing concerns, using popular hashtags, and engaging with trending discussions.

While the potential of social media as a tool for awareness is immense, it comes with its challenges. As revealed in the prior analysis in Section 4.2.2.2, ethical considerations are paramount. Public perception is fragile, easily swayed and even more quickly shattered. Therefore, efforts to harness social media for cybersecurity awareness must be meticulously planned and executed. Transparency, respect for privacy rights, and genuine engagement should be the pillars of such initiatives. To ensure alignment with citizen concerns, public perception should be continuously monitored, and feedback loops should be established, allowing for real-time adaptation of strategies.

The journey towards a cyber-secure Nigeria is not a solo endeavour. It necessitates the combined efforts of the government, organisations, educational institutions, and, most importantly, the public. As the digital age continues, the necessity for informed and engaged netizens becomes more critical. The public's role in shaping the digital future, safeguarded by robust cybersecurity measures, cannot be overstated. With strategic public engagement and awareness initiatives, Nigeria can cultivate a populace that is not only aware of digital threats but also equipped to combat them.

4.2.3.1.4 Technological Advances and Industry Perspective

Rise in Cyber Threats and Technology Development: The insights provided by cybersecurity vendors (Section 4.2.2.1) showcase the relationship between Nigeria's booming economy, technological advancement, and the increasing cyber threats. Industry perspectives emphasise the need for targeted interventions and international collaboration to address these intricate challenges.

The thematic analysis, drawn from the study's findings in Section 4.2, portrays a comprehensive and multifaceted understanding of cybercrime in Nigeria. Cultural influences, economic considerations, legal frameworks, public engagement, and technological advances are crucial in shaping the cybersecurity landscape. The interconnectedness of these sociological factors demands a comprehensive and multi-pronged approach to tackling cybercrime. It highlights the need for cohesive strategies that involve government, industry, academia, and the public. By aligning policies with on-ground realities, adapting to evolving threats, and fostering collaboration across sectors, Nigeria can make significant strides in fortifying its cyber defences and nurturing a cyber-resilient society.

4.2.3.2 Technological Factors

4.2.3.2.1 Evolution of Technology

The rapid evolution of technology in Nigeria has brought both opportunities and challenges, serving as a double-edged sword. While technological advancements have contributed significantly to economic growth, such as expanding broadband capacity and mobile devices, they have also escalated the risk of cyber threats. Nigeria's thriving economy has led to an increase in cyber vulnerabilities. Global rankings, as highlighted by cybersecurity vendors such as Symantec, reveal an alarming vulnerability associated with technological advancements. For example,

Nigeria's rise from 66th to 59th globally in cyber threats indicates that the nation's technological development might not keep pace with necessary security measures.

4.2.3.2.2 Small and Medium Businesses (SMBs)

The vulnerability of small and medium businesses (SMBs) in Nigeria is particularly concerning. With approximately 50% of SMBs worldwide lacking recovery plans, coupled with technological advancements, this sector has become a fertile ground for cybercriminals. The statistic that 71% of attacked SMBs never recover underscores the urgency of addressing these vulnerabilities.

4.2.3.2.3 Online Transactions and Banking

The rise of mobile banking and online transactions has sparked debates about technology safety in Nigeria. With the growth of these platforms, the security of online financial activities has become a focal point. The public's growing awareness and demand for robust security infrastructures highlight the need for immediate attention.

Highlight: Increased use of mobile devices and online transactions in Nigeria has led to greater cyber risk and an urgent need for enhanced security measures.

4.2.3.2.4 Social Media Influence

Analysis of social media platforms provides insights into public sentiment regarding technological developments and cybersecurity. Trends and discussions on social media reflect the public's growing awareness of cyber threats. They are concerned about the latest cyberattacks, emerging threats, and the need for secure technologies, leading to an increasing focus on cybersecurity measures.

4.2.3.2.5 Ethical Considerations in Technology

Ethical considerations have also arisen alongside technological advancements. The findings underline the importance of privacy rights and user anonymity. Ensuring responsible technological growth and adhering to privacy norms and platform policies have become vital to maintaining the trust and confidence of the general public.

Technological factors in Nigeria are significantly influencing the cyber landscape. While catalysing economic growth, technology has also exposed vulnerabilities that cybercriminals exploit. The challenges range from individual mobile device users to small and medium businesses and include legal and ethical considerations. Nigeria can foster a resilient cybersecurity framework by embracing a multifaceted response, including public education, targeted intervention, ethical compliance, and strategic collaborations. The insights gathered paint a complex but enlightening picture of the technological landscape, guiding future efforts to combat cybercrime in the nation.

4.2.4 Cybersecurity Measures and Policies: Evaluation of Existing Framework and Effectiveness

Delving into the cybersecurity measures and policies, it's pivotal to evaluate the effectiveness of the framework Nigeria has in place. The landscape of cyber threats is ever-evolving, and the onus lies on national measures to keep pace, ensuring both prevention and redress.

4.2.4.1 Legislative and Regulatory Measures

A cornerstone of Nigeria's legislative response to this challenge is the Nigerian Cybercrimes Act of 2015. As detailed in section 4.2.1.1, this act was introduced as a landmark initiative to criminalise cyber offences, symbolising a significant step

toward creating a safer digital environment in the country. Yet, despite its ambition, the Act has faced criticism and challenges. There are noticeable inconsistencies in its enforcement, highlighting the struggle of translating policy into practice. Furthermore, the rapidly evolving nature of cyber threats has sometimes outpaced the adaptability of this legislative framework, emphasising the necessity for periodic revisions and updates. Moreover, while Nigeria has endeavoured to foster international collaborations to tackle cybercrime, there's also a palpable need to look inward. The evident lack of synergy among national agencies has sometimes hindered a cohesive and unified response. For the legislative and regulatory measures to be effective, it's recommended to strengthen the enforcement mechanisms and enhance inter-agency coordination. Moreover, the dynamic nature of cyber threats demands that the legal framework undergo continuous revisions to remain relevant and practical.

4.2.4.2 Technological and Infrastructure Measures

On the technological front, the vulnerabilities that permeate the Small and Medium Businesses (SMBs) sector stand out starkly. As gleaned from insights in 4.2.2.1, cybersecurity vendors have been sounding alarms about the pronounced susceptibility of SMBs to cyber threats. This concern is further accentuated considering the rapid digitisation the business world is witnessing. Additionally, the surge in the use of mobile devices coupled with the increasing reliance on online banking, as noted in social media analysis in 4.2.2.2, brings forth a new set of challenges. While offering convenience, these platforms have become hotspots for potential cyber-attacks, demanding robust and tailored technological solutions. To navigate these challenges, it's imperative to develop specific technological interventions that address the needs of SMBs. Simultaneously, there's a pressing requirement to build secure and resilient frameworks to safeguard mobile

transactions, ensuring both sectors are shielded from the myriad of cyber threats lurking in the digital realm.

4.2.4.3 Educational and Awareness Measures

In recent times, there has been a noticeable increase in public awareness regarding cybersecurity. This observation is supported by the findings from social media analysis detailed in section 4.2.2.2. Many individuals are becoming more knowledgeable about online threats and the need to protect themselves digitally. However, challenges remain. The rise of phenomena like "Yahoo Boys" and increased rates of cyberbullying suggest that not all segments of society are adequately informed or cautious.

To address these gaps, several strategies can be implemented. Utilising social media platforms, which already play a significant role in people's daily lives, can be an effective way to promote awareness campaigns. Additionally, engaging with community leaders and popular influencers can help relay important cybersecurity messages to a broader audience. Finally, including cybersecurity topics in school curricula will ensure that the younger generation is equipped with the knowledge to navigate the online world safely.

4.2.4.4 Economic Considerations

The economic implications of cybersecurity in Nigeria are significant. As mentioned in academic sources and confirmed by the Nigerian Communications Commission in section 4.2.1.2, the country faced a loss of around $550 million in 2020 due to cybercrimes. Such a substantial financial impact highlights the pressing need to strengthen cybersecurity measures. To mitigate such losses in the future, a multipronged approach is recommended. Investment in better cybersecurity infrastructure is crucial. It will protect against immediate threats and instil

confidence among investors and businesses. Public-private partnerships can also play a role. These collaborations can combine the resources and expertise of both sectors to develop and implement effective cybersecurity strategies. Lastly, offering incentives to businesses, especially smaller ones, to adopt stringent cybersecurity measures can provide additional layers of defence. When taken together, these measures can significantly reduce the economic toll of cybercrimes in Nigeria.

Evaluating existing cybersecurity measures and policies in Nigeria reveals a complex landscape with significant achievements and evident gaps and challenges. The findings from the data collected provide a multi-dimensional view of the situation, uncovering areas that require urgent attention.

Connecting back to the thematic analysis, the identified themes intertwine, reflecting the interconnected nature of cybersecurity's legislative, technological, educational, and economic aspects. To create a more secure cyber environment, Nigeria must pursue an integrated approach, weaving together these themes and addressing the identified shortcomings. The insights gleaned from the various sources - government documents, academic research, cybersecurity vendors, and social media - offer a robust foundation for crafting nuanced and effective strategies moving forward. By building on these insights, Nigeria can strengthen its cybersecurity architecture, protecting its citizens, economy, and future development.

4.3 ANALYSIS OF THE IMPACT OF CYBERCRIME ON NATIONAL SECURITY IN NIGERIA

The pervasiveness and complexity of cybercrime in Nigeria present significant challenges to the nation's security infrastructure. In an increasingly interconnected and digitised world, cybersecurity goes beyond the scope of individual protection and privacy and has broad implications for national security. The following analysis focuses on how cybercrime has influenced Nigeria's national security, emphasising the potential consequences, vulnerabilities, and challenges.

4.3.1 Potential Consequences

The potential consequences of cybercrime on national security in Nigeria are multifaceted, and they extend beyond the digital realm into the broader socio-economic and geopolitical context. Here is an in-depth look into these three crucial aspects:

4.3.1.1 Economic Impact

In Nigeria, the repercussions of cybercrime on the economy are profound, with the nation suffering financial setbacks of up to $550 million in 2020 alone. These ramifications permeate various segments of the economic landscape. Starting with businesses and individuals, they often bear the brunt of cybercriminal activities. Direct financial losses due to malicious activities like fraud, theft of funds, or infringement on intellectual property rights are common. Such setbacks can be particularly debilitating for small and medium-sized enterprises (SMEs), who might face the loss of assets and the burden of elevated cybersecurity expenses.

On a broader scale, the national economy suffers. When businesses experience losses, it naturally results in a decrease in revenue. This domino effect then leads to

reduced tax collections, which in turn hampers the government's fiscal capacity. The state's ability to channel investments into crucial public sectors, significantly those concerning security and defence, is compromised with diminished funds. Moreover, the overarching cloud of cyber threats casts a shadow on Nigeria's investment climate. Potential domestic and international investors might be hesitant or reluctant to pour capital into a market vulnerable to cyber-attacks. Such reluctance can stifle economic progress and technological innovation. As a result, Nigeria risks lagging in the digital transformation race, especially compared to nations that are more aggressively adopting and integrating digital technologies into their infrastructures.

4.3.1.2 Loss of Confidence in Digital Platforms

A rising concern in Nigeria is the eroding confidence in digital platforms, which has become more evident, with over 3,500 reported cybercrime incidents in 2019. Such a trend bears significant consequences for various stakeholders. From a consumer standpoint, this mistrust adversely affects their online behaviour. The scepticism surrounding the security of online services means that people are less likely to utilise digital platforms, whether it's for shopping, online banking, or accessing e-services provided by the government. This apprehension does more than restrict the individual's use; it can impede the nation's broader push towards digitisation. Such reluctance denies the populace the manifold advantages and conveniences of contemporary technology.

Businesses, too, are not insulated from the implications of this dwindling trust. When the digital landscape appears riddled with vulnerabilities, businesses might think twice before fully embracing digital avenues. Their hesitation to commit to digital transformation, driven by the fear of cyber threats, can put them, and by

extension Nigeria, at a competitive disadvantage on the global stage, where many economies are rapidly advancing their digital frontiers.

Furthermore, the government's vision and efforts are not immune to these challenges. A lack of confidence in digital platforms can curtail the government's ambitious plans to cultivate a thriving digital economy. Such sentiments can undermine e-governance strategies, making it difficult for the government to deliver services efficiently and innovate in line with technological advancements. Ultimately, this could lead to an economic landscape that is slow-moving and lacks the resilience and dynamism crucial in today's digital age.

4.3.1.3 Information and Intelligence Compromise

The unauthorised access and potential compromise of sensitive data stand at the forefront of threats to Nigeria's national security. The implications are profound and varied. A particularly worrisome aspect of this is the potential leakage of intelligence. When adversaries target core institutions such as intelligence agencies or military establishments, there's a risk that classified data could fall into the wrong hands. Such breaches might unveil Nigeria's defence strategies, giving hostile forces invaluable insights into the nation's preparedness and response mechanisms.

Moreover, the integrity of intelligence operations can come under severe strain. Cyber interventions in the processes of intelligence gathering, its subsequent analysis, and its dissemination can lead to severe disruptions. Such disruptions might hinder ongoing intelligence operations and pave the way for the spread of misinformation. This cloud of uncertainty can make the decision-making process at the highest echelons of government more challenging.

Lastly, these compromises provide adversaries with more than just data; they gain a strategic upper hand. By being privy to Nigeria's confidential information, these adversaries could undermine the country's geopolitical standing and clout. Such an

imbalance can detrimentally affect Nigeria in various domains, from diplomatic negotiations to forging international partnerships and asserting influence on global platforms.

The potential consequences of cybercrime in Nigeria are far-reaching and interconnected. The economic impact, loss of confidence in digital platforms, and compromise of information and intelligence are not isolated phenomena but reflect complex challenges. Together, they paint a picture of a nation grappling with digital threats that have the potential to undermine its economic stability, social trust, and national security integrity. Addressing these consequences requires a holistic and concerted effort, aligning economic, technological, social, and security strategies.

4.3.2 Vulnerabilities

The vulnerabilities in Nigeria's defence against cybercrime can be traced to three core areas: legal and regulatory gaps, technological infrastructure, and human resource and capacity constraints. Each presents unique challenges and collectively exacerbates the nation's susceptibility to cyber threats.

4.3.2.1 Legal and Regulatory Gaps

In 2015, Nigeria took a significant step forward in its approach to cybercrime by introducing the Nigerian Cybercrimes Act. The intention behind this legislation was clear and robust, but its practical enforcement revealed inconsistencies. This could be attributed to the mutable landscape of cyber threats, which demand a constantly evolving legal response. Eboibi and Ogorugba (2023) emphasise this point, asserting that laws, though essential, must adapt to the dynamic nature of the threats they aim to address. The complexity deepens considering the international dimension of cyber threats. As Andress (2014) points out, tackling these global challenges in isolated silos is flawed. The essence of his argument underscores the

need for a unified and collaborative strategy, both domestically and internationally. Effective cyber defence, therefore, is not just about individual nations like Nigeria adapting to rapidly mutating threats, a perspective shared by Goodman (2015), but also about synchronising efforts across borders to create a robust, collective defence.

Technological Infrastructure

While Nigeria's accelerated march towards digitalisation opens doors for socio-economic growth, it simultaneously exposes the nation to cyber vulnerabilities. Lewis (2018) aptly captures this situation by suggesting that technological progress can sometimes run ahead of protective safeguards. This is particularly evident in the mobile domain. The proliferation of mobile devices, each with its unique architecture and operating system, weaves a challenging web for cybersecurity, a sentiment echoed by Schneier (2015). Beyond just mobile threats, the digital environment of Nigeria, and indeed the world, is riddled with advanced cyber-attacks and malicious software. Zetter (2014) offers a profound understanding of these dangers, illustrating their potential to undermine the foundations of our digital society, particularly vital infrastructures.

4.3.2.2 Human Resource and Capacity Constraints

In the context of the digital era, having the right human resources is paramount in tackling cybersecurity threats. Like many countries, Nigeria faces significant challenges in acquiring specialised personnel to manage cyber threats' intricate dynamics. As Yaghmaei et al. (2017) noted, the cybersecurity workforce gap continues to widen globally, and countries must make strategic investments to bridge this divide. Furthermore, the technological armamentarium required to defend against cyber threats is vast and rapidly evolving. This is not merely about having technology; it's about having the right technology. Shackelford et al. (2016)

emphasise that even the most fortified cyber defences can be rendered obsolete without tailored technological tools that adapt to region-specific challenges. Lastly, it's not only technical specialists who need to be in the loop. The broader populace, spanning various sectors, needs a foundational understanding of cyber risks. Von Solms and van Niekerk (2013) affirm that cybersecurity awareness is paramount, as uninformed personnel can inadvertently become the weakest link in the cybersecurity chain.

The vulnerabilities faced by Nigeria in its battle against cybercrime form a complex web that intertwines legal, technological, and human resource factors. The gaps within these areas contribute to a landscape where cyber threats can thrive and evolve, posing significant challenges to national security. Closing these vulnerabilities requires a multifaceted approach that includes the following:

Regularly Updating Legal Frameworks: Ensuring that laws and regulations are aligned with current threats and technological advancements.

Enhancing Coordination Between Stakeholders: Promoting collaboration between government agencies, the private sector, and international partners to provide a united front against cybercrime.

Investing in Human Capital and Technology: Building capacity through education, training, technological investment, and public awareness campaigns.

By addressing these vulnerabilities strategically, Nigeria can fortify its defences against cybercrime, safeguarding its digital landscape and broader national security interests.

4.3.3 Challenges

The challenges in tackling cybercrime in Nigeria manifest in the intricate problems related to multi-agency coordination, public awareness and education, and adaptation to emerging threats. Addressing these challenges is essential for fortifying national security against the risks of cybercrime.

4.3.3.1 Multi-Agency Coordination

Effective management of cybersecurity threats necessitates seamless coordination among various responsible agencies. Cavelty (2014) insightfully discussed how a cacophony of diverse strategies often exacerbates the intricate realm of cybersecurity. Each agency, with its unique perspective and priorities, could approach the issue in its own way, leading to a maze of strategies that may or may not align. This fragmentation often results in inefficiencies, redundancies, and, at times, counterproductive efforts. Therefore, the absence of a singular, coherent strategy can seriously dilute the efficacy of response mechanisms.

As highlighted by many experts, communication remains the linchpin of effective cybersecurity operations. In her works, Nissenbaum (2009) underscores the role of transparent, timely, and efficient information exchange in bolstering security efforts. In situations where cyber threats evolve rapidly, delays in communication can cost dearly. A lag of even a few hours could escalate a minor threat into a full-blown crisis. Furthermore, the issue of jurisdictional overlaps cannot be sidestepped. Different agencies might, at times, find themselves stepping on each other's toes, leading to confusion and ambiguity. Brenner (2007) delves into this complex scenario, pointing out that the overlap can create operational challenges and legal quandaries without clearly defined boundaries. Effective response hinges on every agency understanding its domain and operating within its scope.

4.3.3.2 Public Awareness and Education

Public awareness of cybersecurity serves as the first line of defence against cyber threats. Furnell (2004) elaborates on the gap between general awareness and the ability to put that knowledge into actionable defence mechanisms. While the average individual might be aware of terms like 'phishing' or 'malware,' they may not necessarily know how to defend against such threats. This disparity can render even the most aware individuals vulnerable. Furthermore, the cyber landscape is littered with pitfalls, where seemingly harmless actions can invite threats. In their comprehensive research, Anderson and Moore (2006) emphasise how rudimentary lapses, such as using weak passwords or clicking on unverified links, can be gateways for cybercriminals. These threats don't just target individuals but can also compromise entire systems or networks if accessed through critical nodes.

To counter this, a 'one size fits all' approach to cybersecurity education is insufficient. Different demographics have different exposure levels, comprehension abilities, and vulnerabilities. Drevin, Kruger, and Steyn (2007) advocate for a more nuanced approach, emphasising the need for tailored campaigns. Such targeted initiatives are more likely to resonate, ensuring adequate comprehension and subsequent application by the recipients.

4.3.3.2 Adaptation to Emerging Threats

The dynamic nature of cyber threats requires an equally adaptive response mechanism. Tavani (2011) underscores the rapid mutation of cyber threats, which can quickly outpace conventional security measures. The inertia often seen in existing structures can provide cybercriminals with ample opportunities. Addressing threats that evolve almost daily requires a nimbleness that current bureaucratic systems might find challenging. Modifying policies to address these evolving threats is pivotal. Yet, as Solove (2008) highlights, the interplay between

policy-making and its practical application in cybercrime is fraught with challenges. Bureaucratic lags and the occasional lack of foresight can result in obsolete strategies even before implementation. Rapid, informed decision-making is essential to keep pace with the changing cyber landscape.

Comprehensive threat intelligence forms the bedrock of effective response mechanisms. Continuous monitoring, analysis, and interpretation of cyber threats can provide invaluable insights. Nissenbaum (2020) discusses the role of centralised intelligence in comprehensively understanding and effectively responding to cyber threats. Without a unified framework for threat analysis, nations might find themselves perennially on the back foot.

The labyrinth of challenges in Nigeria's cybercrime scenario cuts across various dimensions: coordination, awareness, and adaptability. To navigate this complex landscape:

- Enhanced Inter-Agency Collaboration is pivotal. As Deibert (2013) notes, fostering a collaborative environment, defining roles, and ensuring transparent communication can significantly bolster collective efforts in combating cybercrime.
- Robust Public Awareness Campaigns are integral. Whitman and Mattord (2011) elucidate on the transformative power of informed citizens, who can act as an essential line of defence against cyber threats, thereby complementing national efforts.
- Agile Policy and Strategy Development becomes indispensable. Clark and Landau (2011) stress the need for policies that can adapt in real-time, ensuring that the nation is perpetually equipped to counter emerging threats.

Nigeria must approach the cyber threat landscape with strategic forethought, adequate resources, and unwavering commitment to fortify its digital ramparts and protect national interests. Tackling these challenges is not merely about countering immediate threats but building a resilient and secure digital future.

4.4 COMPARISON WITH PREVIOUS STUDIES AND RESEARCH FINDINGS

The rigorous examination of cybercrime's impact on Nigeria's national security offers an invaluable juxtaposition with previous studies and scholarly insights. Analysing government documents reveals a significant transformation in Nigeria's approach to cybersecurity. Establishing the Nigerian Cybercrimes Act of 2015 marked a turning point in creating a legal framework (Federal Ministry of Justice, 2015). Although this was a significant step, the comparison with previous periods highlights an unmistakable evolution and underscores shortcomings, such as insufficient coordination (NITDA, 2015) and inconsistent enforcement (Nigerian Police Force, 2019).

Academic sources further illuminate this complex landscape. The "Yahoo Boys" phenomenon explored by Aborisade (2023) echoes the governmental focus on social engineering and online fraud. The findings from Afolaranmi (2023) regarding cyberbullying align with the broader concerns about cyber threats impacting individuals, especially youth. Eboibi (2017) assessment of legal responses mirrors the government's self-reflection on gaps in the legal framework. Similarly, Okonigene and Adekanle (2018) on economic implications correspond to the alarming $550 million loss reported by the Nigerian Communications Commission (2020).

Comparison with other regions, such as South Africa, as conducted by Gaillard (2021), provides a valuable context for evaluating Nigeria's unique challenges and

strategies within the broader African cyber landscape. The insights from Frank and Odunayo (2013) on Nigeria's global ranking further contextualise the national efforts within the international arena.

The perspective from cybersecurity vendors like Symantec enriches this analysis, offering an industry viewpoint that transcends academia and government. The alarming rise in Nigeria's global ranking from 66th to 59th (Symantec, 2012) aligns with the government's concerns but also emphasises unique industry-focused insights, such as the impact on Small and Medium Businesses (SMBs) and the role of mobile devices.

Finally, the social media analysis reflects the pulse of the public sentiment, resonating with the broader concerns and suggesting actionable paths forward. The call for more robust security measures, better education, and strict regulations on social media platforms mirrors the findings in government and academic research but adds a personal, citizen-centred dimension.

In essence, this comparative analysis paints a multifaceted picture of cybercrime in Nigeria, drawing connections and identifying disparities across government documents, academic research, industry insights, and public sentiment. The findings build upon previous studies, offering a synthesised, comprehensive understanding of Nigeria's cybersecurity landscape. The analysis creates a rich tapestry of insights by weaving together these diverse sources, highlighting progress and areas for targeted intervention and sustained effort. It emphasises the complexity of the task, revealing a nation on the cusp of significant transformation, grappling with a multifaceted challenge that requires collaboration across sectors, strategic planning, and public engagement. The echoes and contrasts across these sources validate the current work and pave the way for future research and action.

4.5 INTERPRETATION OF THE RESULTS

The interpretation of the results draws on the rich findings collected and examined in the previous sections. By connecting the raw data to theoretical frameworks, the interpretation paints a meaningful and comprehensive portrait of the findings in the broader context of Nigeria's national security and cybercrime landscape. Below, these insights are dissected in light of the research questions and objectives.

4.5.1 How Does Cybercrime Impact National Security in Nigeria?

The influence of cybercrime on Nigeria's national security has emerged as an area of critical concern in this work, in line with the main research question.

Economic Impact: To previous findings by Okonigene and Adekanle (2018), this work confirms the staggering economic effect of cybercrime on Nigeria. Losses amount to hundreds of millions, leading to profound national economic instability.

Social and Cultural Impact: Echoing observations by Aborisade (2023), the rise of cybercriminal subcultures like the "Yahoo Boys" has extended beyond mere criminality. Social trust is eroding, and the cultural implications are broad and deep, impacting national security.

4.5.2 What are the Sociological and Technological Factors Contributing to Cybercrime in Nigeria?

This section addresses the sub-question regarding sociological and technological factors, aiming to explore cybercrime's types and characteristics.

Sociological Factors: Unemployment, lack of education, and cultural acceptance of cybercrime are contributing factors, reflecting the observations of scholars like Sadegh (2018).

Technological Factors: Technological inadequacies, such as outdated cybersecurity infrastructure and a slow adaptation to emerging threats, are identified, supporting the broader conversation around technological contributions to cybercrime in Nigeria.

4.5.3 What are Nigeria's Current Cybersecurity Measures and Policies, and How Effectively Are They Combating Cybercrime?

Addressing the second sub-question and corresponding to the objectives of evaluating and assessing cybersecurity measures:

Government Initiatives: The work highlights efforts like the Nigerian Cybercrimes Act of 2015 but also finds gaps in enforcement and collaboration, as outlined by Eboibi (2017).

Private Sector Collaboration: The importance of engaging cybersecurity vendors and multi-stakeholder collaboration is emphasised, reflecting a growing consensus in the field.

Public Engagement and Education: The necessity of raising public awareness and education as proactive measures to combat cybercrime is underscored.

The interpretation of the results weaves together the multi-dimensional aspects of cybercrime, offering a robust understanding tailored to this dissertation's specific research questions and aims. By aligning theoretical frameworks with empirical findings, this work advances the understanding of cybercrime's influence on Nigeria's national security, the underlying sociological and technological factors, and the current measures and their effectiveness. The implications of this research resonate beyond academia, providing actionable insights for policymakers, industry stakeholders, and citizens. This work accentuates the need for a unified approach

encompassing legal, technological, social, and cultural considerations. It illustrates the urgent necessity for enhanced strategies and collaboration, positioning Nigeria within the global discourse on cybersecurity and offering a guide for future research and national resilience initiatives.

CHAPTER FIVE - DISCUSSION

5.1 INTERPRETATION OF THE RESULTS IN THE CONTEXT OF THE STUDY OBJECTIVES

The core of this work delves into understanding the dimensions of cybercrime within Nigeria and its implications for national security. Given the broad digital landscape and Nigeria's place in it, the results of this research shed light on the intricate relationship between cybercriminal activities and the nation's security framework. Here, the interpretation is structured around the main objectives:

5.1.1 Impact of Cybercrime Activities on Nigeria's National Security

The primary objective of this research sought to explore the ramifications of cybercriminal activities on Nigeria's national security. This segment delves deeply into this, elucidating the multifaceted repercussions of such illicit activities, informed by empirical findings.

1. **Economic Repercussions**

Delving into the economic intricacies, cybercrime has firmly entrenched its claws into Nigeria's financial fabric. Corroborating with Okonigene and Adekanle's (2018) insights, the work sheds light on the staggering economic magnitude of cybercrime's influence. With losses scaling to hundreds of millions, Nigeria's economic horizon faces a shadow cast by these illicit activities. This isn't merely a loss in numeric terms; the ripple effect spans sectors, influencing foreign investments, trust in digital economies, and even the broader perception of Nigeria in international financial markets. A destabilised economic landscape marred by cybercrime could lead to decreased investor confidence and potential threats to

macroeconomic stability. Consequently, as resources are diverted or become scarce, the nation's capacity to uphold and maintain its security infrastructure diminishes. This makes Nigeria susceptible to myriad threats, both from within its borders and beyond.

2. Sociocultural Dimensions

Cybercrime's tendrils have also reached the societal and cultural core of Nigeria. Echoing the observations of Aborisade (2023), there has been an evident shift in societal norms, particularly with the emergence and acceptance of cybercriminal subcultures, notably the "Yahoo Boys." Initially perceived as rebellious or fringe, these factions have seemingly woven their narratives into the broader cultural tapestry. The implications are far-reaching. Such groups, by glorifying cybercrime, erode foundational societal values. Trust, a cornerstone of cohesive societies, stands compromised. As individuals grow wary of each other, the societal fabric unravels, leading to fragmentation. In such a fractured setting, national unity and collective action against overarching economic, social, or security-related threats become daunting. This erosion of trust doesn't just remain confined within the nation but extends to international relationships, partnerships, and collaborations. If trustworthiness is questioned on the global stage due to prevalent cybercrime cultures, it has potential diplomatic and geopolitical repercussions.

3. Psychological Impact

Beyond economic and sociocultural implications, cybercrime's psychological toll on individuals and communities cannot be overlooked. Victims of cybercrime often face immense emotional distress, with feelings of violation, vulnerability, and distrust. Such distress can cascade into broader societal concerns, with heightened anxiety, scepticism about digital platforms, and reluctance to engage in the digital economy. This psychological dimension further adds complexity to the broader

national security concerns, as a society grappling with fear and mistrust can impede cohesive national strategies and initiatives.

5.1.2 Underlying Causes: Sociological and Technological Factors

The research's pivotal objective was to dissect the underpinnings behind the escalating presence of cybercrime in Nigeria. Delving deeper into this objective, this segment accentuates the intricate interplay between sociological drivers and technological gaps, each contributing to the cybercrime phenomenon.

1. **Sociological Drivers**

The socio-economic tapestry of Nigeria, woven with various challenges and intricacies, offers a magnifying lens into the motivators driving cybercrime.

- **Unemployment**: Nigeria, like many developing nations, grapples with unemployment. Despite being educated, a significant portion of its youth remains unemployed or underemployed. This demographic, brimming with potential, often finds itself at a crossroads. The allure of cybercrime, often perceived as a lucrative alternative, thus becomes enticing for many. This isn't merely a pursuit of wealth but, at times, a desperate bid for survival in a challenging economic milieu.
- **Education**: While Nigeria has made strides in its educational framework, gaps remain. Sadegh (2018) sheds light on the potential deficiencies in the educational realm. There's a twofold challenge here: firstly, a lack of awareness and education about the repercussions of cybercrime and, secondly, a potential mismatch between market demands and the skills imparted by educational institutions. The former leads to a lack of moral deterrence, and the latter feeds into the unemployment challenge.

- **Cultural Normalization**: The emergence and acceptance of cybercrime within specific cultural subsets, notably the "Yahoo Boys," underscore a worrisome trend. What was once deemed illicit and taboo has, over time, become a symbol of rebellion, success, or even aspiration for some. This cultural shift, where cybercrime is normalised and occasionally glamorised, fuels its proliferation.

2. Technological Gaps

Parallel to the sociological dimensions, technological factors cast their shadow on Nigeria's cyber landscape.

- **Rapid Digitization**: Nigeria, in its bid to embrace the digital age, has witnessed accelerated technology adoption. This rapid digitisation, spanning sectors from finance to health, has its set of vulnerabilities. With a vast populace coming online, often without adequate cyber hygiene awareness, the digital space becomes a fertile ground for cybercriminals.
- **Infrastructure Lags**: A stark finding from the research was the evident disparity between technological adoption and cybersecurity infrastructure. While businesses and individuals quickly adopt the latest technologies, security mechanisms lag. The nation's digital defences, thus, appear as brittle bulwarks against a savvy adversary.
- **Emerging Threat Landscape**: With an increasingly tech-literate population, the variety of cyber threats has also evolved. Cybercriminals have fine-tuned their arsenal from basic phishing attacks to sophisticated ransomware campaigns. Nigeria's challenge lies in addressing today's threats and preempting tomorrow's. This requires continuous investments, research, and collaboration.

The underlying causes of cybercrime in Nigeria are socio-economic challenges and technological vulnerabilities. Addressing them requires a nuanced, multi-pronged approach. Efforts should not merely be reactionary in addressing the aftermath of cybercrime but also preventive, tackling the root causes head-on

5.1.3 Evaluating Nigeria's Countermeasures Against Cybercrime

Addressing the escalating tide of cybercrime, the research aimed to meticulously evaluate the measures adopted by Nigeria in its bid to ensure cyber resilience. Through a comprehensive lens, this section delves into the nation's legislative architecture and the collaborative endeavours between public and private sectors, gauging their effectiveness and identifying potential areas of enhancement.

1. Legislative Efforts

At the heart of Nigeria's institutional response to cyber threats is its legal framework, which, in theory, sets the tone for its cyber posture.

- **The Nigerian Cybercrimes Act of 2015**: Instituted as a bulwark against the rising tide of cyber misdemeanours, the Act aimed to offer a robust legal response. As highlighted by Eboibi (2017), it underscores the country's recognition of the gravity of cyber threats and its commitment to curbing them. Yet, the proverbial devil lies in the details.
- **Implementation Hurdles**: While the Act is a commendable legislative endeavour, its translation into tangible results on the ground presents a different picture. The research illuminated gaps in its enforcement, implying that having a law in place isn't tantamount to its practical application. Factors like limited resources, training, and even bureaucratic inertia might play roles in this enforcement deficit.

- **Loopholes and Evolution**: As with many legal instruments, the dynamic nature of cyber threats means that laws need continuous updating to stay relevant. Specific provisions of the Act might already be obsolete or not cover newer forms of cybercriminal activities. The challenge lies in ensuring the legislation remains agile, adapting to the rapidly evolving threat landscape.

2. **Public and Private Collaboration**

The holistic fortification against cyber threats transcends governmental boundaries. Recognising this, the research underscores the integral role of non-state actors and public awareness campaigns.

- **Private Sector's Pivotal Role**: In a landscape where technology drives much of the economy, the private sector, especially cybersecurity vendors, emerges as a linchpin in the defence strategy. Their expertise, resources, and real-time insights into emerging threats can bolster national defences. However, fostering this collaboration requires trust, sharing of intelligence, and regulatory support.
- **Public Awareness and Proactivity**: An informed and vigilant citizenry is one of the most formidable defences against cyber threats. Shifting from merely reacting post-breach to preventing breaches requires disseminating knowledge on cyber hygiene, the modus operandi of cybercriminals, and promoting safe online behaviour. Public campaigns, workshops, and collaborations with educational institutions can play pivotal roles in this transformative journey.

While Nigeria has made commendable strides in structuring its defences against cybercrime, the journey is ongoing. The effectiveness of these countermeasures hinges on continuous evaluation, adaptation, and an inclusive approach that

harnesses the strengths of both state and non-state actors. It's a narrative of resilience, collaboration, and agility in the face of a mutable adversary.

5.2 Limitations of the Study and Future Directions

5.2.1 Limitations of the Study in Understanding Cybercrime and National Security in Nigeria

The quest to comprehend the nexus between cybercrime and national security, especially in the Nigerian context, is intricate and dynamic. While this work endeavoured to shed light on this multifaceted relationship, it is pivotal to recognise its inherent constraints, which define its scope and signify areas where further exploration might be fruitful. First and foremost, the work's focus was quite specific, emphasising the impacts, causes, and countermeasures of cybercrime in Nigeria. Although this offered a deep dive into Nigeria's unique challenges and context, it inadvertently circumscribed the broader global context. Cyber threats, after all, know no borders. They flourish within a tangled web of transnational networks, complex international laws, and the operations of sprawling multinational corporations. Simply put, by zeroing in on Nigeria, the research might have overlooked the vast interconnected ecosystem of cybercrime, which invariably has implications for Nigeria but operates on a far more expansive scale.

Additionally, the very nature of cybercrime presents challenges in data collection. The clandestine operations of cybercriminals, their use of dark web networks, and sophisticated anonymising techniques mean that the full breadth of cybercriminal activities likely remains hidden, lurking in the shadows of the digital world. The sensitivity of the topic adds another layer of complexity. Stakeholders might be reluctant to share data due to concerns about revealing vulnerabilities or the potential legal repercussions of such revelations. This hesitancy, paired with the

covert operations of cybercriminals, suggests that the work's data might only represent the tip of the iceberg.

A notable feature of the digital realm is its rapid evolution. In this fast-paced environment, today's state-of-the-art defences can quickly become tomorrow's obsolete technologies, and today's cutting-edge cyber threats might be outdated in the face of emerging technologies. This presents a formidable challenge for any research in the area. While relevant now, The work's findings are in a perpetual race against time, trying to remain pertinent in the face of the ceaseless advancement of cybersecurity measures and cybercriminal tactics.

Lastly, the cultural tapestry of Nigeria, with its myriad ethnicities, languages, and traditions, is a rich backdrop against which cybercrime operates. While the research made significant strides in understanding the sociological nuances of cybercrime within this tapestry, it's almost inevitable that some subtleties escaped its grasp. Nigeria's diversity means that cybercrime might manifest differently across its various communities, influenced by local beliefs, practices, and circumstances.

5.2.2 Future Directions in Cybercrime and National Security Research in Nigeria

In exploring the complex interplay between cybercrime and national security, it becomes apparent that understanding this issue is an ongoing journey filled with opportunities for further research. The recognition of the limitations of the present work opens the door to a range of future research directions that can enhance the comprehension of the cyber landscape in Nigeria and beyond.

Transnational Perspectives: Cybercrime is a borderless phenomenon often operating within extensive networks that cross national boundaries. Therefore, there is a need for future studies to consider perspectives beyond Nigeria,

incorporating regional and global viewpoints. Understanding the international dimensions of cybercrime reveals a broader array of challenges and opens up the potential for more comprehensive solutions. By examining how cyber threats function on the global stage, the responses at the national level can be better informed and more targeted.

Real-time Analyses: The digital world is characterised by rapid changes, with threats evolving at an unparalleled pace. Traditional research methods, although thorough, may struggle to keep up with this speed. Therefore, there is an urgent need for real-time analyses in cybersecurity. Using machine learning and artificial intelligence, future research can remain agile, continuously monitoring and assessing the cyber landscape. This approach ensures that strategies remain proactive and ahead of emerging threats.

Public Perception and Behavioral Studies: At its foundation, cybercrime is a human activity. While technological countermeasures are essential, understanding the human elements of this issue can provide invaluable insights. This requires an in-depth exploration of the psychological dimensions of cybercrime. What motivates individuals to become cyber criminals? How does the general populace perceive these threats, and what factors influence their online behaviours? By addressing these questions, future research can create countermeasures that tackle the root causes of cyber threats, making them more effective.

Policy Analysis and Recommendations: Policies such as the Nigerian Cybercrimes Act of 2015 form the groundwork for national defences against cyber threats. However, there is a need for continuous evaluation and improvement. Future research can play a pivotal role in this process, offering in-depth analyses of existing policies, identifying implementation gaps, and assessing their impacts. Furthermore, by studying international best practices, research can inform policy

recommendations that are globally informed and locally relevant to Nigeria's unique context.

Multi-disciplinary Approaches: The multifaceted nature of cybercrime necessitates an approach that is equally diverse in its perspectives. This calls for interdisciplinary research that combines insights from criminology, sociology, computer science, international relations, psychology, and more. Such an approach ensures a more comprehensive understanding, shedding light on how cybercrime intersects with Nigeria's society, technology, and geopolitics.

5.3 Implications for Policy and Practice

The findings of this work have significant implications for policy and practice in Nigeria, contributing valuable insights to the ongoing struggle against cybercrime and its impact on national security.

5.3.1 Policy Implications

1. Legislative Revisions: The current work has identified gaps in implementing the Nigerian Cybercrimes Act 2015. Policymakers should consider revisions to the legislation to address these gaps, providing more clarity on enforcement mechanisms and ensuring that penalties for violations are appropriate and serve as a deterrent to potential cybercriminals.

2. International Cooperation: Considering the transnational nature of cyber threats, Nigeria urgently needs to engage in global initiatives against cybercrime. Policymakers should partner with other countries and international organisations to share information, experiences, and best practices. Nigeria should consider acceding to international cybercrime agreements, such as the Budapest Convention on Cybercrime, to enhance international cooperation.

3. Multi-sector Collaboration: Policies should encourage collaboration between public and private sectors, including telecommunications companies, cybersecurity vendors, and financial institutions. A multi-sector approach is crucial to developing a comprehensive strategy to combat cybercrime, considering each sector's different perspectives and expertise.

4. Socioeconomic Interventions: The work highlights sociological drivers behind the surge in cybercrime, including unemployment and a potentially deficient educational framework. Policymakers should consider interventions to address these root causes, such as creating job opportunities and improving educational quality, which could help reduce the allure of cybercrime as a viable alternative for income generation.

5.3.2 Practical Implications

The findings of this work shed light on the pressing need for an integrated approach to tackle cybercrime in Nigeria, addressing technological gaps, enhancing professional capacity, promoting public awareness, and challenging the sociocultural factors contributing to the proliferation of cybercrime. First and foremost, enhancing cybersecurity infrastructure emerges as a critical area of focus. The research highlights that technological gaps in Nigeria's digital defences play a significant role in the rise of cybercrime. In response to this, practitioners in the field must prioritise the development of a robust cybersecurity infrastructure. This involves implementing advanced threat detection and response systems to guard against cyber threats effectively. By bolstering digital defences, Nigeria can create a formidable barrier against cybercriminals seeking to exploit technological vulnerabilities.

In addition to strengthening cybersecurity infrastructure, the need for continuous training and capacity building for cybersecurity professionals is evident. The ever-

evolving nature of cyber threats necessitates that cybersecurity professionals remain at the cutting edge of their field. Regular workshops, seminars, and certification programs can equip professionals with the knowledge and tools to effectively combat the latest cyber threats. These initiatives can enhance the skills and readiness of cybersecurity professionals, empowering them to defend Nigeria's digital landscape with more excellent proficiency.

Moreover, public awareness campaigns and education are indispensable in the fight against cybercrime. The work underscores their significance in shifting from a reactive to a proactive approach to cyber threats. Practitioners should prioritise implementing programs that educate the public on the risks associated with cybercrime, safe online practices, and the channels for reporting suspicious activities. An informed and vigilant public can become a valuable ally in detecting and thwarting cybercriminal activities, fostering a culture of collective responsibility and vigilance.

Lastly, the sociocultural dimensions of cybercrime must be addressed. Practitioners should engage community leaders, religious organisations, and civil society groups to challenge the normalisation of cybercrime. This can be achieved through awareness campaigns and community dialogues to shift cultural perceptions around cybercrime. By addressing these sociocultural factors, Nigeria can begin to root out the underlying drivers contributing to the prevalence of cybercrime in the country.

5.4 Recommendations

The dynamic interplay between cybercrime and Nigeria's national security has been a focal point of this research. Through a comprehensive examination of the implications, underlying causes, and countermeasures associated with cybercrime, the work has unveiled a multi-dimensional issue that demands nuanced solutions. The repercussions of cybercrime resonate not just economically but extend to the

very fabric of Nigeria's sociocultural tapestry. In the face of rapidly advancing technology and an increasingly digital society, Nigeria stands at a crossroads in its fight against cyber threats. In light of the empirical findings and comprehensive discussions encapsulated in this work, there are definitive steps and strategies that Nigeria should consider to fortify its cyber landscape and ensure national security. The following recommendations are rooted in the understanding that while the challenges are multifaceted, so are the solutions.

1. **Policy Revisions:** There's a pressing need to revisit and update the Nigerian Cybercrimes Act of 2015. While it stands as a testament to the nation's early recognition of digital threats, the evolving nature of cybercrime demands regular policy revisions. Updated regulations should address current challenges and anticipate future threats.

2. **Private Sector Collaboration:** Government bodies should foster closer collaborations with the private sector, especially tech companies and cybersecurity firms. Such partnerships can accelerate the development of cutting-edge cybersecurity solutions tailored to Nigeria's unique challenges.

3. **Education and Curriculum Integration:** Integrate cybersecurity education into the national curriculum. Students should have foundational knowledge about online safety and ethics starting from the basic educational level. This proactive measure can curb future cybercrime by instilling a culture of cyber awareness from a young age.

4. **Community Engagement:** Beyond top-down approaches, there's value in grassroots initiatives. Engaging local communities, traditional leaders, and influencers can ensure that cybercrime awareness permeates even the remotest parts of Nigeria. Addressing local myths and misconceptions about cybercrime can foster a collective stance against it.

5. **International Collaborations:** Given the transnational nature of many cybercrimes, Nigeria should actively pursue international collaborations. Sharing intelligence, resources, and best practices with other nations can fortify Nigeria's defences against global cyber threats.
6. **Establishment of Cybersecurity Task Force:** Form a dedicated task force or agency focused on cybersecurity. This body can oversee the nation's digital defences, conduct periodic threat assessments, and spearhead public awareness campaigns.

CHAPTER SIX

CONCLUSION

6.1 Conclusion

Navigating the convoluted landscape of cybercrime in Nigeria, this research unravelled the underlying sociological and technological factors driving this persistent challenge. The crux of the investigation revolved around the central question: "How does cybercrime impact national security in Nigeria?" In addressing this, the study delved into the multi-faceted impacts of cybercrime, ranging from the economic to the socio-cultural.

The economic ramifications of cybercrime were vividly evident, with Nigeria grappling with losses that soar into the hundreds of millions. This not only shakes the nation's financial stability but casts a shadow on its prospects for foreign investment. Coupled with this, the social fabric of the nation also stands compromised. The emergence and proliferation of cybercriminal subcultures, most notably the "Yahoo Boys", paint a picture of a society grappling with trust deficits and cultural shifts. These social changes are not isolated phenomena but are rooted in tangible sociological factors, such as unemployment and education gaps, further compounded by a cultural acquiescence towards cyber malfeasance.

On the technological front, Nigeria's cyber vulnerabilities emerge as a byproduct of its digital ambitions. The nation's impressive strides in broadband penetration and its burgeoning digital economy bring with them a set of unique challenges. Small and medium enterprises emerge as particularly vulnerable entities, often lacking the requisite defences or recovery blueprints to ward off cyber threats.

However, a landscape of challenges also presents opportunities for introspection and rectification. This research critically assessed the nation's cybersecurity stance,

underscoring the Cybercrime Act 2015. While this legal instrument symbolises Nigeria's intent to combat cyber threats, its efficacy remains hamstrung by implementation gaps and existing loopholes. This legislative assessment is further bolstered by a comprehensive exploration of the existing and potential strategies encompassing technology, public engagement, and international collaboration.

In essence, the research serves as both a mirror and a beacon. It reflects the current cybercrime state in Nigeria while illuminating the path ahead. The myriad of challenges underscored by this study emphasises the urgency of a cohesive and coordinated response. Policymakers, law enforcement agencies, the private sector, and the public must cooperate to chart a future where Nigeria's digital domain remains robust and resilient. The research adds to the corpus of knowledge on Nigerian cybercrime and seeds the grounds for further investigations. These findings will catalyse future academic endeavours and, more importantly, inspire tangible policy shifts that fortify Nigeria against tomorrow's cyber threats.

BIBLIOGRAPHY

A, A.D., U, A.A., J.b, E. and O.r, A. (2019). Challenges And Way Out Of Cyber Security Issues In Nigeria. *Villanova Journal of Science, Technology and Management*. [online] Available at: https://acjol.org/index.php/vjstm/article/view/1802/1747 [Accessed 10 Feb. 2023].

Abomhara, M. and Koien, G.M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*, 4(1), pp.65–88. doi:https://doi.org/10.13052/jcsm2245-1439.414.

Aborisade, R.A., 2023. Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of Parents' Disposition Towards Children's Involvement in Cybercrimes. *Deviant Behavior*, *44*(7), pp.1102-1120.

Adegbuyi, O., 2020. Understanding the Surge in Cybercrime: A Nigerian Case Study. *Journal of Cybersecurity Research*, 12(3), pp. 215-230.

Adeniyi, I.A. (2021). Cyber Security in Nigeria: Appraising Cybercrime, the Existing Legal Framework, the Challenges and the Way Forward. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.3991151.

Adepetun, A. (2018). Financial losses to cybercrimes on steady rise to N198b. *The Guardian Nigeria News - Nigeria and World News*. [online] 7 Jun. Available at: https://guardian.ng/technology/financial-losses-to-cybercrimes-on-steady-rise-to-n198b/ [Accessed 17 Apr. 2023].

Adomi, E.E. and Igun, S.E. (2008). Combating Cyber Crime in Nigeria. *The Electronic Library.*, 26(5), pp.716–725. doi:https://doi.org/10.1108/02640470810910738.

Afolaranmi, A.O., 2023. Chapter Seven Effects of social media on the peaceful coexistence of African people: A critical review. *Disruptive social media: Towards a resilient social media ecosystem in Africa*, p.93.

Akinyetun, T.S. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues,* 1(2), pp.86–109.

Alao, D., Osah, G. and Eteete, A. (2019). Unabated Cyber Terrorism and Human Security in Nigeria. *Asian Social Science*, 15. doi:https://doi.org/10.5539/ass.v15n11p105.

Alberts, D.S. and Papp, D.S. (2000). *Volume 2. Information Age Anthology: National Security Implications of the Information Age*. apps.dtic.mil. Available at: https://apps.dtic.mil/sti/citations/ADA461472 [Accessed 25 Apr. 2023].

Alghamdi, M. (2020). A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail Its Spread Worldwide. *International Journal of Engineering Research and Technology,* 9.

Anderson, R. and Moore, T., 2006. The economics of information security. *science*, *314*(5799), pp.610-613.

Andress, J., 2014. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Avant, D. and Sigelman, L. (2010). Private Security and Democracy: Lessons from the US in Iraq. *Security Studies*, 19(2), pp.230–265. doi:https://doi.org/10.1080/09636412.2010.480906.

Awhefeada, U.V. and Bernice, O.O. (2020). Appraising the Laws Governing the Control of Cybercrime in Nigeria. *JOURNAL OF LAW AND CRIMINAL JUSTICE*, 8(1). doi:https://doi.org/10.15640/jlcj.v8n1a3.

Babayo, S., Muhammad, Y., Usman, S. and Bakri, M. (2021). Cybersecurity and Cybercrime in Nigeria: the Implications on National Security and Digital Economy. 4, pp.27–61.

Baldwin, D.A. (1995). Security Studies and the end of the Cold War. *World Politics*, 48(1), pp.117–141. doi:https://doi.org/10.1353/wp.1995.0001.

Bello, M. (2018). *Investigating Cybercriminals in Nigeria : a Comparative Study*. [online] 1library.net. Available at: https://1library.net/document/y9mlr4jq-investigating-cybercriminals-in-nigeria-a-comparative-study.html.

Bernik, I. (2014). Cybercrime. *Cybercrime and Cyberwarfare*, pp.1–56. doi:https://doi.org/10.1002/9781118898604.ch1.

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

Brenner, S.W., 2006. At light speed: Attribution and response to cybercrime/terrorism/warfare. *J. Crim. L. & Criminology*, *97*, p.379.

Canongia, C. and Mandarino, R. (2012). *Cybersecurity: The New Challenge of the Information Society*. [online] Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions. Available at: https://www.igi-global.com/chapter/cybersecurity-new-challenge-information-society/60310 [Accessed 1 Dec. 2022].

Cavelty, M.D., 2014. *Cybersecurity in Switzerland*. Springer International Publishing.

Chukwu, E., 2019. The Rise of Cybercrime in Nigeria: An Analysis of the Underlying Factors. *International Journal of Cyber Criminology*, 7(2), pp. 125-142.

Clark, D.D. and Landau, S., 2011. Untangling attribution. *Harv. Nat'l Sec. J.*, *2*, p.323.

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, [online] 4(10). Available at: https://www.timreview.ca/article/835.

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, [online] 4(10). Available at: https://www.timreview.ca/article/835.

Creswell, J.W., 2014. *A concise introduction to mixed methods research*. SAGE publications.

Cusumano, E. (2015a). Bridging the Gap: Mobilisation Constraints and Contractor Support to US and UK Military Operations. *Journal of Strategic Studies*, 39(1), pp.94–119. doi:https://doi.org/10.1080/01402390.2014.1003638.

Cusumano, E. (2015b). The scope of military privatisation: Military role conceptions and contractor support in the United States and the United Kingdom. *International Relations*, 29(2), pp.219–241. doi:https://doi.org/10.1177/0047117814552142.

Cusumano, E. and Kinsey, C. (2015). Bureaucratic Interests and the Outsourcing of Security. *Armed Forces & Society*, 41(4), pp.591–615. doi:https://doi.org/10.1177/0095327x14523958.

Deibert, R.J., 2013. *Black code: Inside the battle for cyberspace*. Signal.

Dewar, R. 2014. 'the Triptych of Cyber Security: A Classification of Active Cyber Defense'. 6th International Conference on Cyber Security

Drevin, L., Kruger, H.A. and Steyn, T., 2007. Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, *26*(1), pp.36-43.

Eboibi, F.E. and Ogorugba, O.M., 2023. Rethinking Cybercrime Governance and Internet Fraud Eradication in Nigeria. *J. Legal Ethical & Regul. Isses*, *26*, p.1.

Eboibi, F.E., 2017. A review of the legal and regulatory frameworks of the Nigerian Cybercrimes Act 2015. *Computer law & security review*, *33*(5), pp.700-717.

Ekekwe, N. (2021). *The Updated Nigeria's National Cybersecurity Policy and Strategy*. [online] Tekedia. Available at: https://www.tekedia.com/the-updated-nigerias-national-cybersecurity-policy-and-strategy/ [Accessed 25 May 2023].

Falode, Adewunmi. (2021). Cybersecurity Policy in Nigeria: A Tool for National Security and Advancement.

Federal Bureau of Investigation. (2022). *Internet Fraud*. [online] Available at: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud.

Federal Ministry of Education. (2021). *National Cybersecurity Policy and Strategy 2021*. [online] Available at: https://education.gov.ng/national-cybersecurity-policy-and-strategy-2021/#18 [Accessed 27 Mar. 2023].

Frank, I. and Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution . *International Journal of Cognitive Research in Science, Engineering and Education*, 1(1), pp.100–110.

Frank, I. and Odunayo, E., 2013. Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education*, *1*(1), pp.100-110.

Furnell, S., 2005. Why users cannot use security. *Computers & Security*, *24*(4), pp.274-279.

Gaillard, A., 2021. Cybersecurity Challenges and Governance Issues in the Cyberspace'When Stronger Passwords Are not Enough: Governing Cyberspace in Contemporary African Nations' Case Study: Can South Africa and Nigeria Secure Cyberspace without a Lock? *Available at SSRN 3877526*.

Garba, A. and Bade, A. (2021). The Current State of Cybersecurity Readiness in Nigeria organizations. *International Journal of Multidisciplinary and Current Educational Research*, 3(1), pp.154–162.

Goel, P. (2019). *A Literature Review of Cyber Security*. [online] *IJRAR1CBP189 International Journal of Research and Analytical Reviews*. Available at: https://www.ijrar.org/papers/IJRAR1CBP189.pdf.

Goodman, M., 2015. Future Crimes A Journey To The Dark Side OfTechnology-And How To Survive It. *3ª ÉPOCA*, p.111.

Grabosky, P. (2015). Organized Cybercrime and National Security. *Cybercrime Risks and Responses*, pp.67–80. doi:https://doi.org/10.1057/9781137474162_5.

Halder, D. and Jaishankar, K., (2011). *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations: Laws, Rights and Regulations*. Hershey, PA, USA: IGI Global.

Handler, S. and Rowley, L. (2022). *The 5×5—Cybercrime and National Security*. [online] Atlantic Council. Available at: https://www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/#:~:text=%E2%80%9CCybercrime%20impacts%20national%20security%20in%20different%20ways%2C%20including [Accessed 24 May 2023].

Hassan, A.B., Lass, F.D. and Makinde, J., (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology*, *2*(7), pp.626-631.

Holmes, K.R. (2015). *What is National Security?* [online] The Heritage Foundation. Available at: https://www.heritage.org/military-strength-essays/2015-essays/what-national-security.

Ibikunle, Francis. (2013). Approach to Cyber Security Issues In Nigeria: Challenges And Solution.

Ibrahim, U. (2019). The Impact of Cybercrime on the Nigerian Economy and Banking System. *NDIC Quarterly*, 34(12), pp.1–20.

Idowu, O.A. (2021). Cybercrimes and Challenges of Cyber-Security in Nigeria. 3, pp.1–12.

International Telecommunication Union (2004), "Understanding Cybercrime: A Guide for Developing Country." Retrieved from http://www.itu.int/ITUD/cyb/cybersecurity/legislation.html

Iwenwanne, V. (2021). *More than email scams: the evolution of Nigeria's cyber-crime threat*. [online] The National. Available at: https://www.thenationalnews.com/world/africa/2021/07/22/more-than-email-scams-the-evolution-of-nigerias-cyber-crime-threat/.

Izuogu, S., 2017. Technological Factors in Nigeria's Cybersecurity Landscape. In: J. Okereke, ed. Cybersecurity in Developing Nations, 1st ed. *Springer*, New York, pp. 79-94.

Kinsey, C. (2012). *Contractors and War: The Transformation of United States' Expeditionary Operations*. Stanford University Press.

Ladan, M.T. (2015). Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.2680299.

Lewis, J.A., 2018. After the Breach: The Monetization and Illicit Use of Stolen Data.

Maglaras, L. and Janicke, H. (2022). *Cyber Security and Critical Infrastructures*. Mdpi AG.

Makeri, Y.A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), pp.315–321. doi:https://doi.org/10.23956/ijarcsse/v6i12/01204.

MOLOKWU, A.N., 2022. Socioeconomic predictors of cybercrime among Nigerian youths in Ibadan metropolis. *Turkish International Journal of Special Education and Guidance & Counselling ISSN: 1300-7432*, *11*(1), pp.61-68. Yaghmaei, E., van de Poel, I., Christen, M., Gordijn, B., Kleine, N., Loi, M.,

Morgan, G. and Weber, K., 2017. Canvas white paper 1–cybersecurity and ethics. *Available at SSRN 3091909*.

National Counterterrorism Center (2013). *Boko Haram*. [online] www.dni.gov. Available at: https://www.dni.gov/nctc/groups/boko_haram.html.

National Identity Management Commission, 2007. National Identity Management Commission Act, 2007.

Ndubueze, P. (2020). *Nature, Causes and Consequences of Cybercrime in Nigeria.* pp.60–80.

Nigerian Communications Commission, 2020. *Report on Cybercrimes Cost in Nigeria*. Abuja: Nigerian Communications Commission.

Nigerian National Information Technology Development Agency (NITDA), Year. *Annual Report*. Abuja: NITDA.

Nigerian Police Force, 2019. *Cybercrime Report*. Abuja: Nigerian Police Force.

Nissenbaum, H., 2020. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Norman, J. (2018). Book Review: Routledge Handbook of Private Security Studies. Edited by Rita Abrahamsen and Anna Leander. *War in History*, 25(2), pp.297–299. doi:https://doi.org/10.1177/0968344518760407k.

Nwanko, W. and Ukaoha, K. (2019). Socio-Technical Perspectives on Cybersecurity: Nigeria's Cybercrime Legislation in Review. *International Journal of Scientific & Technology Research*, 8.

Odumesi, J.O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3), pp.116–125. doi:https://doi.org/10.5897/ijsa2013.0510.

Odumesi, J.O., (2006). Combating the menace of cybercrime: The Nigerian Approach (Project). *Department of Sociology, University of Abuja, Nigeria*, p.45.

Ogunjobi, O. (2020). The Impact of Cybercrime on Nigerian Youths.

Ohwovoriole, O. (2019). "Nigeria Losses About N127bn to Cybercrime Annually." ThisDay. https://allafrica.com/stories/201906190144.html. Accessed March 25, 2020.

Ojedokun, U.A., 2018. Political and Social Dimensions of Cybersecurity in Nigeria. *Global Security and Intelligence Studies*, 4(1), pp. 50-65.

Ojukwu, C.C. and Shopeju, J.O., 2010. Elite corruption and the culture of primitive accumulation in 21st century Nigeria. *International journal of peace and development studies*, *1*(2), pp.15-24.

Oke, O.O. (2015). An Appraisal of the Nigerian Cybercrime (Prohibition, Prevention Etc) Act, 2015. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.2655593.

Okoli, A.C. (2022). *Nigeria insecurity: 2022 Was a Bad Year and Points to Need for Major Reforms*. [online] The Conversation. Available at: https://theconversation.com/nigeria-insecurity-2022-was-a-bad-year-and-points-to-need-for-major-reforms-194554.

Okonigene, R.E. and Adekanle, B., 2009. Cybercrime in Nigeria. *Business Intelligence Journal*, *1*(1), pp.93-99.

Olumide, A.O., Adams, P. and Amodu, O.K., 2016. Prevalence and correlates of the perpetration of cyberbullying among in-school adolescents in Oyo State, Nigeria. *International Journal of Adolescent Medicine and Health*, *28*(2), pp.183-191.

Onuoha, F. and Ogbonanya, M., 2019. Review and Analysis of Nigeria's National Security Strategy 2019. *Accountability Brief: a Policy on Nigeria's National Security Strategy*.

Onuoha, S. (2022). *Cyber Crimes : Nigeria Loses N200bn Every Year*. [online] Daily Business Update. Available at: https://businessupdate.com.ng/2022/01/20/cyber-crimes-nigeria-loses-n200bn-every-year/ [Accessed 7 Apr. 2023].

Osho, O. and Onoja, A. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *International Journal of cyber criminology*, 9(1), pp.120–143. doi:https://doi.org/10.5281/zenodo.22390.

Osho, O., Falaye, A. and Abdulhamid, S. (2013). Combating Terrorism with Cybersecurity: The Nigerian Perspective. *World Journal of Computer Application and Technology*, 1, pp.103–109. doi:https://doi.org/10.13189/wjcat.2013.010401.

Ovejero, A., Yubero, S., Larrañaga, E. and de la V. Moral, M., 2016. Cyberbullying: Definitions and facts from a psychosocial perspective. *Cyberbullying across the globe: Gender, family, and mental health*, pp.1-31.

Oyelere, S.S., Sajoh, D.I., Malgwi, Y.M. and Oyelere, L.S. (2015). Cybersecurity issues on web-based systems in Nigeria: M-learning case study. *2015 International*

Conference on Cyberspace (CYBER-Abuja), pp.259–264. doi:https://doi.org/10.1109/cyber-abuja.2015.7360510.

Perwej, Y., Qamar, A., Jai, D., Akhtar, N. and Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, 9, pp.669–710. doi:https://doi.org/10.18535/ijsrm/v9i12.ec04.

Rayes, A., and Salam, S. (2019). Internet of Things: From Hype to Reality. Geneva: Springer.

Ruzza, S. (2010). *Combattere. I dilemmi delle democrazie*. Bonanno.

Sadegh, S.M., 2018. The sociological study of the reasons for the youth tendency towards crime in cyberspace. *Journal of Advanced Pharmacy Education & Research*| *Oct-Dec*, *8*(S2), p.167.

Schiliro, F. (2023). Towards a Contemporary Definition of Cybersecurity. doi:https://doi.org/10.48550/arXiv.2302.02274.

Schneier, B., 2015. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Shackelford, Scott J., Timothy L. Fort, and Danuvasin Charoen. "Sustainable cybersecurity: Applying lessons from the green movement to managing Cyber Attacks." *U. Ill. L. Rev.* (2016): 1995.

Shea, S. (2021). *What is Cybersecurity? Everything You Need to Know*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/cybersecurity.

Singer, P. (2007). *Corporate Warriors: The Rise of the Privatized Military Industry*. *www.bing.com*. Cornell University Press.

Singh, R. (2021). A Review On Cyber Security. 8.

Solove, D.J., 2008. Understanding privacy.

Sule, B., Yahaya, M., Sambo, U. and Mat, B. (2021). Cybersecurity and Cybercrime in Nigeria: The Implications on National Security and Digital Economy. 4, pp.27–61.

Symantec; Cyber Threats: Nigeria Ranks 59th - Symantec; Symantec Fingers Explosive ICT Devt in Nigeria's Growing Cyber Threat by Prince Osuagwu (June 25, 2012)

Tanko, A. (2021). Nigeria's security crises - five different threats. *BBC News*. [online] 18 Jul. Available at: https://www.bbc.co.uk/news/world-africa-57860993.

Tavani, H.T., 2016. *Ethics and technology*. Wiley.

Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, *38*, pp.97-102.

Week, C. (2019). *Nigeria Lost $800m to Cybercrimes In 2018 – Report*. [online] www.nigeriacommunicationsweek.com.ng. Available at: https://www.nigeriacommunicationsweek.com.ng/nigeria-lost-800m-to-cybercrimes-in-2018-report/ [Accessed 3 Apr. 2023].

Whitman, M.E. and Mattord, H.J., 2011. *Principles of information security 4th edition*. Cengage Learning.

Yakubu, M.A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7, pp.315–321. doi:https://doi.org/10.23956/ijarcsse/V6I12/01204.

Yusuf, C.N.I.B. (2014). Cyber Threats and National Security in Nigeria: Challenges and Options. *NDC E-JOURNAL*, [online] 13(2), pp.131–146. Available at: https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/view/133/115 [Accessed 6 Nov. 2022].

Zetter, K., 2014. An unprecedented look at Stuxnet, the world's first digitalweapon. *Wired*.