Nigeria's Cybercrime Landscape: Examining the Trends, Patterns and Impacts of Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) 2024

Peter Timi Omimakinde*

Abstract

Cybercrime is a pervasive and complex issue that encompasses a broad spectrum of illicit activities, posing significant threats to individuals, governments, and organizations worldwide. Its far-reaching impacts result in devastating consequences, including business collapse, reputational damage, hindered financial growth and even loss of life. In response to these threats, Nigerian lawmakers enacted Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (hereinafter called 'the Principal Act') aimed at curbing these illicit activities. Despite the existence of the Principal Act, cybercrime continues to rise, evolving into new trends and patterns that render the Principal Act inadequate. To address the inadequacies in the Principal Act, the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 (hereinafter called 'the Amended Act') was signed into law. Using doctrinal method, this paper therefore examined the innovations introduced by the amended act to the Principal Act, specifically as it relates to the emerging trends and patterns of perpetrating cybercrimes. The paper further discussed the various trends and patterns of cybercrimes and its effect on Nigeria's national development. The research revealed that the innovations in the amended Act has broadened the scope of electronic documents and its admissibility in any proceedings in Nigerian Courts or Tribunals. It is accordingly observed that a fairly adequate regulatory framework has been provided to combat cybercrimes in Nigeria. However, the lack of resources and institutional challenges may greatly impede the full enjoyment of the innovations in the amended Act. In view of these, this paper concluded by pontificating on veritable recommendations, which include that the law enforcement agencies be equipped with updated skills, knowledge and insight for effective fight against cybercrimes. It additionally calls for a comprehensive interpretation of cybercrimes and the establishment of Electronic Document Verification Department (EDVD) for effective implementation of the amended Act.

Keywords: Cybercrimes, Cyberspace, Trends, Patterns, Impacts,

1. Introduction

The advent of technology has transformed the world into a global village, bridging geographical divides and making economies accessible through electronic means via the internet and computer. The computer, an innovation that surpassed people's imagination at the time, only revealed its significance after its invention. Notably, Thomas Watson, IBM's former chairman, predicted in 1943 that the world market could only support five computers.[1] While debates surrounding the definition of a computer and the number of generations developed continue, it is widely accepted that the first electronic digital computer was invented in the 1940s, during the final years of World War II.[2]

Human developments or improvements in information and communication technology (ICT) has led to the information being represented into electronic or digital format which has led to the rapid demand of free, open and global access to information by its users. However, the rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activities, but has also given rise to new patterns of criminal activities. These developments pose significant challenges for legal systems and law enforcement agencies[3] to curtail.

As the global population becomes increasingly computer-literate and computing technologies advance, Nigeria has come under international scrutiny for its involvement in cybercrime, ranking among other countries with the highest e-crime rates. According to the World Cybercrime Index,

* **Peter Timi Omimakinde** B.L., LL.M. A Doctoral Degree Candidate, Faculty of Law, University of Jos, Jos Plateau State, Nigeria. Email: omimakindepeter@gmail.com/omimakinde@nigerianbar.ng, Tel: 08066906557

[1] J L Xingan, 'Cyber Crime and Legal Countermeasures: A Historical Analysis', *International Journal of Criminal Justice Science*, Vol. 12 Issue 2 (2017), 196.

[2] D Hamilton, '*Technology, Man and the Environment*', (London: Faber and Faber, 1973), p 82.

[3] Brenner, S., '*Law in an Era of Smart Technology'*, (London: Oxford University Press, 2007). p 374.

Nigeria ranks as the leading country in West Africa for cybercrime and is positioned fifth (5th) globally.[4]

Nigeria is experiencing a surge in internet usage, accompanied by a rising tide of internet facilitated crimes.[5] These crimes encompass various pattern, including identity theft, desktop counterfeiting, cyber harassment, fraudulent emails, ATM spoofing, pornography, piracy, hacking, inheritance or wills fraud, phishing and spamming; posing significant threats to citizens' personal data and becoming increasingly common.

Cybercrimes, as in the past, involve both computers and individuals as victims, with one being the primary target. For simplicity, we will consider the computer as either a target or a tool. Hacking, for instance, involves attacking a computer's information and resources. However, today, cybercrime has advance to the use of other digital technologies, including phones, POS, ATM, etc, all of which can operate with or without the use of computer in perpetrating cybercrimes. The perpetrators and victims of cybercrimes come from diverse backgrounds, highlighting the challenges in arresting, prosecuting and punishing cybercriminals.

Thus, the easy access to the internet, facilitated by the liberalization of the telecommunications sector, contributes to the rise in cybercrime, and cybercriminals show no respect for individuals, targeting people regardless of age, ethnicity, disability, gender, religion or socioeconomic status. This has become a significant threat to country's e-commerce growth, tarnishing its's reputation and hindering opportunities for law abiding citizens abroad. [6] An organized group, such as Black Axe, have been linked to cyber financial fraud, employing social media, online dating sites, and emails to deceive victims.[7] Similarly, a recent crackdown by Portuguese authorities dismantled a Nigerian network involved in money laundering and recruitment of money mules across Europe, identifying over 25 suspects[8] and uncovering substantial transfers to Nigeria bank accounts from seized computer and phones.[9] Moreover, an INTERPOL[10] shed light on Black Axe's extensive cybercrime operations, highlighting a notable case in which Canadian authorities uncovered a $5 billion money-laundering scheme linked to the group in 2017[11]

[4]World Cybercrime Index, 'Overall-Top 15 Countries', retrieved from https://www.researchgate.net/figure/World-Cybercrime-Index-overall-top-15-countries_tbl1_379729675 accessed on January 5, 2025

[5] As at mid-2023, Nigerian Communications Commission Report reveals that internet penetration in the country stood at 47.36% with over 92 million active internet users. See www.punchng.com/identity-for-sale-how-hackers-breach=security-steal-data-of-vulnerable-nigerians/%3famp accessed on January 6, 2025.

[7] The Arrest of More than Seventy Members of Black Axe by INTERPOL, retrieved from https://cyberjustice.blog/2023/01/27/the-arrest-of-more-than-seventy-members-of-black-axe-by-interpol/ , see also; www.channelstv.com/2024/08/28/nigeria-interpol-arrests-over-300-members-of-dreaded-criminal-group-black-axe/amp/ accessed on December 26, 2024

[8]Channels, 'Interpol Arrest 300 Members of Black Axe, Others' retrieved from www.channelstv.com/2024/08/28/nigeria-interpol-arrests-over-300-members-of-dreaded-criminal-group-black-axe/amp/ accessed on December 26, 2024

[9] Ibid

[10] Also known as the International Criminal Police Organisation, is an inter-governmental organization which reunites 195 countries and fights against Cybercrime, Counter-terrorism and Organized emerging crime.

[11] Interpol Arrest 300 individuals connected with Black Axe, Nigerian-Founded Confraternity' retrieved from Nairametrics.com/2024/08/28/Interpol-arrests-300-individuals-connected-with-black-axe-nigerian-founded-confraternity/%3famp=1 accessed on December 26, 2024

It is undeniable that cybercrime has a profound impact on a country's economic growth and its effects cannot be overstated. The internet can thrive if there is adequate legal framework regulating the users, including the service providers who often than not are accused of aiding and abating the cybercriminals. Internet has a global application and demands global solution. However, prosecuting cybercrime has proven to be a daunting task, much like unraveling a "Gordian Knot". Meanwhile, Crime and criminality have been present throughout human history. Crime remains elusive and ever strives to hide itself in the face of development. Nations, including Nigeria have developed strategies to address crime based on its nature and extent. Nigeria recognized the importance of safeguarding its digital infrastructure against cyber threats and in response to growing demands for a legal framework, alongside public confidence in the internet's benefits, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015[12] was signed into law on May 15, 2015 by the Former President - Goodluck Ebele Jonathan to combat the trending patterns of cybercrime.

Despite the enactment of the Principal Act, cybercriminals continue to evolve, exploiting new patterns and loopholes. The persistent threat has prompted legislators to review the Principal Act, addressing its shortcomings to better combat the ever-changing landscape of cybercrimes. In this regard, the legislator amended the Principal Act and on February 28, 2024, President Bola Ahmed Tinubu signed the Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act 2024[13] into law; comprising 13 sections, which amended 11 sections of the Principal Act. The amended Act clarify ambiguous provisions; address inadequacies and overcome implementation obstacles. It also bolsters Nigeria's cybersecurity framework, combat terrorism and violent extremism, enhance national security, and protect Nigeria's economic interests.[14]

Given the trends and patterns of cybercrimes, it becomes essential to examine the innovations introduced by the amended Act as well as its effects on national development.

Meaning of Cybercrimes

1. Cybercrimes

A primary problem for the examination of cybercrimes is the lack of a consistent and statutory definition for the activities that may constitute cybercrimes.[15] The Principal Act (i.e, Cybercrimes Act 2015) does not explicitly provide a comprehensive definition of cybercrime. However, according to Gupta and Agrawal; "cybercrimes are computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic network".[16]

The definition described above focuses on computer-meditated activities that are illegal or considered illicit, conducted through global electronic networks. Whereas, cybercriminals have begun to exploit phones and other internet-enabled devices to commit cybercrimes, making it possible to initiate these crimes without the need for computers. For instance, according to the data submitted to Nigeria Inter-Bank Settlement System (NIBSS) by financial institutions through the Industry Fraud Reporting Portal, it reveals that the mobile channel is the preferred means for fraud.

[12] Hereinafter referred to as "The Principal Act"
[13] Hereinafter referred to as "Amended Act"
[14] O Duale, & A Adedipe, 'The Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024 – A Primer on Key Amendments retrieved from https://www.doa-law.com accessed on January 10, 2025
[15]M Yar, 'The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory', *Eur. J. Criminol*. 2(4): 2005, 407-427.
[16]D Guptar, and T Agrawal, '*Cyber Laws'* (India: Premier Publishing Company) p 54.

It additionally reveals that the web and POS businesses were the most exploited payment channels by fraudsters in 2023.[17] The word 'cybercrime' is a series of organized crimes that take place in cyber space and not necessarily with the use of computer. Cyber space is also known as the internet.[18] The evolving nature of cybercrime, marked by a shift from computer-based offenses to the use of mobile phones and other devices, underscores the necessity for a revised and more comprehensive definition of cybercrime, specifically one that accurately reflects the changing landscape of this illicit activity. Hence, it is submitted that cybercrime refers to a broad range of criminal offenses committed by individuals or groups using internet connectivity and electronic devices to target individuals, public entities or corporate organizations with the intention of obtaining unlawful benefits or causing harm.

Cybercrime is considered one of the fastest growing crimes globally. Criminals are increasingly exploiting the internet's speed, convenience and anonymity to commit various borderless crimes. These crimes cause serious harm and pose significant threats to victims worldwide[19]

Trends and Patterns of Cybercrimes

Cybercrime can involve computers or other digital technology devices as agents, facilitators or targets. Crimes can occur solely online or in combination with physical locations. Cybercrime patterns include but not limited to Hacking, Identity theft, Cyber Stalking/Bullying**,** Inheritance fraud**,** cyber terrorism, Phishing attack, Cyber Pornography, cyber defamation, Malware distribution, Ransomware attacks, Doxxing, Trolling, Catfishing, Business Email Compromise and Cryptojacking. This article will discuss a few of these patterns.

1. **Hacking/Unauthorised Access**

The term 'hacking' encompasses various meanings. In a cybersecurity context, it specifically refers to unauthorized access, alteration or manipulation of computer systems or data. However, hacking can also involve modifying devices or system for improvement, without illicit intentions.[20]

Recent incidents in Nigeria illustrate the severity of hacking by some of the users of Flutterwave, a digital payment system, valued at $3billion in its latest fundraising.[21] In the cause of investigation, it was found that users who had not activated some of the Flutterwave's recommended security settings had been susceptible. Additionally, healthcare data breaches have occurred in Nigeria, such as the incident where hackers accessed medical records at private hospital, Abuja, demanding for ransom to prevent publishing sensitive information. This pattern

[17] Punch Newspaper: Bosun Tijani, 'Calls For Stronger Regulations Intensify Amid Rising Identity Theft', retrieved from https://punchng.com/calls-for-stronger-regulations-intensify-amid-rising-identity-theft/ accessed on December 24, 2024

[18] The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers)

[19] . http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime accessed on December 27, 2024

[20] D Halderand, & K Jaishankar, '*Cybercrime and the Victimization of Women Laws, Rights, and Regulations'*, (Washinton: Hershey, PA, (2011) 98

[21] Coingeek, 'Nigerian Fintech Giant Flutterwave Loses $6.4M in Hack, and Traders are Feeling the Heat', retrieved from https://coingeek.com/nigerian-fintech-giant-flutterwave-loses-6-4m-in-hack-and-traders-are-feeling-the-heat/ accessed on January 10, 2025

of cybercrime involves system compromise, security bypass and unauthorised data access.[22] Such crime is characterised by unlawful interception of inbound and outbound data by hackers.

2. Identity Theft and Catfishing

Both identity theft and catfishing involve deception and misrepresentation. While identity theft occurs when an individual or corporation impersonates another person or corporation to commit fraud for financial gain, catfishing occurs when someone on the internet creates a fictitious identity for the purpose of starting a relationship.[23] For clarity, catfishing occurs online and takes the form of romantic or social manipulation and creating a false identity, while identity theft can occur online or offline with the aim of stealing an existing identity for financial or material gain. An example of catfishing is the popular case of Manti Te'o, a football star, who was catfished by his girlfriend.[24]

Thus, when identity theft happens online, it is called online identity theft. Identity theft is a prevalent cybercrime that takes place in cyber space and has cost Nigerians over N25.5 billion in just four years.[25] Section 4 of the amended Act broadens the scope of identity theft to accommodate public and private organizations.

Statistics for year 2023 reveals that 748% of internet users in Nigeria suffered internet-related attacks, including identity theft[26] and a report estimated that about 0.8% (i.e., 127 billion naira) of Nigeria's Gross Domestic Product (GDP) was lost to cybercrimes, which includes identity theft[27]. Prominent cases of identity theft include that of a Lagos based civil servant which was reported to have lost over N3million to a fraudulent bank transaction. Investigations revealed that the fraudsters had obtained her bank details through a phishing email disguised as legitimate communication.[28] Similarly, Chukwuemeka Onyegbula, a Nigerian citizen was indicted by a Federal Grand Jury in Seattle for conspiracy to commit wire fraud and aggravated identity theft.[29]

Common sources of stolen identity information include data breaches on government, federal[30] or private websites. A recent investigation by Paradigm Initiative (PIN), a digital rights advocacy

---

[22] Ashaolu, O. & Oduwole, A., '*Understanding Information Technology Law Through the Cases*' (Lagos: Freedom Press) 2010, p. 98

[23] O Savage, and A Ashiru, 'The Protection of Women Against Cyberstalking and Cyber-Harassment in Nigeria, England and the United States: An Appraisal of the Legal Framework', *Journal of International Law and Jurisprudence*, (2021) Vol. 7 No. 1, 164.

[24] Ibid

[25] Vanguard Newspaper, Identity Theft Hits Nigeria Hard' retrieved from www.vanguardngr.com/2024/09/identity-theft-hits-nigeria-hard/ accessed on January 12, 2025

[26] Sumsub Fraudlympics, 'Nigeria, China and Indonesia Take Medals in Global Graud', retrieved from https://sumsub.com/newsroom/sumsub-fraudlympics-2024-nigeria-china-and-indonesia-take-medals-global-fraud-leaderboard/ accessed on December 28, 2024

[27] Africannews, 'Nigeria loses Over $430m Annually to Cybercrime' retrieved from www.africanews.com/2016/07/20/nigeria-loses-over-430m-annually-to-cybercrime/ accessed on December 29, 2024

[28] Punch, 'Identity For Sale: How Hackers Breach Security, Steal Data of Vulnerable Nigerians' retrieved from www.punchng.com/identity-for-sale-how-hackers-breach-security-steal-data-of-vulnerable-nigerians/%3famp accessed on January 10, 2025

[29] Oversight.Gov., 'Nigerian National Indicted in Washington State for Fraud on Covid-19 Economic Relief Programs' (June 24, 2021), retrieved from https://www.oversight.gov/nigerian-indicted-washington-state-fraud-covid-19-economic-relief-programs accessed on January 10, 2025

[30] C J Hoofnagle, 'Identity Theft: Making the Known Unknowns', *Harvard Journal of Law and Technology*, Vol. 21, (2007) 113

group, uncovered the shocking sale of Nigerians' personal data, including financial details and National Identification Numbers, on a private website known as 'XpressVerify.com.ng' for as little as N100. Although, the website was promptly taken down, the incident prompted further investigations and a public interest lawsuit filed at the Federal High Court in Abuja against NIMC & 8 others.[31] These breaches can expose sensitive information like credit card numbers, addresses, email ID's, etc. to perpetrate identity theft.

3. Cyber Stalking/Bullying

Cyber stalking/bullying involves the use of electronic devices, such as cell phones, computers, or tablets, with internet connectivity to repeatedly harass, bully or threaten someone. Stalking on the other hand can take many forms, including harassment, blackmail and sexual exploitation and can be motivated by anger or other factors. The amended Act expands the definition of cyberstalking to include sharing pornography[32] or false information with the intent to bully, annoy or disrupt public order. In contrast, the Principal Act defined cyberstalking more broadly as "grossly offensive, indecent or of an obscene and menacing character." This reflects the evolving landscape of digital communication and its potential consequences.[33]

In this digital age, people have a lot of information on various networks on the internet, making them vulnerable to online stalking. Recent technological advancements have led to many people joining social media networks. Cyberstalking occurs on the internet or through other electronic means, involving harassment or stalking of individuals, groups or organizations. This can also include false accusations, defamation, slander, libel, vandalism, solicitation for sex or gathering information to threaten or harass a person.[34] Accordingly, people easily become victims of stalking. Stalking and blackmail are increasing due to the rapid growth of the internet. Recently, a Federal High Court sitting in Lagos sentenced a TikToker identified as Okoye Blessing Nwakaego to three (3) year imprisonment or a fine of One Hundred and Fifty Thousand Naira for cyberstalking (i.e., social media bullying) Nollywood actress - Eniola Badmus through a social media app called 'TikTok'.[35]

4. Cyber Terrorism

Cyber terrorism involves premeditated, politically motivated attacks on information systems, computer, programs and data. These attacks, often carried out by subnational groups or clandestine agents, can result in violence against non-combatant targets, including death, injury, explosions or severe economic loss.[36]

---

[31] Ibid (n. 28) See also Paradigm Initiative, 'Major Data Breach: Sensitive Government Data of Nigeria Citizens Available Online for Just 100 Naira' retrieved from https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizen-available-online-for-just-100-naira/ accessed on January 6, 2025

[32] Section 23 of the Principal Act captures all forms of pornography.

[33] L Hamu, 'Highlights of Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024' retrieved from https://hamulegal.com/highlights-of-cybercrimes-prohibition-prevention-etc-amendment-act-2024/ accessed on January 10, 2025

[34] B H Spitzberg, & G Hoobler, "Cyberstalking and the technologies of interpersonal terrorism", *New Media & Society*. 1. 4: 71–72.

[35] Channels TV., 'Court Sentences Lady to Three Years in Prison for Cyber-Stalking Eniola Badmus' retrieved from www.channelstv.com/2023/08/02/court-sentences-lady-to-three-years-in-prison-for-cyber-stalking-eniola-badmus/amp/ accessed on January 10, 2025.

[36] Ibid

A notable example of cyber terrorism is the case of Farouk Abdulmutallab, also known as the "Underwear Bomber". In 2009, Abdulmutallab attempted to detonate explosives on a flight from Amsterdam to Detroit, putting 290 lives at risk. Although the bomb partially detonated, passengers and crew intervened, thereby preventing a larger disaster.[37] Abdulmutallab was convicted of terrorism-related charges and sentenced to life imprisonment.[38]

Cyber terrorism can also involve attacks on critical infrastructures, such as large-scale disruptions of computer networks using malware, viruses or physical attacks. These acts, also known as electronic terrorism or information war, target individuals, governments and organizations.[39] exploiting the increasing reliance on technology and the internet in daily life.

5. **Spam and Phishing**

Spamming and phishing are common cybercrimes patterns that have become prominent due to technological advancements. Spam refers to unwanted emails and messages, while phishing involves cybercriminals offering bait to obtain sensitive information. A common growing trend in phishing involves sharing money with social media commentators who complete specific tasks, ultimately aiming to deceive individuals into revealing confidential data.

Phishing baits can take various patterns, such as business proposals, lottery announcements or promises of easy money. Phishing has several variants, including tab nabbing, tab jacking, vishing and smishing.[40] In 2023, a phishing attack targeted multiple Nigerian banks, resulting in the theft of millions of naira from customer accounts. Investigation revealed that the hackers had exploited weak authentication protocols.[41]

Spamming involves sending identical messages indiscriminately to numerous recipients on the internet. This is sometimes referred to as email bombing[42] also known as electronic junk mail or junk news group postings. This is because spam is used to spread computer viruses, Trojan horses or other malicious software, with the objective of identity theft. However, phishing is the most common pattern of spamming, involving emails that falsely claim to be from a legitimate enterprise. The goal is to scam users into surrendering private information.

Phishing emails direct users to visit a website, where they are asked to update personal information, such as passwords, credit card numbers, social security numbers and bank account numbers. Legitimate organizations already possess this information.

It is estimated that as much as 80% of all the emails sent are spam. This staggering statistic highlights the significant waste generated by spam. Many people wonder why spammers bother,

[37] U.S. Immigration and Customs Enforcement, 'Underwear Bomber Umar Farouk Abdulmutallab Sentenced to Life.' Retrieved from https://www.ice.gov/news/releases/underwear-bomber-umar-farouk-abdulmutallab-sentenced-life accessed January 10, 2025

[38] Ibid

[39] Available at https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/assessed 04/05/ 2024

[40] "Types of Cybercrime Acts and Preventive Measures". Retrieved from http://www.thewindowsclub.com/types-cybercrime. Assessed on accessed on 4th May 2024.

[41] Ibid (n. 28)

[42] A O Ayub, & L Akor, 'Trends, Patterns and Consequences of Cybercrime in Nigeria', *Gusau International Journal of Management and Social Science, Federal University*, Vol. 5, No. 1 (2022) p. 246

given the low response rate. However, even a tiny percentage of responses can generate a profit due to the low cost of sending bulk emails.[43]

6. Cyber Defamation

Cyber defamation is a growing concern, fuelled by the ease and speed of spreading defamatory statements online. Defamation refers to any false statement that harms the reputation of an individual, business, product, group, government, religion or nation. To constitute defamation, a statement must be false, made to someone other than the person defamed and result in injury to their reputation. [44] The vast nature of the internet allows such statements to spread globally within seconds, which is one of the crimes cybercrime laws seeks to curb. Although, the provisions appear to be targeted towards Journalist. In Nigeria, at least, 29 journalists have faced prosecution under the Principal Act since it was enacted and as at October 2024, report from CPJ reveals that more Journalists are facing prosecution.[45]

Defamation can take two forms: slander (spoken defamation) and libel (written defamation).[46] Thus, slander refers to oral defamation while libel refers to written defamation. Online publications intended to ridicule someone can be considered internet defamation. Internet libel knows no borders; someone in Nigeria can publish defamatory content about someone in another country. Defamatory content can be altered or deleted and perpetrators may remain anonymous.

7. Cyber Pornography

The internet's rapid growth has unfortunately led to a significant surge in pornography distribution. Cyber pornography, which involves creating, displaying, distributing, importing or publishing explicit materials online, has become a major concern. The rise of online pornography has overtaken traditional content, with internet publications increasing exponentially.[47] This phenomenon has created jurisdictional challenges due to the internet's lack of boundaries, high traffic and potential anonymity. As a result, controlling online content has become increasingly difficult, with service providers often bearing the blame.[48] Moreover, the posting of pornographic content by children is on the rise, and child pornography has become a lucrative and devastating criminal enterprise.

---

[43]H Simon, 'Spot the Difference - Spam and Phishing Scams' retrieved from http://www.brighthub.com/internet/security privacy/articles/63828.aspx accessed on December 26, 2024

[44]B Ishabakaki, 'Defamation In Social Media (Cyber Defamation) Legal Perspective In Tanzania' retrieved from https://www.linkedin.com/pulse/defamation-social-media-cyber-legal-perspective-benedict-ishabakaki. accessed December 26, 2024

[45] CPJ., 'Nigeria Police Charge 4 Journalist with Cybercrimes for Corruption Reporting', retrieved from https://cpj.org/2024/10/nigeria-police-charge-4-journalists-with-cybercrimes-for-corruption-reporting/ accessed on January 13, 2025

[46]E Bingireki, '*Defamation in Tanzania*', retrieved from http://hakiakili.blogspot.com/2012/06/defamationin-tanzania.html, accessed on January 13, 2025

[47]Cyber Pornography Law in India- *The Grey law decoded* (Puneet Bhasin, 2015) 17

[48]A Verma, 'Cyber pornography in India and its Implication on Cyber Café Operators' (India: University Institute of Legal Studies, Chandigarh) 23.

The distribution of child pornographic material has increased dramatically through the widespread use of the Internet. Children are sexually abused and the records of this abuse are made globally accessible online.[49] Abusers exchange or sell these images, often through criminal networks.

Recent cases in Nigeria have highlighted the severity of this issue. The Lagos Zonal Command of the EFCC apprehended Olukeye Olalekan[50] for child pornography and another individual, Olukeye Adedayo, [51] was accused of hacking into social media accounts to blackmail victims, including a 14-year-old Canadian boy, which ultimately led to his death. [52] Investigation revealed that the suspect later used the nude images of the 14year old to blackmail him, a situation that led to his death. The victims are not only traumatised through the acts of sexual abuse but also victimised by the global and irrevocable distribution of the images.[53] These cases demonstrate the urgent need for effective measures to combat cyber pornography and protect vulnerable individuals.

8. Inheritance or Will Fraud

Inheritance or will fraud crimes generally take the form of providing false and misleading information to someone about the fact he has inherited money.[54] Scammers use various tactics, including emails, social networks, phone calls and mail, to convince victims to provide financial information or pay fees to receive the non-existent inheritance.[55]

This pattern of cybercrime primarily targets individuals aged 60 and above. Meanwhile, inheritance or Will fraud is not explicitly recognised in Nigerian law, it however, falls under the umbrella of fraud-related offenses. A recent case of Inheritance or Will fraud involved a Nigerian – Okezie Bonaventure, who pleaded guilty to an inheritance fraud scheme that defrauded over 400 victims in the United States. Ogbata sent personalised letters to elderly victims, falsely claiming they were entitled to a multimillion-dollar inheritance left for them by a family member who had died overseas years before.[56]

Inheritance or Will Fraud often involves scammers posing as representatives of fake law firms or banks, claiming that the victim is an heir to a large inheritance. The scammers then request money to cover legal fees, taxes or other expenses, promising a large sum of money in return. However, the money never arrives and the victim's financial information may be compromised.

---

[49] Statista graph reveals child pornography content reported worldwide between 2015 and 2019. In 2019, the association Point de Contact identified 11, 268 child pornographic contents. See www.statista.com/statistics/1246231/child-pornography-content-worldwide/ accessed January 10, 2025

[50] EFCC, Lagos, 'EFCC Arraigns Alleged Sextortion in Lagos' retrieved from https://www.efcc.gov.ng/efcc/news-and-information/news-release/9907-efcc-arraigns-alleged-sextortionist-in-lagos accessedon January 15, 2025

[51] EFCC., 'EFCC Arraigns Man for Alleged Sextortion in Lagos' retrieved from https://www.efcc.gov.ng/efcc/news-and-information/news-release/9496-efcc-arraigns-man-for-alleged-sextortion-in-lagos accessed on January 13, 2025

[52] Ibid

[53] Ibid

[54] NYC Criminal Defense, 'A NYC Criminal Defense Attorney Explains Inheritance and Will Fraud' retrieved from https://nyccriminallawyer.com/fraud-charge/financial-fraud/inheritance-and-will-fraud/ accessed on January, 16, 2025

[55] Ibid.

[56] Office of Public Affairs: U.S. Department of Justice, 'Nigerian National Pleads Guilty to Scheme That Defrauded More Than 400 U.S. Victims' retrieved from https://www.justice.gov/opa/pr/nigerian-national-pleads-guilty-scheme-defrauded-more-400-us-victims accessed on January 16, 2025

Cyber Crime and its Effects on Nigeria's National Development

The rapid evolution of cyberspace has brought both opportunities and challenges to Nigeria's national development. While technology has the potential to drive growth and innovation, its darker side has also enabled criminal activities that hinder national progress. In other words, the disadvantages of cyberspace development have far-reaching consequences for Nigeria's national growth.

Cybercriminals exploit technology for their nefarious activities, including financial fraud, Cyber extortion, Online harassment, Cyberbullying, Disinformation and fake news amongst others. These crimes undermine Nigeria's economic stability, erode trust in institutions, compromise national security and jeopardize citizens' well-being. Victims of cybercrimes suffer long-lasting effects and businesses can collapse, leading to economic hardship.

As stated earlier, a common technique scammers employ is phishing, where scammers send false emails requesting personal information. Providing this information allows criminals to access bank and credit account, open new accounts and damage credit ratings. This damage can take months or years to repair.[57] A single successful cyber-attack can have far-reaching implications, including financial losses, intellectual property theft and loss of consumer confidence, some of which will be discussed subsequently. However, it is imperative to state that one of the main effects of cybercrime on a country or company is revenue or economic loss. This loss can occur when an outside party obtains sensitive financial information and uses it to withdraw funds from an organization. Cybercrimes can also lead to business closures and loss of national resources. Additionally, compromised e-commerce sites can result in lost income when consumers are unable to use the site due to hacking and other cyber-related offenses.

Cybercrimes result in significant monetary losses. For instance, year 2023 report by Comparitech,[58] reveals that over 88.5 million people fall victim to some sort of cybercrime annually, with losses ranging from simple password theft to extensive financial scams. The average loss per victim is of $8,069.[59] As consumers become more aware of traditional cyber threats, criminal have adapted by developing new patterns that exploit mobile devices and social networks to maintain their illicit gains.[60]

1. Intellectual Property

Intellectual property is a product of human intellect that is protected by law from unauthorized use. Ownership creates a limited monopoly, but cybercrime has impeded this exclusive right. Cybercrime has significantly impacted the entertainment, music and software industries. Estimating the extent of damages is a complex process, ranging from hundreds of millions to hundreds of billions of dollars.[61].

Cybercrime is a major obstacle to innovation, as it can drastically reduce the returns on investment in research and development. When a company's intellectual property is stolen, competitors can quickly develop similar products, diminishing the originator's market advantage. Typically, the value of Research & Development (R&D) lies in the temporary lead it provides, attracting new

[57] Ibid

[58] Comparitech, 'Cybercrime Victims Lose an Estimated $714 billion annually' retrieved from https://www.comparitech.com/blog/vpn-privacy/cybercrime--cost/ accessed January 2, 2025

[59] Ibid

[60] Ibid

[61] Ibid

customers until others catch up. However, if stolen IP cuts this lead time from 12 months to just three months, the return on investment drops to a quarter of its potential value, undermining the incentive for innovation.[62]

2. **Damaged Reputations**

When customer records are compromised due to a cybercrime-related security breach, a company's reputation can suffer significantly. Customers who have their financial data intercepted by hackers lose trust in the organisation and often take their business elsewhere, resulting in lost revenue and long-term damage to the company's reputation. [63]

A notable example is the 2017 Equifax data breach, which exposed the personal information of 147 million people.[64] The company agreed to a global settlement, including up to $425 million to help those affected by data breach.[65] Nigeria reporters recently reported similar case where allegations surfaced that the National Identity Management Commission (NIMC) database had been compromised. Although, NIMC denied these claims, but cybersecurity experts pointed out that Nigeria's lack of a robust data protection infrastructure made such breaches not only possible but inevitable.[66]

3. **Reduced Productivity and Financial Growth**

Information technology personnel spend significant time handling and rectifying cybercrime incidents,[67] which could have been spent generating profits. This diversion of resources hinders organizational growth. A significant concern is the theft of confidential information due to cybercrime, such as customer credit card details, which erodes customer trust. As a result, customers may switch to more secure alternatives, ultimately impacting the company's financial growth.[68]

The measures companies implement to counteract cybercrimes can have a negative impact on employee productivity. This is because security protocols require employees to spend more time entering passwords and performing other procedural tasks, taking away from their core responsibilities.[69]

Cyber criminals also target businesses of all size, attempting to compromise company servers to steal sensitive information or exploit them for malicious purposes. To combat this, companies must prioritise cybersecurity investments, including hiring specialised staff and regularly updating software to prevent intruders. A survey by Cobaltt[70], found that large companies spend an average

[62] Net Losses: 'Estimating the Global Cost of Cybercrime Economic Impact of Cybercrime II Center for Strategic and International Studies', retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf accessed on January 9, 2025.

[63] Available at https://www.techwalla.com/articles/effects-of-cyber-crime accessed on the January 9, 2025

[64] Federal Trade Commission, 'Equifax Data Breach Settlement', retrieved from https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement accessed on January 14, 2025

[65] Ibid

[66] Ibid (n. 28)

[67] Ibid

[68] M O Mbaskei, 'Cybercrimes: Effect on Youth Development', retrieved from http://www.i-genius.org accessed on December 29, 2024

[69] Retrieved from https://prezi.com/ku8hy2seczt4/causes-and-effects-of-cyber-crime/ed, accessed on December 29, 2024

[70] Cobalt, 'Top Cybersecurity Statistics for 2024' retrieved at https://www.cobalt.io/blog/cybersecurity-statistics-2024 accessed on January 13, 2025.

of $8.9 million annually on cybersecurity measures. The survey also revealed alarming statistics: 100% of respondents experienced at least one malware incident in the previous 12 months and 71% reported unauthorised computer hijacking by outsiders. In Nigeria, the Senate expressed concerns in November 2023 about the significant economic impact of cybercrimes, estimating an annual loss of $500million due to various cybercrime patterns across the country[71]

4. **Shrink the Competitive Edge of Organizations**

Cybercrime has caused significant financial and physical damage to individual, private and public organizations in Nigeria and worldwide.[72] Annually, billions of dollars are lost globally due to cybercrimes, threatening national security and financial health. When hackers steal confidential information and future plans, companies can suffer substantial losses. If this stolen information is sold to competitor companies, it can significantly reduce the affected company's competitive strength.[73]

An Examination of the Cybercrime (Prohibition, Prevention, Etc.) (Amendment) Act, 2024

The amended Act is a crucial legislation designed to bolster Nigeria's cybersecurity posture. The amendment Act aims to rectify oversights in the Principal Act by inserting omitted words and addressing related matters.[74] Notably, the provisions in the amended Act are not entirely novel, as they were already in the corresponding sections of the Principal Act. This article examines the changes in the Act and its impacts on the Nigerian legal jurisprudence.

1. **Electronic Signatures**: Section 17 of the Principal Act which governs electronic signatures for purchases and transactions has undergone amendments. Section 2 of the amended Act substitutes the word "Signature" with "except where they are legally verified in Certified True Copies". By this provision, certain transactions are excluded from being considered valid under electronic means unless they meet specific verification requirements. Section 17 (4) (b) – (h) provides listed documents required to be certified thus:
    a. Creation and execution of wills, codicil and other testamentary documents
    b. Death certificate
    c. Birth certificate
    d. Matters of family law such as marriage, divorce, adoption and other related issues
    e. Issuance of court orders, notices, official court documents such as affidavits, pleadings, motions and other related judicial documents and instruments
    f. A cancellation or termination of utility services
    g. An instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature

[71] Ibid (n. 7)
[72] E S Meke, 'Urbanization and Cyber Crime in Nigeria: Causes and Consequences', *JPIL*, Vol. 2:1 (2018) 87
[73] B Anah, M Hassan, *et al*., 'Cybercrime in Nigeria: Causes, Effects and the Way Out' Faculty of Science and Technology, Computer Science Department, Bingham University, Karu. Nasarawa State. Nigeria available at http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf accessed on December 28, 2024
[74] See the Preamble to the Amended Act.

h. Any document ordering withdrawal of drugs, chemicals and any other material either on the ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.

The combined reading of the Principal Act and the amended Act reveals that documents, including electronically created and executed Wills, are valid or binding only if 'legally verified in Certified True Copies'. To be valid or binding, these documents must:

1. Be verified by a competent authority.
2. The verification must be done in a Certified True Copy format.
3. The verification process must fulfil the 'legal' requirement for certification of documents,[75] including payment of prescribed fee.

The Supreme Court has in plethora of cases emphasized the importance of certification, particularly in the case of *Lorapuu v State***,**[76] where the Court held thus:

> The whole essence of the court's insistence on the scrupulous adherence to the certification requirement… is to ensure its authenticity, vis-à-vis the original, to third parties… only a properly certified copy is admissible…

Furthermore, for a certified copy of electronic documents of transaction to be deemed authentic and have legal standing, the certification must show evidence of necessary payment. This is in conformity with the Supreme Court's decision in the case of *Aliyu v. Namadi*[77], where the court held at page 203, Paras E – F thus:

> Before a court can place reliance on a certified true copy of a … document, certain requirements must be met, one of which is that necessary payment for the certification must have been made

The above decisions of the Apex Court underscored the significance of certification and payment for certified documents. However, a recent decision clarified that payment for certification can only be mandatory if the issuing authority has prescribed the fee. In other words, if the issuing authority has not prescribed a payment for certification, a certified electronic transaction will be deemed authentic and have legal standing, without compliance with the evidence of payment for certification. This was evident in the case of *Audu v. Federal Republic of Nigeria*[78] where Per Jummai Hannatu Sankey, JSC held at page 30-33, paragraphs C - D thus:

> The dictionary meaning of the word "prescribe" is: "to lay down, in writing or otherwise, as a rule or a course of action to be followed." What this invariably means is that the words in Section 104 (supra) "the legal fees prescribed in that respect…" must refer to the legal fees laid down by the body, organisation or person

[75] See *Daggash v. Bulama (2004) 14 NWLR (PT. 892)* 144 where the Court decision stipulates that a certificate written at the foot of a certified true copy of a public document (in the instant analysis, the amended Act captured some private document which include Wills) should contain, (a) the date, (b) the name of the officer who certified the document, (c) the official title of the officer who certified the document and (d) the seal of the officer who certified the document, if such officer is authorised by law to make use of a seal. See also, ENEJI V. STATE (2024) 11 NWLR (PT. 1948

[76] (2020) 1 NWLR (Pt. 1706) 391

[77] (2023) 8 NWLR (Pt. 1885) 161

[78] (2024) LPELR-62977 (SC)

> in the custody of a … document and on whom a demand is made for a certified true copy of that document. In the instant case, there was nothing before the trial Court showing that the office of the Accountant General of the Federation which issued the certified true copies through the 2nd accused person, and which were admitted as Exhibits D and E, had any laid down or prescribed legal fees for issuing certified true copies of documents in its custody. Thus, the payment of legal fees cannot be a mandatory requirement for the certification of Exhibits D and E."

In essence, the above pronouncement of the Supreme Court necessitates a prescribed fee for certifying electronic documents under the Cybercrime Act. However, the amended Act as well as the Principal Act lacks clarity on the legal verification process, including the omission to prescribe payment for certification and the definition of a competent authority for the purpose of obtaining 'legally verified Certified True Copies' of electronic transactions as stated under Section 17 of the Principal Act. This provision is crucial in preventing fraud cases involving generating electronic document, such as inheritance or Will's fraud in Nigeria. It also complements Section 84 of the Evidence Act[79] which governs admissibility of documents produced by computers. The combined provisions of Section 2 of the amended Act and 17 (4) (a) of the Principal Act further complement Sections 4 and 9 of the Wills Act 1837 which regulates the creation and execution of Wills, as the Wills Act does not address electronic Wills, codicil or testamentary documents.

The amended Act expands the scope of documents requiring certification to include private documents relating to electronic transactions before such documents can be binding. The legal implications of this position are that documents related to electronic transactions lacking proper verification and certification will not be admissible as evidence in Nigerian courts and tribunals.

2. **Enhanced Cyber Incident Response and Reporting Timeline:** Section 3 of the Act significantly amends Section 21 (1) of the Principal Act. The amendment replaces 'Coordination Center' with 'through their respective sectoral CERTs or sectoral Security Operations Centres (SOC)'. This change enhances coordination and response to cyber incidents by leveraging sector-specific CERTs and SOCs. Additionally, subsection (b) reduces the reporting timeline for cyber incidents. Section 21 (3) of the Principal Act now requires reporting within 72 hours of detection, replace the previous 7-days timeframe. This emphasizes the importance of swift reporting and response to minimize the effects of cyber incidents.
3. **Accountability and Identity Theft Liability to Corporations**: As previously stated, Section 4 of the Act amends Section 22 of the Principal Act, broadening the definition of Identity Theft. The offense is no longer limited to employees or persons engaged in the services of a financial institution. Corporations found guilty of identity theft are now liable to imprisonment for a term of 7years or a fine N5,000.000.00 or both. Similarly, Section 6 of the Act further amends Section 27 (2) of the Principal Act, substituting 'financial institution' with 'any public or private organisation'. These provisions expand corporate liability in Nigeria by providing clear direction for holding corporations accountable for crimes committed. The Act additionally enhances accountability by requiring organisations to implement robust cybersecurity measures to prevent and respond to cyber incidents. However, more deterrence measure is

[79] This Principal Act has now been amended by the Evidence (Amendment) Act, 2023 introducing electronic records

expected for corporate entities. This could include the imposition of higher fines.[80] Such fines should be sufficient to achieve sentencing purposes and deter corporations from engaging in identity theft. The fines could also come with a possibility of suspension or banning from the conduct of business once criminal guilt is proved.

4. **Pornography and False Information**: Section 5 of the Act introduces significant changes to Section 24 (1) of the Principal Act, specifically concerning pornography. The Section replace paragraphs (a) and (b) of the Principal Act with new provisions, making it an offense to distribute or share:

    (a) Pornographic content; or

    (b) False information with the intention of causing public disorder, threatening life or sending harmful messages.

5. **Enhancement of Security for Emerging Technological Payment Channels:** Section 7 of the Act accommodates emerging payment technologies by amending Section 30 of the Principal Act. The amendment adds 'or any other payment technology means to broaden the scope of the section, making it applicable to various payment systems and technologies. This change acknowledges the growing trend of digital payments, online banking and contactless transactions. By incorporating 'other payment technology means', the amendment enhances payment security and reduces the risk of cybercrime in the payment ecosystem, having been proscribed by law.

6. **Mandatory Requirement for NIN:** Section 8 amends Section 37 (1) of the Principal Act, introducing the requirement for mandatory identity verification using the 'National Identification Number (NIN) issued by the National Identity Management Commission.' This provision applies to customers conducting electronic financial transactions, aiming to combat financial crimes.

7. **Enhanced Data Protection:** Section 9 replaces the provision of Section 38 (1) of the Principal Act. The new subsection requires service providers to:

    a. Keep and protect specific traffic data and subscriber information

    b. Comply with the Nigeria Data Protection Act and relevant regulations

    c. Retain data for a period of two (2) years.

8. **Strengthening National Cybersecurity**: Section 10 amends and substitute Section 41 (1) paragraphs (d) – (h)of the Principal Act with new paragraphs (d) – (j). the new provisions require:

    a) Establishment of Sectoral CERTs and SOCs: ensure the establishment of sectoral Computer Emergency Response Teams (CERT) and sectoral Security Operation Centres (SOC) that feed into the national CERT.

[80] S Omimakinde, & P Omimakinde, "Criminal Liability of Corporations under the Administration of Criminal Justice Act 2015 and Companies and Allied Matters Act 2020: A Critique", *Obafemi Awolowo University Law Journal*, Volume 4, No.1 & 2, 2020.

b) Protection of National Cyberspace: Ensure all public and private organisations integrate and route their internet and data traffic to the sectoral SOCs, protecting the national cyberspace.

c) National Computer Forensic Laboratory: Establish and maintain a National Computer Forensic Laboratory and coordinate its utilisation by law enforcement, security and intelligence agencies.

d) Capacity Building: Build capacity for the effective discharge of functions by relevant security, intelligence, law enforcement and military services.

e) Public-Private Partnerships: Establish platforms for public-private partnerships (PPP).

f) Additional Measures: Take necessary actions for the effective performance of functions by relevant security and enforcement agencies.

9. National Security: An Imposition of a Taxing Matter: Section 11 of the amended Act revises Section 44 of the Principal Act making non-compliance with the payment of levy or tax on electronic transactions a criminal offense. This levy requires businesses listed in the Second Schedule of the Principal Act[81] to pay 0.5% (0.005) of the transaction value. The introduction of the cybersecurity levy as a revenue-generating instrument by the Act was intended to ensure effective implementation of the provisions of the Act and internationally agreed-upon cybersecurity protocols binding on Nigeria.[82] Although, the levy was introduced by the Principal Act as a revenue-generating instrument amid other types of revenues[83] and created to aid the Office of the National Security Adviser, including the Council of Cybercrime Advisory[84] in implementing their functions and combating cybercrimes in the country.[85] By the amended Act, the statutory functions of the National Security Adviser has been extended to include administering the levy and ensuring compliance to the payment of the levy. Thus, Section 11 of the Act which substitutes subsections (6) - (8) with new provisions stipulates as follows:

a) The National Security Adviser's Office will administer the levy, maintain records and ensure compliance.

b) The Auditor General for the Federation will provide guidelines for auditing the levy account.

c) Businesses failing to remit the levy will be liable on conviction to a fine of not less than 2% of their annual turnover. Non-compliance may also result in closure or withdrawal of their operational license.

---

[81] Such Businesses are; (a) GSM Service providers and all telecommunication companies, (b) Internet Service Providers; (c) Banks and other Financial Institutions; (d) Insurance Companies; and (e) Nigerian Stock Exchange

[82] Punch Newspaper, 'Cybersecurity Levy: intent, timing right, but strategic Communication lacking – Ex-lawmaker' retrieved from https://www.punchng.com/cybersecurity-levy-intent-timing-right-but-strategic-communication-lacking-ex-lawmaker/?utm_source=auto-read-also&utm_medium=web£google_vignette accessed on January 13, 2025

[83] Section 44 (2) (b-e) of the Principal Act

[84] Section 42 of the Principal Act

[85] Section 43 of the Principal Act

Indeed, Nigeria's government faces a dilemma in balancing taxation with its primary responsibilities. While taxation is essential for any country's survival, it is submitted that only a living citizen can fulfil tax obligation. The government's failure to protect citizens' lives and properties, provide jobs and implement laws that benefit Nigerians raise concerns. The country is struggling with inflation[86] and citizens are finding it difficult to afford basic necessities. The government had, on July 2024, approved increase in the country's minimum wage from N30,000 to N70,000[87] with the clause that such increase will be due for renewal after three years.[88] The government additionally promised creation of jobs. Similarly, among other issues with the Academic Staff Union of Universities, include endorsement of renegotiated 2009 agreement with the Nigerian government[89] all of which remain unattended to. Amidst the ongoing hardship, the Central Bank of Nigeria (CBN) issued a circular on May 6, 2024 to all commercial merchants and stakeholders, mandating compliance with the National Cybersecurity levy (i.e., 000.5% levy).[90]

It is not in doubt that as the world shifts towards online trade, this levy will only increase the cost of doing business and the cost of goods, ultimately contributing to the ongoing hardship. Moreover, the imposition of taxes without addressing significant threats like cybercrimes may be seen as misplaced priorities, cybercrime is a critical issue that the government should consider addressing, rather than using it as a means to generate revenue for the office of National Security Adviser. This is tantamount to a situation of robbing Peter to pay Paul. Hence, it is crucial for the government to reassess its priorities and create a safer and more prosperous environment for Nigerians to survive.

10. **Court's Power to Revoke Passports and Citation of the Amended Act:** Section 12 of the amended Act deletes subsection (4) of section 48 of the Principal Act. The provision empowered the court to cancel the international passport of persons convicted and in the case of a foreigner, their passport is to be withheld. While Section 13 stipulates that the Act may be cited as the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024.

Challenges to the Implementation of Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) 2024

1. **Lack of Effective Cooperation Between Nigerian Authorities and International Partners:** Cybercrime is a cross-national and multi-jurisdictional phenomenon. Cybercrime is basically regarded as an international crime. This is because a successful prosecution of the crime often touches on various aspect of jurisdiction, hence, the introduction of Section 50[91] of the

[86] According to the National Bureau of Statistics (NBS), the country's inflation figure hit 34 percent as at June, 2024. See www.channelstv.com/2024/0729/breaking-tinubu-signs-new-minimum-wage-bill-into-law/amp/ accessed on January 3, 2025

[87] The Cable, 'Tinubu Signs N70,000 Minimum Wage Bill into law' retrieved from https://www.thecable.ng/breaking-tinubu-signs-n70000-minimum-wage-into-law/ accessed on January 13, 20250

[88] See Section 2 of National Minimum Wage (Amendment) Bill, 2024 which amend the Principal Act by inserting new Sections 3(1 and 3 (4)

[89] AJLS, 'ASUU Strike Update Today 2024 Latest News', retrieved from https://www.ajils.ng/asuu-strike-update/ accessed on January 3, 2025

[90] CBN, Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024 – Implementation on the Collection and Remittance of the National Cybersecurity Levy' retrieved from https://www.cbn.gov.ng/Out/2024/CCD/CIRCULAR%20REF%20PSMDIRPUBLAB017004%2006052021.pdf accessed on January 12, 2025

[91] The provision stipulates that the Federal High Court in Nigeria has jurisdiction to try offences under the Act, regardless of where the offence occurred, if the offence was committed within Nigeria, on a Nigeria registered ship or aircraft, or by a Nigerian citizen or resident, provided the conduct is also an offence in the country where it was committed or if committed outside Nigeria.

Principal Act to address issues on jurisdiction and international co-operation. Thus, international cooperation to combat crimes in Nigeria has faced significant challenges. One major setback in this regard is the fact that corruption and political interference have undermined efforts to investigate or prosecute cross-national crimes, such as cybercrime. In a bid to make Section 50 of the Act effective, Nigerian Politicians, both within and outside the country, must refrain from encouraging cybercrime or Cybercriminals. Instead, they should support initiatives that combat these illegal activities. In addition, Nigeria must strengthen its judicial system, enhance international cooperation and address the root causes of corruption and impunity.

2. **Limited Resources:** Nigeria's cybersecurity efforts are hindered by limited resources, including inadequate funding, underdeveloped infrastructure and a shortage of skilled personnel. The limited budget restricts access to necessary tools and technology, while the lack of advanced infrastructure and skilled cybersecurity professionals impedes effective investigate and prosecution of cybercrimes activities.

3. **Institutional Challenges:** Nigeria faces institutional challenges in combating cybercrime, including lack of coordination and corruption. Insufficient collaboration between law enforcement agencies, regulatory bodies and Members of the Advisory Council hinders effective investigation and prosecution. Furthermore, corruption within these institutions undermine efforts to combat cybercrime, as some officials prioritize personal gain or political loyalty over enforcing the law, leading to selective prosecution of cybercrime cases and political with-hunting.

4. **Hardship by Design:** hardship by design refers to the intentional or unintentional creation of policies, systems or environments that perpetuate hardship or suffering for certain individuals or groups. It is submitted that Nigerians are going through hardship by design perpetrated by government. The government's policies introduced for the wellbeing of its citizens are often promoted without proactive measures for implementation. Whereas, policies relating to taxes are promptly implemented and imposed on citizens. The imposition of 0.5% levy which Section 11 of the amended Act criminalises, is designed to cause hardship on Nigerians. The lack of implementation of policies that promotes the wellbeing of citizens, exacerbates the suffering of Nigerians, driving some to engage in criminal activities, including cybercrime, as a means of survival. Although, the Cybercrimes Act aims to combat cybercrime offences. However, unaddressed issues like the unimplemented agreements with members of ASUU and minimum wage may hinder its effectiveness. The swift implementation of a 0.005% levy or tax on electronic transactions without implementing the minimum wage may worsen the economic situation and potentially driving more citizens to engage in cybercrime.

Conclusion

Internet has revolutionised the way we live and work and has strangely created new opportunities for organized crime networks to thrive. Online markets and devices provide the same benefits to criminals as they do to legitimate businesses, by allowing them to commit new crimes and old ones in new ways. To effectively regulate cybercrimes in Nigeria, there is a need for reforms and re-organization. The amendment Act has addressed some critical gaps and strengthened cybersecurity, thereby ensuring legal provisions in the Principal Act are up to date with the trends and patterns adopted by cybercriminals. However, continuous efforts are necessary to curb

cybercrime activities and promote effective implementation of the principal Act alongside its amended Act.

Recommendations

To Tackle the Trends and Patterns of Cybercrimes in Nigeria, The Following are recommended

1. The government must prioritize implementing policies that directly impact citizens' welfare. This includes promptly enforcing the Minimum Wage Policy and honouring the agreements entered into with the Academic Staff Union of Universities (ASUU). In addition, job creation should be a top priority. By addressing these critical areas, the government can effectively decrease the number of individuals who might turn to cybercrime out of desperation. This approach will not only reduce cybercrime activities but also demonstrate the effectiveness of the amended Act by instilling fear in potential perpetrators.
2. It is submitted that the amended Act be revised to accommodate the following:
    a. Comprehensive interpretation of "cybercrimes" to reflect the evolving nature of digital technologies. It is a fundamental principle of criminal law that for an act to be considered a crime or offense, it must be explicitly defined and prohibited by a statute or law. This principle is often referred to as "*nullum crimen sine lege*". Indeed, the Principal Act has outlined various offenses and penalties related to cybercrimes and the amended Act has updated the Act. However, there is more to be done.
    b. Establishment of an Electronic Document Verification Department (EDVD) as competent authority across the 36 states of the Federation, including FCT for ease of compliance. This department would be responsible for evaluating electronic documents to verify their authenticity and certify them as "Certified True Copies" in compliance with the law.[92]
    c. Incorporate provisions or guidelines for the legal certification of electronic generated documents which may include payment of prescribed fee as held in the case of *Audu v. Federal Republic of Nigeria* (Supra), and issuance of receipt of payment for certifying documents relating to electronic transactions or copies of such certified electronic document held by the competent authority for the purpose of achieving the provisions of the amended Act as well as comply with the requirements for certification.
3. The law enforcement agents, particularly the EFCC should be equipped with updated skills, knowledge and insight for effective fight against cybercrimes. As it is necessary that security personnel, and other law enforcement agencies know more about internet technology than the internet criminals in order to devise strategies to fight the menace.
4. Finally, there is a pressing need for specialized training for Judges and Members of the Advisory Council,[93] to enhance their understanding of the extant Cybercrimes Act and its practical applications. This training would equip Members of the Advisory Council on their approach in combating cybercrimes, and also equip Judges with the necessary knowledge, to effectively adjudicate cases relating to cybercrimes, and ensuring that justice is served. The judiciary must also acknowledge the revolutionary impact of Information and

[92] Ibid (n.76)

[93] Member of the Advisory Council are listed under the First Schedule of the Principal Act

Communication Technology (ICT) on the legal landscape. Most Judges still rely on traditional standards for burden of proof in internet-related cases, leading to seemingly unjust outcomes and unenforceable orders. To address this, Judges must be educated on the latest ICT trends and their implications for cybercrime cases.