JATSS
e-ISSN:2687-5861

Journal of Applied and Theoretical Social Sciences

JATSS, 2023; 5(4), 413-430

First Submission:11.02.2023
Revised Submission After Review:16.11.2023
Accepted For Publication: 29.12.2023
Available Online Since:31.12.2023

Review Article

Combatting the Threat of Cybercrime in Nigeria: Examining Current Laws and Policies

Lucy Tsado [a] Abiodun Raufu [b] Emmanuel Ben-Edet[c]& Doris Krakrafaa-Bestman[d]

Abstract

Cybercrime has been a major global criminological challenge in recent years. Regarded as one of the epicenters of international Internet fraud, Nigeria is gaining notoriety as a cybercrime hotbed. With the continuing advancement in technological innovations and the growth of terrorism in Nigeria, cyberattacks are also a continuing threat. Efforts to tackle the threat of cybercrime have mainly been ineffective. Even though the Nigerian government has introduced measures to tackle the danger posed by cybercrime to economic and social growth, the piecemeal approach it has used in the past has yielded no tangible results. In this paper, we argue that cybercrime cannot be confronted by the Nigerian government alone without a comprehensive, holistic approach, including international cooperation. We examined the various strategies employed by the Nigerian government to curb cybercrime and why cyber criminality has been a malignant tumor that has refused to subside. We also outline some policy measures and recommendations

Keywords: Nigeria, cybercrime policy, cybersecurity, cyberattacks, information and communications technology (Icts)

JEL Codes: K14, K24, K40, K42, P37, Z38

[a] Asst. Prof. Dr., Lamar University, College of Arts and Sciences, Beaumont, Texas/USA ltsado@lamar.edu , ORCID ID: https://orcid.org/0000-0002-1657-3693 (Corresponding Author)

[b2]Asst. Prof. Dr., Southern University and A&M College, Baton Rouge, Louisiana/ USA, abiodunraufu@yahoo.com, ORCID ID: https://orcid.org/0000-0002-8428-173X

[c] Asst. Prof. Dr., Clark Atlanta University, School of Arts & Sciences, W.E.B. Du Bois Department of Sociology & Criminal Justice, Atlanta, Georgia/ USA , eben-edet@cau.edu ,
ORCID ID: https://orcid.org/0000-0002-3465-1464

[d] Asst. Prof. Dr., Alabama A & M University, Huntsville, Alabama/ USA, doris.krakrafaab@aamu.edu, ORCID ID: https://orcid.org/0000-0001-5090-9587

JATSS
e-ISSN:2687-5861
Journal of Applied and Theoretical Social Sciences

JATSS, 2023; 5(4),413-430

İlk Başvuru: 11.02.2023
Düzeltilmiş Makalenin Alınışı: 16.11.2023
Yayın İçin Kabul Tarihi: 29.12.2023
Online Yayın Tarihi: 31.12.2023

Derleme Makalesi

Nijerya'da Siber Suç Tehdidiyle Mücadele: Mevcut Yasaların ve Politikaların İncelenmesi

Lucy Tsado [a] Abiodun Raufu [b] Emmanuel Ben-Edet[c]& Doris Krakrafaa-Bestman[d]

Öz

Siber suç, son yıllarda önemli bir küresel kriminolojik sorun haline geldi. Uluslararası İnternet dolandırıcılığının merkez üslerinden biri olarak kabul edilen Nijerya, bir siber suç yatağı olarak ün kazanıyor. Teknolojik yeniliklerde devam eden ilerleme ve Nijerya'da terörizmin büyümesiyle birlikte, siber saldırılar da devam eden bir tehdittir. Siber suç tehdidiyle mücadele etme çabaları çoğunlukla etkisiz kalmıştır. Nijerya hükümeti, siber suçların ekonomik ve sosyal büyümeye yönelik oluşturduğu tehlikenin üstesinden gelmek için önlemler almış olsa da, geçmişte uyguladığı parça parça yaklaşım somut sonuçlar vermedi. Bu yazıda, uluslararası işbirliği de dahil olmak üzere kapsamlı ve bütüncül bir yaklaşım olmadan siber suçla Nijerya hükümetinin tek başına mücadele edemeyeceğini savunuyoruz. Nijerya hükümeti tarafından siber suçları engellemek için kullanılan çeşitli stratejileri ve siber suçluluğun neden azalmayı reddeden kötü huylu bir tümör olduğunu inceledik. Ayrıca bazı politika önlemlerini ve tavsiyelerini de ana hatlarıyla belirtiyoruz.

Anahtar Kelimeler: Nijerya, siber suç politikası, siber güvenlik, siber saldırılar, bilgi ve iletişim teknolojisi (ICT'ler)

*JEL Kodlar:*K14, K24, K40, K42, P37, Z38

[a] Asst. Prof. Dr., Lamar University, College of Arts and Sciences, Beaumont, Texas/USA ltsado@lamar.edu , ORCID ID: https://orcid.org/0000-0002-1657-3693 (Corresponding Author)

[b2]Asst. Prof. Dr., Southern University and A&M College, Baton Rouge, Louisiana/ USA, abiodunraufu@yahoo.com, ORCID ID: https://orcid.org/0000-0002-8428-173X

[c] Asst. Prof. Dr., Clark Atlanta University, School of Arts & Sciences, W.E.B. Du Bois Department of Sociology & Criminal Justice, Atlanta, Georgia/ USA , eben-edet@cau.edu ,
ORCID ID: https://orcid.org/0000-0002-3465-1464

[d] Asst. Prof. Dr., Alabama A & M University, Huntsville, Alabama, USA doris.krakrafaab@aamu.edu, ORCID ID: https://orcid.org/0000-0001-5090-9587

Introduction

Combatting the Threat of Cybercrime in Nigeria

The advent of computers, the Internet and Information and Communications Technology (ICTs) are regarded as some of the greatest milestones of human civilization. The Internet and ICTs has transformed human society, enhancing economic and social interaction. The use of ICTs continues to grow as governments, organizations, and individuals depend on its capability to provide services, conduct business, and stay socially active. Unfortunately, technology can be a double-edged sword. Its advancement has given rise to the digital and information age while also wreaking unintended negative consequences and creating opportunities for cybercrime.

Cybercrime is a global phenomenon that requires complex solutions, having far-reaching consequences for global economy and security. While street crimes receive more attention than cybercrime, the scope of the economic damage to individuals, organizations, and governments by cybercrime cannot be underestimated. Global annual financial loss to cybercrime, according to Lewis (2018), in a study in conjunction with the Center for Strategic and International Studies (CSIS), and the global security software company McAfee, is estimated at nearly $600 billion, which is almost 1 percent of global GDP, up from $445 pre-2014.

The advent of cybercrime in Nigeria can be traced to efforts to align the Nigerian economy with global standard transaction models in the 1980s, involving transitioning the country's fledgling analog computing technology into the digital era. ICTs that facilitate these transactions, also enable cybercrime and Internet fraudsters who try to exploit the unsuspecting across the world. The influx of foreign investors to Nigeria, with an eye on Nigeria's vast market, fueled by its population of almost 200 million, provided fertile ground for cybercriminals to "rip off" people (Terwase et al., 2014). Being crimes of opportunity, cybercrime in Nigeria has generally morphed along with successive changes in technology and social media platforms. The ubiquitous and anonymous nature of the Internet allows people with nefarious intent to commit crimes distant from their location.

Cybercrime has no doubt given Nigeria a negative image. The Nigerian government is still perceived as ineffective in preventing cybercriminals from their nefarious activities or prosecuting them when they are apprehended. Furthermore, the nexus of cybercrime and terrorism is an emerging threat to Nigeria. While incidences of cyberterrorism have not yet been recorded in Nigeria, there is no telling what technological capabilities such groups have acquired or are planning to acquire. It is only a matter of time before they gain access to technology that will have far reaching economic and political consequences for the Nigerian populace as well as a negative image with regards to cybercriminality. Therefore, it is critical for Nigeria to examine the country's laws and policies guiding the use of technology, and recognize the need to update prevention of, and response to cybercrime.

This paper examines Nigeria's response to cybercrime to recommend further steps to address the country's policies. It is essential to address cybercrime policies and adopt stricter cybersecurity strategies in response as well as to prevent further cybercrimes. The distinction between cybercrime and cybersecurity is critical because while cybercrime is the use of information technological and ICT infrastructure to commit a criminal act, cybersecurity involves prevention and a response to cybercrimes. Cybersecurity involves all efforts to *prevent* cybercrimes from occurring; *detect* why, how, and where cybercrimes are happening; *respond* to and recover from incidences of cybercrimes and cyberattacks. This explanation is essential because in examining Nigeria's laws and regulations, the distinction between the two is not spelt out, and there is no emphasis on cybersecurity. Without an all-encompassing effort toward prevention, the situation is likely to worsen as the laws are reactionary rather than proactive. Therefore, it is essential that we examine why and how cybercriminals from Nigeria continue to evolve as a threat, as well as develop concise solutions to thwart their activities by strengthening laws so they address response, (investigation and apprehension), recovery and prevention.

Current Literature

According to Ogunwale (2020), there has been a global campaign against the growing threat of cybercrime especially in Nigeria's financial institutions, which, if not adequately handled, could lead to a lasting disaster for the national economy. Ogunwale further affirms that the Central Bank of Nigeria (CBN) bank verification number project has foiled the duplication of identity by criminals to commit fraud. Banks are desperate for help as NGN 203 billion has been lost to debit and credit fraud in the last 14 years, with some cases left unrecorded. Awoyemi, Omotayo, and Mpapalika (2021) acknowledge that in Nigeria, the high rate of unemployment, the quest for wealth among youths (by any means necessary), bungling security of personal devices, and the lack of effective cybercrime laws, have contributed mainly to the rise in the level of cybercrime and make it a serious problem for the country. Onuora, Uche, Ogbunude and Uwazuruike (2017) also claims that in the last few years, many criminal elements in Nigeria have been using these modern telecommunication networks, such as the internet and mobile phones, to commit all crimes that portray a terrible global image for the nation. Omodunbi, Odiase, Olaniyan, and Esan (2016) further attest to several universal phishing scams that are exponentially increasing. It has become one of the fastest-growing cybercrimes in Nigeria. Kovacs (2022) states that legislation in Nigeria itself is a crucial area. When it comes to finding ways to reduce different types of cybercrime, politicians, the general public, security professionals, and other academics should look to the research conducted by cybercrime scholars as the primary source of knowledge.

The definition of cybercrime, the extent of cybercrime, and the types of cybercrime prevalent in Nigeria are important for this policy review.

Definition of Cybercrime

There is no universal definition of cybercrime, mainly because it means different things to different people. It therefore depends on the context in which the term is being used. Cybercrimes evolve as technological developments improve, presenting new opportunities; hence definitions keep evolving. For instance, David Wall (2001) classified cybercrime into four main groups: cyber-trespass, cyber-deception/theft, cyber-pornography and obscenity, and cyber-violence. Wall stated that cyber-trespass involves unauthorized crossing of already established boundaries in cyberspace like software piracy. Cyber-deception/theft, on the other hand, consists of using cyberspace to steal or cause harm. A good example is identity theft using ICTs. Cyber-pornography and obscenity involve cases where sexually explicit materials are traded in cyberspace, example, child internet pornography or abuse. Cyber-violence consists of using cyberspace or ICTs to instigate violence that has an ensuing impact on people's lives; an example that suffices here is cyber-terrorism. Cyber-violence could be carried out by an individual or a social/political group against others. In the context of Nigeria, the definitions that fit the Nigerian cybercrime mold the best involve cyber-trespass and cyber-deception/theft, because they are the most common types of cybercrimes committed by Nigerian fraudsters. While researchers have not established the prevalence of cyber-pornography and cyber-violence in Nigeria, these areas should nevertheless be addressed through legislation. The prevalent and pervasive growth of terrorism across the world and Nigeria indicates cyberterrorism should be comprehensively addressed in the laws and policies of Nigeria.

Other researchers have also attempted to conceptualize cybercrime in various ways. According to Renu (2019), cybercrime refers to a wide variety of criminal activities involving the use of computers and Internet technology. Cybercrime can also be classified in three ways: crimes where a computer is the primary instrument of crime, crimes where a computer is attendant to the offense, and crimes where the crime target is a computer (Sarre et al., 2018). Indeed, McGuire and Dowling (2013) classified cybercrime into two types: "cyber-enabled" crime and "cyber-dependent" crime. Cyber-enabled crimes are traditional cybercrimes that are facilitated using a computer. This includes credit card fraud, identity theft, mail fraud, electronic information theft for profit, drug trafficking, voyeuristic activities, stalking, harassment, Internet scams, or other menacing behavior. Cyber-dependent crimes, on the other hand, are crimes that cannot take place without cyber-technology. For example, cybercriminals can use malware to cause extensive damage to databases of companies. They can cripple infrastructural facilities of countries using the ICTs. They can hack computers of individuals and agencies to steal, destroy, or distort information. The reason cybercrime poses a significant threat is perhaps the cybercriminals' ability to use ICTs to perpetrate terrorism and espionage (Sarre, 2017).Worse still, the ubiquitous nature of ICTs means attacks can be launched from remote locations worldwide by cybercriminals who are not necessarily adept in utilizing technology.

Yet still other scholars have postulated various definitions of cybercrime in their desire to establish a common ground. Hassan and colleagues (2012) defined cybercrime as a process that involves the use of computers and the Internet by individuals to commit crimes. It could also reasonably include a wide variety of criminal offenses and activities that can be narrowed down to any illegal actions directed through electronic operations targeting the security of computer systems and the data processed by them (Olayemi, 2014).

While no one description or perspective offers a better definitional fit than another, the various classifications demonstrate the difficulty of defining the term. Instead, it is perhaps necessary to focus on a particular perspective that explains cybercrime from a law enforcement perspective, focusing on jurisdiction and response. Therefore, one useful classification of cybercrime for criminal justice purposes was provided by Kremling and Sharp-Parker (2018). They argued that a definition of cybercrime should be addressed within the context of jurisdiction and the laws that address prevention and responses to the crime. In this light, categorizations and contexts are essential as they allow governments and law enforcement organizations to devise strategies and tactics to protect, prevent, respond, and recover from various types of cybercrime using definitions that are clearly spelt out with consequences for each offense.

Cybercrime Statistics and Data Collection

According to the Ninth Annual Cost of Cybercrime Study prepared by the Ponemon Institute and Accenture (2019), the risk value of the cost of cybercrime globally will be $5.2 trillion from 2019 to 2023. In recent years, Africa has become a hub of cybercrime activities, with Nigeria, in particular, as the most active country in this respect. But contrary to conventional wisdom, Africa is as much a victim of cybercrime as it is a hotbed of cybercriminals who target the rest of the world. In 2016, an estimated 24 malware incidents targeted Africa (Kshetri, 2019). According to Serianu, a Kenya-based IT business advisory company, African economies lost $3.5 billion to cybercrimes in 2017. With a loss of $649 million, Nigerian victims sustained the highest loss, followed by Kenya's at $210 million with South Africa losing $157 million (Kshetri, 2019). Unfortunately, Nigeria does not have a reliable data collecting strategy that determines an estimate of victims' actual loss to cybercrime, like the US Internet Crime Complaint Center (IC3), through which the FBI collects data about cybercrimes and alerts the public about different fraud schemes as well as emerging scams. The United Kingdom has Action Fraud, while Canada has an extensive cyber-reporting center based on the type of cybercrime. While all these are developed countries with advanced technological and investigative capabilities, Nigeria needs to create a similar fact-gathering, report-enabling, public alert system, and align itself with developed countries. From the FBI's 2018 and 2019 IC3 reports, no African country is listed among the top 20 victim countries except South Africa (FBI, 2018; FBI, 2019). If we are to go by Serianu's 2017 estimates in the report cited above, Nigeria should be listed in the FBI's top 20 victim countries alongside South Africa. Nigeria simply has not been effectively collecting data to monitor cybercrime activities.

Cybercrime Problem in Nigeria

With an estimated 200 million people, Nigeria has more than 100 million Internet users and an estimated 150 million mobile telecommunications subscribers (Orji, 2019). According to Renals and Conant (2016), unlike the high-technology complicated cybercrimes that take place in the more developed parts of the world, Nigerian scammers are better known for the traditional but effective cybercrimes such as phishing, hacking, malware attacks, electronic card fraud, Automated Teller Machine scams, identity theft, marriage scams, mail fraud, and lately, Business Email Compromise (BEC) fraud. However, this may no longer be the case as an examination Nigeria's recent National Cybersecurity Policy and Strategy (NCPS, 2021) report, identified seven emerging threats, including cybercrime. The other six are online child abuse, pandemic induced cyberthreats, online gender exploitation, cyber-terrorism, election interference and other cyber threats.

While Nigerian cybercriminals operate within and outside the country, their activities beyond the country's border are discussed quite frequently. For example, in 2019, America's Federal Bureau of Investigation (FBI) arrested several Nigerians involved in fraudulent activities and online scams, leading to a loss of $6 million and further potential losses of about $40 million (US Department of Justice, 2019). This resulted from joint operations between America's FBI and Nigeria's Economic and Financial Crimes Commission (EFCC) (Techxplore, 2019). In July 2020, another sting operation led to the arrest of some other scammers in Dubai who were engaged in BEC-type frauds, including a popular social media presence going by the nickname "Hushpuppie." These joint operations in recent times are worthy of mention although we have yet to see if these will lead to a reduction in cybercrime in Nigeria.

According to Ehimen and Bola (2010), one fertile area for cybercriminals known as "Yahoo-yahoo boys", in Nigeria has been the Nigerian stock exchange market, which they have abused since 2011. These activities have since grown into an epidemic that has had crippling effects on the Nigerian state. Okeshola and Adeta (2013) stated that Yahoo-yahoo boys fraudulently represent themselves as having goods to sell or fronting a deceptive loan scheme project. They may pose as fake businessmen to a financial institution where money can be loaned out to prospective investors. In this regard, a great many individuals and organizations have fallen victims to the fraud. These criminal acts are viewed as a two-way street (criminal and victim) fueled by both sides' greed. These acts involve electronic financial fraud (payment and settlement methods) popularly referenced as 419 (advance fee fraud) in

Nigeria, which has led to some scholars broadly defining it as a criminal act that covers information technology infrastructure, including illegal access or unauthorized access, constituting an illegal interception that involves technical resources of nonpublic transmission of computer data to, from, or within a computer system (Ehimen & Bola, 2010). Nigerian 419 fraudsters cut across diverse professions. Some armed with college degrees would typically prefer foreigners as their principal target. The reasons for the criminals' preference are evident, because of the difficulty in investigating or prosecution arising from differences in security and legal systems of countries and higher per capita income in the targeted countries (Mba et al., 2017).

Theoretical Perspective

Theoretical perspectives that allow cybercrime to thrive in Nigeria are also important to offer suitable responses to the problem by looking at *why* cybercrimes occur in the Nigerian realm, as well as *how* to prevent, respond, and recover from them.

Most of the acts of cybercrime that involve Nigeria are property crimes falling under cyber-trespass to cyber-deception/theft. To understand property crime, one must first understand some of the underpinning reasons as to why people steal from others, rather than make their own money. To understand that aspect of human behavior, we applied institutional anomie theory expounded by Steven Messner and Richard Rosenfeld (2007). Simply put, the theory, which is a macro-level perspective of Robert Merton's anomie theory, seeks to explain crime based on cultural pressure that is exerted on individuals to achieve culturally defined goals in a society with weak social institutions (Messner & Rosenfeld, 2007).

At the heart of the increasing poverty and crime rates in Nigeria is the state of anomie inflicted on society by governance failure to provide the basic minimum amenities to the citizenry. Poor leadership and weak social institutions, and the propensity by the administration to acquire political power for the sole purpose of wealth accumulation through the appropriation of public funds, have influenced the value system and legitimized wealth acquisition by fair or foul means. The socioeconomic challenges have led to a higher number of the population living in poverty. Unemployment and lack of legitimate means to make money have forced youth to look for illegitimate means to survive, including using ICTs to defraud victims. The traditional value system has been weakened as survival by fair or foul means has become the mantra. Worse still, this cultural norm built around the adulation of wealth has influenced a generation of younger Nigerians who have been led to believe that successful wealth acquisition by criminality is just a sign of smartness (Uzochukwu et al., 2019).

An explanation for *how* to prevent cybercrimes from occurring can be explained using Routine Activities Theory (RAT). RAT is a crime prevention theory, which states that crime can happen only when there are three factors present: an opportunity to commit a crime, a willing criminal, and the absence of a capable guardian (Cohen & Felson, 1979). Though RAT is typically applied in a physical realm, its application has been expanded to the cyber domain by various authors (Grabosky, 2001; Williams, 2010; Yar, 2005). In the case of Nigeria, the capable guardian to curb cybercriminals' access to victims is made possible through strategy, policy and laws, physical and logical protections, and citizen education about ICTs, which to date are mostly ineffective. In any case, most of the behavior to prevent cybercrime, especially those that affect individual victims, largely depends on the victims' actions. While there are willing participants (motivated offenders), their activities can be curbed by reducing opportunities to commit a crime using precautions such as standard cybersecurity principles and restrictions enforced by expanding the laws for apprehension and prosecution (capable guardian). However, if the government cannot enforce the apprehension as well as the prosecution of cybercriminals, then the creation of comprehensive laws and principles to govern the proper use of ICTs by Nigerians is impractical. Therefore, examining statutes to ensure they effectively reduce and restrict the incidence of cybercrime is essential.

Existing Laws

There are substantial and procedural legal provisions created by Nigerian legislation to fight cybercrime. This legislation includes the Nigeria Criminal Code Act of 1990, the Advanced Fee Fraud and Other Fraud Related Offences Act of 2006, the Evidence Act of 2011, the Corrupt Practices and Other Related Offences Act of 2000, the Economic and Financial Crimes Commission Act of 2004, and the Cybercrimes (Prohibition, Prevention, Etc) Act of 2015. It should be noted that the term "cybercrime" is not mentioned in some of these acts, because the acts were extracted from other legal statutes. This discussion is limited to statutes that have legal connotations to cybercrime and not the entire statutes or acts.

Criminal Code Act of 1990

This act explains the crime involving obtaining something of value by misrepresentation. The most prominent provision of the act is Chapter 38, which gives details about obtaining that valuable by false pretenses and cheating. Chapter 38 includes Sections 418 to 426; however, Section 419 is the most famous and relevant to cybercrime. Section 418 criminalizes misrepresentations, while the famous Section 419 focuses on criminalizing fraudulent behavior with the intent to steal property from another person (Criminal Code Act, 1990). Therefore, this act broadly addresses fraud rather than cybercrime specifically.

Advanced Fee Fraud and Other Fraud Related Offences Act 2006

The Advance Fee Fraud and Other Fraud Related Offenses Act of 2006 covers offenses related to cybercrime. Interestingly, studies on this subject show that this act is currently the only act in Nigeria apart from the Cybercrime Act that addresses cybercrime issues, specifically focusing on regulating Internet service providers and cybercafés. Under this act, offenses relating to cybercrime are stated in Part 1, Section 1 (1) (Advance Fee Fraud, and Other Fraud Related Offences Act 2006).

Evidence Act of 2011

This act provides for the admissibility as legal evidence of statements in a document produced by computers. The Evidence Act was amended in 2011 to make provisions for the admissibility of statements in documents produced by computers. Still, it was more substantive than procedural, because there was no legal structure on cybercrime, thus limiting the act's full effectiveness until the Cybercrime Act of 2015. Computer-generated documents are admissible under Part V, Section 84 (1), (Evidence Act, 2011).

Corrupt Practices and Other Related Offences Act 2000

The Corrupt Practices and Other Related Offences Act of 2000 mandated the Independent Corrupt Practices and Other Related Offenses Commission (ICPC) to address Nigeria's corruption. The act's goal was to prohibit corruption in Nigeria by ensuring that perpetrators of corrupt practices are punished as well as individuals who act as whistleblowers are protected. It works in tandem with the African Union Convention on Preventing and Combating Corruption and the United Nations Convention Against Corruption. It has three main duties: to enforce the apprehension and investigation of suspected reports of corruption, prevent corruption by correcting public systems that are susceptible to corruption, inform the public and build trust to enlist the public's aid in the fight against corruption. While this act has no direct connection with fighting cybercrime, it has joined the EFCC in strategizing against cybercriminals, among other financial perpetrators, to bring them to justice (ICPC, 2020).

Economic and Financial Crimes Commission Act 2004 (EFCC)

Part 11, Section 6 of the EFCC Act charges it with coordinating and enforcing economic crimes laws on crimes such as money laundering, advance fee fraud, computer credit card fraud, counterfeiting, and other such crimes. The EFCC is also in charge of preventing and eradicating financial and economic crimes through investigation (The Economic and Financial Crimes Commission Act, 2004). Apart from the legal provisions to combat cybercrime in Nigeria, the EFCC is also involved in this fight by monitoring the activities of internet cafés (Mutum, 2012).

Cybercrimes (Prohibition, Prevention, Etc) Act of 2015 (The Cybercrimes Act)

The Cybercrimes Act became effective on May 15, 2015, and obligates telecommunication operators, financial institutions, and private users to cooperate with the criminal justice system and the Nigerian Computer Emergency Response Team (ngCERT) (Okoh & Chukwueke, 2020). The Act is both substantive and procedural because it provides the legal procedure for the investigation, prosecution, and conviction of cybercrime occurring in Nigeria.

Some of the provisions of the Act include:

a) It gives the president the power to designate as critical infrastructure certain computer systems, networks, and information infrastructure vital to Nigerian citizens' national economic security and safety.

b) It also grants the president power to implement procedures and guidelines, as well as conduct audits in furtherance of that aim. Examples of systems, which could be designated as such, include transport, communication, and banking.

c) It permits the death penalty for an offense committed against a system or network that has been designated as critical national infrastructure of Nigeria that results in the death of an individual (among other punishments for lesser crimes).

d) If found guilty of unlawfully accessing a computer system or network, hackers are liable to a fine of up to N10 million, or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts by sending electronic messages or accessing and using data stored on computer systems.

e) It makes a case against those who commit identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million, or both a fine and imprisonment.

f) It specifically creates child pornography offenses, with punishments of imprisonment for a term of 10 years or a fine of no less than N20 million, or to both fine and imprisonment, depending on the nature of the offense and the act carried out by the accused persons. Offenses include, among others, producing, procuring, distributing, and possessing child pornography.

g) Its outlaws cyber-stalking and cyber-bullying and prescribes punishments ranging from a fine of not less than N2 million or imprisonment for a term of no less than 1 year, or to both fine and imprisonment, up to a term of no less than 10 years or a fine of not less than N25 million, or both fine and imprisonment, depending on the severity of the offense.

h) It prohibits cyber-squatting, registering, or using an Internet domain name with bad-faith intent to profit from a trademark's goodwill, belonging to someone else, or to profit by selling the name to its rightful owner. Individuals who engage in this are liable upon conviction to imprisonment for a term of no less than 2 years or a fine of no less than N5 million, or both fine and imprisonment.

i) It forbids the distribution of racist and xenophobic material to the public through a computer system or network (e.g., Facebook and Twitter). It also prohibits the use of threats of violence and insulting statements to persons based on race, religion, color, descent, or national or ethnic origin. Persons found guilty of this are liable upon conviction to imprisonment for a term of no less than 5 years or to a fine of no less than N10 million, or both fine and imprisonment.

j) It mandates that service providers shall keep all traffic data and subscriber information confidential, due to the individual's constitutional right to privacy and shall take appropriate measures to safeguard the data retained, processed, or retrieved.

k) It allows for the interception of electronic communication by way of a court order by a judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceeding (The Nigerian Cybercrime Act, 2015).

While these laws are suitable, the problem has been in implementation, especially in specific measures to ensure apprehension and prosecution of cybercriminals.

Discussion

It would appear that the main weapons to fight cybercrime and related offenses in Nigeria before the enactment of the Cybercrimes Act in 2015 were the Independent Corrupt Practice as well as other related offenses commission (ICPC), established in 2000, and the Economic and Financial Crime Commission (EFCC), which was established in 2004 (Olayemi, 2014). Of the two, EFCC has been the most active. Its primary mandate was preventing, detecting, investigating, and prosecuting cases of economic and financial crime in Nigeria (Obuah, 2010). The EFCC Act of 2002 was re-enacted in 2004. Within 2 years of its operation, the agency recovered over N100 billion (US$757 million) and arrested over 500 suspects for cybercrimes and other financial crime-related offenses (Nwoba & Nwokwu, 2018). These steps taken by the Nigerian government in curbing the threat of cybercriminals while also rebranding the Nigerian image are to be commended, but despite all the measures put in place to curb cybercrime, studies still show that cybercrime in Nigeria is on the rise, increasing 23% in 2016 and an alarming 54% in 2018 (Palo Alto Networks, 2019). As at date, accurate data collection on cybercrime in Nigeria is not easily accessible. Therefore, there is still an insurmountable amount of work that needs to be done.

It is obvious that current laws and policies are not enough. There is a need to further investigate why cybercrime is on the rise. There is also a need to re-examine how to prevent and respond to emerging threats by revisiting policies and legislation on cybercrime and cybersecurity. We agree with several authors who have made some suggestions that are helpful. Adesina (2017), explained that there is a dire need to ensure the effectiveness of the 2015 Cybercrimes Act. She further states that equipping Nigeria's intelligence agencies with the right skills and technology to facilitate detection as well as proper regulation and surveillance of cybercafes are important. Mohammed et al. (2019) also identified gaps among the criminal justice operatives and in knowledge of digital evidence applications, such as those used in the digital forensic field. Maitanmi et al. (2013) suggested that firms should secure their network information, and governments should ensure that their laws apply to cybercrime. They also recommended that all stakeholders should work cooperatively to strengthen legal frameworks for cybersecurity (Maitanmi et al., 2013). Odumesi (2014) called for the prompt passage of the 2013 Cybercrime Bill and the establishment of a National Computer Emergency Response Team (CERT) center for the monitoring, detection, and analysis of activities within Nigerian cyberspace. In response to this, the National Cybersecurity Policy (NCP) was written in 2014 which led to the passing of the Cybercrimes Act in 2015, and the establishment of the Nigeria Computer Emergency Response Team (ngCert) also in 2015. In addition, an update of the NCP (2014) was provided in 2021 by way of the National Cybersecurity Policy and Strategy (NCPS). All these are responses to Nigeria's cybercrime and cybersecurity problem. However, despite these measures the cybercrime rate in Nigeria keeps rising.

Definitions are essential when dealing with any crime. It is pertinent that all laws address cybersecurity as well as emerging threats. It is important that definitions of offenses capture all cybercrime possible, current, and emerging as well as the consequences for committing such offenses (Osho, 2020). An effective strategy is to update laws and policies periodically to address emerging technologies and crime as was stipulated in the NCP (2014). Finally, while most cybercrimes have a financial component, some go beyond having financial consequences and are a threat to the privacy, security and safety of the citizens and organizations. Therefore, Nigeria's cybercrime laws need to cover emerging threats like cyberterrorism, cyber-espionage, cyber-sabotage, cyberbullying, and social engineering crimes, to mention a few. The NCPS (2021) may have identified some of these threats, the problem lies in devising tactics for executing the implementation of identified strategies to deal with the problem (NCPS, 2021).

One major problem with addressing cybercrime in many jurisdictions has been the haphazard nature in which laws are created due to a slow reaction to the problem (Alexander, 2014). Therefore, the first step is to utilize a broader approach to address the issues that include prevention and response. This has partly been done by the establishment of the National Cybersecurity Policy (NCP) of 2014 which led to the establishment of the 2015 Cybercrimes Act and ngCert. However, there needs to be an update since the current laws and policies have failed to reduce cybercrime. Hopefully the NCPS (2021) is a step in the right direction. Issues of international/global cooperation, intelligence gathering and sharing, public awareness of cybersecurity and cybercrime, data collection strategies, some of which have been addressed in the NCP (2014) and updated NCPS (2021) document, need improvement by providing specific strategies for implementation. While the 2015 Cybercrimes Act covers issues on prosecution, policies regarding prevention and responses still need to be addressed.

Conclusions and Recommendations

The policy recommendations here are given understanding that the overall problems with rising cybercrime have other factors outside of itself that affect it. Therefore, we cannot suggest changes to cybercrime policy without examining macro level issues like poverty, education, training and awareness campaigns that affect cybercrime. It is with this in mind that we suggest changes in overall cybersecurity strategy, rather than looking at laws alone. We therefore make the following principal suggestions:

1. At a macro level, a poverty reduction strategy to combat cybercrime is necessary (Adesina, 2017; Muhammed, 2015). Many individuals, because of a lack of means and education, engage in cybercriminality. The Nigerian government needs to address social ills like poverty and the structural inequalities that allow criminal enterprises like organized

cybercrime to occur. Nigeria can in turn devise strategies to empower its youth through education, and investing in widespread training and awareness campaigns, targeting the general population, especially youth in cyber hygiene and prevention. Nigeria should use this opportunity to invest in educating and training the next generation of cybersecurity professionals in the country among other ways of providing employment for its citizens.

2. Nigeria's move to improve its cybersecurity strategy has been documented in the recent National Cybersecurity Policy and Strategy of 2021. This is a step in the right direction. However, the NCPS does not provide comprehensive strategies to address feasible implementation. Although the United States' Cyberspace Policy Review (CPR), was written in 2009, it appears to be more effective than Nigeria's 2021 NCPS. In their 2009 review, the United States developed critical initiatives (CPR, 2009), similar to the 8 pillars in Nigeria's NCPS. The United States' CPR (2009) initiatives were broken down into actionable items. For example, "Leading from the Top" was identified as one of the United States' strategies for dealing with cyberspace policy. For this strategy the CPR (2009) recommended that leadership for cyberspace be anchored in the Presidency signaling the seriousness of their stance on cyberspace issues. Furthermore, the policy detailed how this would be carried out. An example that suffices is since 2009, the United States has continued to build on their strategy leading to securing the United States' 2020 elections after the 2016 election threats. On the other hand while Nigeria's NCPS talks about governance, through its "Strengthening Cybersecurity Governance and Coordination" pillar, it seems to lack the commitment to make cybersecurity a top-driven government strategy. Rather one of its strategies for this pillar is recommending a Coordinator for cyberspace activities, without giving comprehensive details on how appointing a coordinator was going to drive cybersecurity policies. While this is still commendable, there is need for Nigeria's government and leadership to commit to driving cybersecurity strategy from the top to ensure that initiatives lead to effective tactics that will enable implementation of viable strategies,that can be turned into achievable goals.

3. A coordinated review of Nigeria's cyberspace and policy should also identify and address gaps in laws, policies and strategies and expound a more comprehensive effort in dealing with the cybercrime challenge. A comprehensive strategy should include updating the 2015 Cybercrimes Act, to comprehensively include or anticipate emerging crimes such as cyberterrorism, social engineering, and BEC. These strategies include new trends and techniques being used by cybercriminals as technology evolves. The 2015 Cybercrimes Act needs to include such provisions that broadly define emerging crimes. With Nigeria looking for investors in critical infrastructural sectors, it is pertinent for the country to provide measures to protect such infrastructure against attacks. The current laws are too general and do not comprehensively address the protection of critical infrastructure. Another imperative step is to improve investigative capabilities of policing agencies by training law enforcement officers through collaborations with foreign security agencies whose citizens are affected by cybercrime involving Nigerian citizens and vice versa. It is also essential to expand the capabilities of ngCERT to include coordination of cyber threats; enhance data collection capabilities and counterintelligence; and creating a comprehensive database that would enable seamless collaborative data sharing on cybercrime perpetration. While all these are listed in the NPCS, the actions that will lead to implementation need to be addressed in the policies. It may not be possible to completely stamp out cybercrimes for now.

While not all countries are on the same page when it comes to laws and extradition, many understand that they cannot prosecute cybercrime on their own. Therefore, they have made agreements/treaties on how to investigate, apprehend and prosecute cybercriminals. It is crucial that Nigeria align itself with countries that have advanced apprehension, investigative, and prosecution capabilities. Training of law enforcement personnel as well as combining resources can be a way to collaborate with other countries more advanced in fighting cybercrime. The advantage of this is it not only allows Nigerian law enforcement personnel to learn from their counterparts from other countries, but allows other countries to see Nigeria as willing to address the problem. The willingness to successfully apprehend and prosecute cybercriminals will also allow Nigeria to build trust with other countries, opening doors to collaborative partnerships, training opportunities, and economic growth from foreign and local investments. We have started to see evidence of these types of alignments with the apprehension of several Nigerian nationals in the past few months by a joint task force of Nigeria's EFCC and America's FBI as mentioned earlier. These sting operations that have involved this cross-country collaboration constitute a step in the right direction. Investigative powers should also be increased. As an example, in late 2019 and mid-2020, Nigeria's Economic and Financial Crimes Commission (EFCC) joined the United States to investigate and apprehend cyber fraudsters in both countries (a program called Techxplore). Such collaborations will help Nigeria bridge the data collection gap and ensure that the government is working in tandem with other countries to fight the danger of cybercrime. These types of investigations will show that Nigeria is willing to apprehend and prosecute cybercriminals.

References

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science*, *13*(4), 19–29.

Advance Fee Fraud and Other Fraud Related Offences Act 2006. Retrieved November 15, 2023, fromhttps://www.asianlaws.org/gcld/cyberlawdb/NG/Advance%20Fee%20Fraud%20and%20other%20Fraud%20Related%20Offences%20Act%202006.pdf

Alexander, C. (2014). The cybersecurity skills gap. *S.C. Magazine*. Retrieved April 15, 2020, from http://www.scmagazine.com/the-cybersecurity-skills-gap/article/385079/

Awoyemi, B. O., Omotayo, O. A., & Mpapalika, J. J. (2021). Globalization and cybercrimes: A review of forms and effects of cybercrime in Nigeria. *Internal Journal of Interdisciplinary Research and Modern Education. 7*(1), 18-25.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*,*44*,588–608.

Criminal Code Act Chapter 77, Laws of the Federation of Nigeria 1990. Retrieved November 15, 2023, from https://www.wipo.int/wipolex/en/text/218191

Cybercrimes (Prohibition, Prevention, ETC) ACT, 2015. Retrieved November 15, 2023, from https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

Cyberspace Policy Review (2009). Retrieved April 15, 2020, from https://irp.fas.org/eprint/cyber-review.pdf

Economic and Financial Crimes Commission (Establishment) Act 2004. Retrieved April 15, 2020, from http://www.vertic.org/media/National%20Legislation/Nigeria/NG_Economic_Crimes_Commission_Act_2004.pdf

Ehimen, O. R., and Bola, A. (2010), Cybercrime in Nigeria. *Business Intelligence Journal*, *3*(1), 93–98.

Evidence Act 2011. Retrieved April 15, 2020, from https://www.refworld.org/pdfid/54f86b844.pdf

Federal Bureau of Investigation. (2018). 2018 Internet Crime Report. Retrieved April 15, 2020, from https://pdf.ic3.gov/2018_IC3Report.pdf

Federal Bureau of Investigation. (2019). 2019 Internet Crime Report. Retrieved April 15, 2020, from https://pdf.ic3.gov/2019_IC3Report.pdf

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social and Legal* Studies, *10*(2), 243–249.

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology*, *2*(7), 626–636.

Independent Corrupt Practices and Other Related Offences Commission. The Establishment Act. (2020). ICPC.gov. Retrieved April 15, 2020, from https://icpc.gov.ng/the-establishment-act/

Kovacs, A. M. (2022). Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria: A Review, Analysis, and Evaluation. *Journal of Central and Eastern European African Studies*, *2*(1),68-81

Kremling, J., & Sharp-Parker, A. M. (2018). *Cyberspace, cybersecurity and cybercrime*. Sage.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 2(*2), 77–81. doi:10.1080/1097198X.2019.1603527

Lewis, J. A. (2018). Economic impact of cybercrime: At $600 billion and counting, no slowing down. Center for Strategic and International Studies. Retrieved April 27, 2020, from https://www.csis.org/analysis/economic-impact-cybercrime

Maitanmi, O., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Impact of cybercrimes on Nigerian economy. *The International Journal of Engineering and Science*, *2*(4), 45-51.

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th international conference on world wide web companion* (pp. 1301–1310). International World Wide Web Conferences Steering Committee.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, 75.

Messner, S. F., & Rosenfeld. R. (2007). *Crime and the American dream*. Wadsworth.

Mohammed, K., Mohammed, Y., & Solanke, A. A. (2019). Cybercrime and digital forensics: Bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(1), 56–63.

Muhammed, T. L. (2015). Overview of the 2015 legal and policy strategy on cybercrime and cybersecurity in Nigeria. SSRN. http://dx.doi.org/10.2139/ssrn.2680299

National Cybersecurity Policy (NCP), (2014).Retrieved May 20, 2022, from https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf

National Cybersecurity Policy and Strategy (NCPS), (2021). Retrieved May 20, 2022, from https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_ STRATEGY_2021.pdf

Nwoba, M. O. E., & Nwokwu, P. M. (2018). Appraisal of Economic and Financial Crimes Commission (EFCC) in the fight against corruption in Nigeria (2007–2017). *The Social Sciences, 13*(1), 94–95.

Obuah, E. (2010). Combating corruption in a "failed" state: The Nigerian Economic and Financial Crimes Commission (EFCC). *Journal of Sustainable Development in Africa, 12*, 27–53.

Odumesi, J. O., (2014). Combating the menace of cybercrime. *International Journal of Computer Science and Mobile Computing, 3*(6), 980–991.

Ogunwale, H. (2020). The impact of cybercrime on Nigeria's commercial banking system. *International Journal of Management and Business Studies*, *2*(3), 75-78.

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research, 3*(9), 98–114.

Okoh, J., & Chukwueke, E. D. (2020). The Nigerian Cybercrime Act 2015 and its implications for financial institutions and service providers. *Financial Worldwide*. Retrieved November 15, 2023, from https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its-implications-for-financial-institutions-and-service-providers

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116–125.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology*, *1*(1), 37-42.

Onuora, A. C., Uche, D. C., Ogbunude, F. O., & Uwazuruike, F. O. (2017). The challenges of cybercrime in Nigeria: an overview. *AIPFU Journal of School of Sciences (AJSS)*, *1*(2), 6-11.

Orji, U. J. (2019). Protecting consumers from cybercrime in the banking and financial sector: An analysis of the legal response in Nigeria. *Tilburg Law Review, 24(1),* 105–124. http://doi.org/10.5334/tilr.137

Osho, O. (2020). Towards the Review of Nigeria's National Cyber Security Policy and Strategy 2014. Retrieved April 20, 2021, from https://www.linkedin.com/pulse/towards-review-nigerias-national-cyber-security-policy-osho-ceh/

Palo Alto Networks. (2019). SilverTerrier: 2018 Nigerian Business Email Compromise. Palo Alto Networks, Unit 42. Retrieved April 20, 2021, from https://unit42.paloaltonetworks.com/silverterrier-2018-nigerian-business-email-compromise/

Ponemon Institute and Accenture. (2019). The cost of cybercrime: Ninth annual cost of cybercrime study, unlocking the value of improved cybersecurity protection. Ponemon Institute. Retrieved April 20, 2021, from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Renals, P., & Conant, S. (2016). Silverterrier: The next evolution in Nigerian cybercrime. Palo Alto Networks. Retrieved April 20, 2021, from https://www.paloaltonetworks.com/resources/research/silverterrier-next-evolution-nigerian-cybercrime

Renu, P. (2019). Impact of cybercrime: Issues and challenges. *International Journal of Trend in Scientific Research and Development, 3(*3). 1569–1572.

Sarre, R. (2017). Metadata retention as a means of combatting terrorism and organized crime: A perspective from Australia. *Asian Journal of Criminology*, *12*, 167–179.

Sarre, R., Lau, L. Y. C., & Chang, L. Y. C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research: An International Journal, 19(*6), 515–518.

Techxplore. (2019). FBI and Nigeria step-up cyber-crime investigations. Retrieved April 20, 2021, from https://techxplore.com/news/2019-09-fbi-nigeria-step-up-cyber-crime.html

Terwase, I. T., Abdul-Talib, A. N., & Zengeni, K. T. (2014) Nigeria, Africa's largest economy: International business perspective. *International Journal of Management Sciences, 3*(7), 534–543.

US Department of Justice. (2019). Massive international fraud and money laundering conspiracy detailed in federal grand jury indictment that charges 80 defendants. U.S. Attorney's Office, Central District of California. Retrieved February 21, 2021, from https://www.justice.gov/usao-cdca/pr/massive-international-fraud-and-money-laundering-conspiracy-detailed-federal-grand-jury

Uzochukwu, C., Chukwuemeka, O. D., & Egbegi, F. R. (2019). An exploratory study of cybercrime in the contemporary Nigeria value system. *European Journal of Social Sciences Studies, 4(*3). https://oapub.org/soc/index.php/EJSSS/article/view/565

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the internet* (pp. 1–18). Routledge.

Williams, M. (2010). The virtual neighbourhood watch: Netizens in action. In Y. Jewkes & M. Yar (Eds.), *Handbook of internet crime* (pp. 562–581). Willan.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.

Information About the Article/Makale Hakkında Bilgiler

The Ethical Rules for Research and Publication / Araştırma ve Yayın Etiği

The authors declared that the ethical rules for research and publication followed while preparing the article.

Yazarlar makale hazırlanırken araştırma ve yayın etiğine uyulduğunu beyan etmiştir.

Conflict of interests/ Çıkar Çatışması

The authors have no conflict of interest to declare.

Yazarlar çıkar çatışması bildirmemiştir.

Grant Support/ Finansal Destek

The authors declared that this study has received no financial support.

Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

Author Contributions/ Yazar Katkıları

The draft process of the manuscript/ Taslağın Hazırlanma Süreci L.K.T./A.R./E.B.E./D.K.B., Writing The Manuscript/ Makalenin Yazılması L.K.T./A.R./E.B.E./D.K.B., Submit, Revision and Resubmit Process/ Başvuru, Düzeltme ve Yeniden Başvuru Süreci L.K.T./E.B.E.