An Appraisal of the Nigerian Cyber Crimes Law from Comparative Perspective

Ortese, P.T.*

Abstract

Cybercrime has emerged as a significant global threat, prompting countries to develop comprehensive legal frameworks to combat such offences. Like many countries, Nigeria has responded with the enactment of the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015. This article examines Nigerian Cyber Crimes Law and compares it with the legal frameworks in the United Kingdom, the United States of America, and South Africa. Through a comparative analysis, this study aimed to identify the strengths and weaknesses of Nigerian law and draw insights from well-established legislation. This study provides an overview of cybercrime laws and their significance in addressing computer-based offences. It delves into Nigerian Cyber Crimes Law, examining its scope, provisions, and enforcement mechanisms. In parallel, an in-depth analysis of the legal frameworks in the United Kingdom, United States, and South Africa was conducted, highlighting important features. Using a comparative analysis framework, this study evaluates Nigerian Cyber Crimes Law against the backdrop of the frameworks of the analysed countries. Factors such as legal definitions, penalties, procedural frameworks, international cooperation, privacy protection, and oversight mechanisms are also considered. Furthermore, this study aimed to shed light on the potential lessons and best practices that Nigeria can gain from countries with well-established cybercrime legislation. Drawing upon successful strategies and policies, this study provides recommendations for improving Nigerian Cyber Crimes Law, including areas that require legislative amendments, enhanced technological capabilities, and cross-border collaboration.

Keywords: Cybercrime, Nigeria, comparative analysis, United Kingdom, United States of America, South Africa

* LLB (Hons) (Abuja), BL, LLM (Calabar), PGDE (Port Harcourt), PhD Student University of Uyo, Akwa Ibom State, Nigeria and Divisional Registrar, National Industrial Court of Nigeria, Uyo Division Email: peterortese@gmail.com Tel. No.:08035446931

1. Introduction

Cybercrime has spread globally owing to the development of information and communication technology and the Internet's international reach, which has sparked the emergence of new types of electronic crimes in the cyber sphere[1]. Phishing, child pornography, intercepting electronic communication, and other cybercrimes are some examples. This change has a severe impact on people's lives, society, and the economy[2]. It is challenging to apprehend criminals and gather the required evidence for their trials, because the victims and perpetrators of these cybercrimes span numerous states and nations. These digital crimes have worsened over time due to the transnational nature of the offences and the defence of national sovereignty[3]. The policing of cyberspace has also been made more difficult by the disparity in federal laws among nations and absence of an international legal framework.

Cybercriminals continue to impede global efforts to prevent cybercrime by exploiting these complexities and variances. In recent years, Nigeria has seen an increase in cybercrime, as more criminals use the internet to commit various crimes[4]. Nigeria enacted the Cybercrime (Prohibition, Prevention, etc.) Act of 2015 to address this problem, making it a crime to engage in hacking, identity theft, and cyberstalking, among other types of cybercrimes[5]. However, Nigeria's cybercrime law efficiency has been contested, contending that it is overbroad and falls short of protecting citizens' rights[6]. Therefore, comparing Nigeria's cybercrime law with the laws of other countries will reveal the law's advantages and drawbacks, and suggest areas for improvement. This article provides an analysis of Nigerian cybercrime law by comparing it with the legal frameworks of other jurisdictions. The aim is to highlight the changing landscape of combating cybercrimes in a world that is becoming increasingly

---

1 B.A,OmodunbiO. M Odiase, andA. O Esan, Cybercrimes in Nigeria: Analysis, Detection and Prevention *journal of Engineering and Technology* (2016) Vol. 1, Issues I, September 37 -41. https://www.researchgate.net> accessed on 15 January 2023.

2 ibid

3 D.S Abraham and S.E Goodman, Cybercrime and Security. *The transnational Dimension. Hoover press:* cyber DPSHPCTBE010006-25 rev.1-34. www hoover.org.> accessed 19 January 2023.

4 ibid

5 Appendix 4 Cybercrimes (Prohibition, Prevention, etc) Act 2015 Explanatory Memorandum

6 I.O George, R, A Ngwoke, Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention, etc) Act 2015 and other legislation *Journal of law, policy and globalization*. (2022) vol. 119. 1 -16. www iiste.org> accessed 15 February 2023.

interconnected. To conduct a comparative analysis of how cybercrimes are defined, it is essential to examine the legal frameworks of jurisdictions known to have robust cybersecurity legislation. These jurisdictions include the United Kingdom, United States, and South Africa. A comparative analysis revealed how different legal systems address similar challenges by examining the common elements and variations in the definitions of cybercrime. When comparing definitions of cybercrime, it is essential to consider how these variations affect legal enforcement, prosecution, and international cooperation in combating cybercrime. Analysing the similarities and distinctions in definitions helps to thoroughly evaluate Nigeria's cybercrime legislation globally. This promotes informed policymaking and legal reform.

2. Conceptual Clarification

This conceptual clarification aims to provide a clear understanding of the topic, as it breaks down the key components and concepts.

2.1 *Cyber Law*

The legal precepts, guidelines, and requirements that control how digital tools, networks, and services are used are referred to as cyber law[7]. It is a subset of law that deals with the legal ramifications of using the Internet, cyberspace, and other electronic devices.[8]Intellectual property rights, privacy, data protection, e-commerce, cybercrime, cyberbullying, and online defamation are just a few of the many themes covered by cyber law[9]. It also discusses the legal implications of digital agreements, contracts, and signatures. Cyber law aims to safeguard the rights and interests of people and organisations in cyberspace by creating a legal framework for their usage[10]. Its objectives are to control how people behave online, prevent cybercrime, and encourage responsible use of technology. cyber laws constantly change and must keep up with the

---

7 M.Rouse (Ed). Dictionary IT Alignment Cyberlaw. Techopedia.www.techopedia.com.> accessed15 March 2023.

8 Ibid

9 Career paths in Information Security: What is Cyber law? (2019) Norwich University Online. wwwonline.norwich.edu.> accessed 15 February 2023.

10 ibid

rapid development of technology. cyber law will continue to be critical in determining how we use and interact with technology as new digital technologies and legal issues emerge[11].

Cyber law is crucial in the modern digital age, where technology permeates every aspect of our lives. This ensures that people and organisations are held responsible for their online behaviour and are safe from dangers. Intellectual property law is one of the main domains of cyber law.[12] This speaks to the legal defence of artistic creations, including books, movies, music, and software. Cyber law also addresses legal matters related to the use of domain names and trademarks and copyrights on the Internet, which is a critical component of cyber law[13]. The protection of data privacy is a critical component of cyber law[14]. This covers areas such as using cookies and other tracking technologies and acquiring, using, and storing personal information online. Cyber law also governs the disclosure of personal information, particularly regarding data breaches and hacking.

Legal facets of e-commerce, such as online contracts, electronic payments, and digital signatures, are also included in cyber law.[15] It controls how online markets and platforms are used and the obligations of online shoppers and retailers. Cybercrime is another crucial element of cyber law, and includes hacking, cyberstalking, identity theft, and online fraud[16]. Along with dealing with cybercrime, cyber law also addresses concerns linked to cyberterrorism, cyberwarfare, and the legal foundation of such cooperation. Cyber law is essential for ensuring that digital technologies are used sensibly and morally and that people and organisations are held responsible for their online behaviour.

2.2 Cyber-crime

Section 2 of the Criminal Code of Nigeria defines crime as an act or omission which renders the person doing the act or making the omission liable to punishment under the Code or under any other Act

---

11 ibid

12 A. Dixit, The Role of Intellectual Property in CyberLaw(2022). *Enhelion Blogs*, http.wwwenhelion.com> accessed 15 April 2023.

13 ibid

14 ibid

15 Intellectual Property in Cyberspace, www.geeksotorageeks.org> accessed 14 May 2023.

16 ibid

or law. Various writers have attempted to define crimes. Glanville defines crime as follows: "a legal wrong that can be followed by criminal proceedings which result in punishment". Okonkwo et al. defined crime by way of procedure used in hearing criminal matters and civil matters. They concluded that crimes or civil actions can only be defined by the procedures involved in hearing the matter.[17]

The word cyber-crime is a hybrid word. It is made of "cyber" and "crime"'. According to Sackson, cybercrime is a crime committed with the help of a computer through a communication device or a transmission media called cyberspace and a global network called the Internet. The Commonwealth Organisation,[18] states that cyber-crime includes not only crimes against computer systems (such as hacking, denial of service attacks and the set-up of botnets) but also traditional crimes committed on electronic networks (e.g. fraud via phishing and spam; illegal Internet-based trade in drugs, protected species and arms) and illegal content published electronically, (such as child sexual abuse material). The author states that cybercrime is any offence carried out involving the use of computers and the Internet.

Cyber-crime is also defined as criminal activity involving an information technology infrastructure, including illegal access; illegal interception that involves technical means of non-public transmissions of computer data to, from, or within a computer system; data interference, which includes unauthorised damage, deleting, deterioration, alteration, or suppression of computer data; system interference that interferes with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data; misuse of devices, forgery (identity theft), and electronic fraud.

Cyber-crime is further defined as a crime that is enabled by or targets computers.[19] According to Chik,[20] cybercrime is distinguished

---

17 N. Okonkwo, et al "*Criminal Law in Nigeria*" (2nd ed.) Spectrum Law Publications, Ibadan (1994)

18 Commonwealth Internet Governance Forum "Commonwealth Cybercrime Initiative" http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA7786970A639B05%7D_Computer%20Crime.pdf. accessed on 3/2/2020 by 8:00pm.

19 W. Clay, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, p.7. (2008).

20 W.B. Chik, "*Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore*", Icfai law books, http://works.bepress.com/warren_ p.4 (2007).

from computer-enabled crimes. They relate to crimes against computer hardware as well as the digital content contained within it, such as software and personal data. Computer-enabled crimes have an adverse effect on the integrity and trust in information technology infrastructure, such as computers or telecommunications networks, and on the security of transactions conducted through them.

"Computer crimes" are often used to define criminal activities committed against a computer or similar device, and data or programmes therein. In computer crimes, computers are the targets of criminal activity. The author's understanding of cybercrime is that it involves activities perpetrated by individuals or computer systems under the control of criminals. These criminals exploit computers and Internet-enabled devices, such as smartphones and iPads, to engage in unlawful Internet activities, regardless of their physical location.[21]

The author asserts that certain writers[22] fail to acknowledge the role of human intention (mens rea) in the commission of cybercrime when categorising it as either computer crimes or computer-enabled crimes. Therefore, the classification of cybercrimes as offences facilitated by computer systems is deceptive. The author aligns with the stance of the Commonwealth Organization for cyber-crimes.[23]

Every day, persons with criminal intent engage in activities or fail to act in ways that harm others online. In Nigeria, a prevalent term is used to refer to persons who engage in advance fee fraud schemes, namely "Yahoo Boys." These people are characterised by their criminal inclinations. Nigeria has established itself as a prominent origin of what is commonly referred to as 419 emails, a term derived from Section 419 of the Nigerian Criminal Code Act, which criminalises advance fee fraud. Nigeria has the top position in Africa as both the target and origin of harmful cyber operations. This trend is expanding beyond the West African sub-region, with Ghana

---

21 The writer's opinion is premised on the fact that cybercrimes are carried out by individuals or by computers programmed by individuals for the purpose of carrying out cybercrimes. This definition also reflects the fact that cybercrimes are borderless crimes.

22 W.B. Chik, "*Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore*", Icfai law books, http://works.bepress.com/warren_ p.4 (2007). Accessed 23/1/2020.

23 Commonwealth Internet Governance Forum "Commonwealth Cybercrime Initiative" Ibid.

also emerging as a notable hub for cybercrime, commonly known as "Sakawa" in Ghana.[24]

3. The Prevalence of Cybercrimes and Legal Framework.

Cybercrime has evolved in Nigeria, as in many other nations, along with technological improvements. The country's path to the digital age began in the late twentieth century, bringing both opportunities and challenges. The Internet has spawned new forms of criminal activity, ushering in an era of cybercrime in Nigeria. Cybercrime began to gain traction in the early 2000s, mostly owing to the spread of Internet access and rising usage of electronic gadgets. The historical context emphasises the importance of legal and regulatory measures to confront rising threats to cyber security and individual rights[25].

Nigeria has implemented a comprehensive legislative framework to address the issue of cybercrimes, as seen by the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act[26] . This legislation defines cybercrimes, stipulates appropriate sanctions for perpetrators, and establishes national cybersecurity policies and strategies. The Nigerian Data Protection Act [27] to safeguard the privacy and personal data of individuals in the digital realm in accordance with international data protection norms. Nigeria's law enforcement authorities, such as the Nigerian Police Force and the Economic and Financial Crimes Commission (EFCC), have established dedicated divisions tasked with investigating and prosecuting cybercrimes[28]. The National Computer Emergency Response Team (ngCERT) assumes the responsibility of orchestrating responses to cybersecurity crises and bolstering the nation's overall cybersecurity position[29].

---

24 N. Ribadu, "*Cybercrime and Commercial Fraud: A Nigerian Perspective*" a presentation at Modern Law for Global Commerce Congress to celebrate the fortieth annual session of UNCITRAL Vienna (2007).

25 N. Kshetri, Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management. Vol.22, 2019. www,tandfonline.com .Acesssed on the 12th August 2023.

26 2015

27 2023, Superuse, A Review of the Nigerian data protection act2023: Highlights and limitations, Stren & Blan jul26 2023 www.strenandblan.com accessed on the 5th September 2023.

28 P Ndem, The Role of the Economic and Financial Crimes Commission (EFCC) in Fighting Cyber Fraud www.papers.ssrn.com Accessed on the 12th August 2023.

2929 F.E Ikuero, Preliminary Review of Cybersecurity Coordination in Nigeria, Nigerian journal of Technology vol.41 No 3 May 2022.Accessed on 23 August 2023.

Nigeria is grappling with a variety of cybercrimes, including phishing, advanced fee fraud, identity theft, cyberattacks, and online extortions. These crimes have significant societal and economic impacts, including defrauding individuals and organisations, damaging Nigeria's reputation, and causing trust erosion[30]. To address these issues, Nigeria requires a multifaceted approach that includes legal and regulatory measures, technological solutions, and international cooperation. Comparing Nigeria's cybercrimes law with other jurisdictions will help assess the country's readiness to address these issues in the global context.

4. Comparing the Cybercrime Legislation of Nigeria and the United Kingdom

Nigeria and the United Kingdom have implemented legislative measures to combat cybercrime; however, notable distinctions exist between the two nations' approaches.

The Nigerian Cybercrime Act 2015 encompasses a broad spectrum of cyber offenses, comprising unauthorized access to computer systems, cyber terrorism, identity theft, and online fraud[31]. In contrast, the UK Computer Misuse Act 1990 pertains to offences such as unauthorised access, modification, or impairment with intent, and the creation or provision of articles for use in computer offences.[32]

The Nigerian Cybercrime Act 2015 stipulates that certain offenses are punishable by a minimum prison sentence of three years or a fine of no less than N7 million (equivalent to approximately $17,000)[33]. Similarly, the UK Computer Misuse Act 1990 prescribes a maximum prison sentence of two years for most offenses[34].

The Nigerian Cybercrime Act 2015 is endowed with extraterritorial jurisdiction, thereby enabling its application to offenses perpetrated beyond the borders of Nigeria[35]. This provision applies to Nigerian citizens, residents, or any act that impacts

---

30 F.E Eboibi, introduction to law and cybercrime. *Handbook on Nigerian Cybercrime law*(ed) Pages 1-237 Benin 2018

31 Section 5 – 36 of the Cybercrime Act 2015.

32 ibid (38)

33 Section 6(4) of the Cybercrime Act 2015

34 Section 1 Computer Misuse Act 1990

35 Section 52 of the Cybercrime Act 2015

Nigerian computer systems. In comparison, the UK Computer Misuse Act of 1990 lacks extraterritorial jurisdiction. The laws in question permit the gathering and acceptance of electronic evidence in a court of law[36]. However, the Nigerian Cybercrime Act of 2015 contains more comprehensive regulations about digital forensics and electronic evidence management[37]. Moreover, it is noteworthy that the Nigerian Cybercrime Act of 2015 mandates that service providers collaborate with law enforcement agencies during investigations[38]. Conversely, the UK Computer Misuse Act of 1990 lacks a corresponding provision.

The Nigerian Cybercrime Act of 2015 stipulates the imposition of corporate liability for cyber offences[39], thereby attributing responsibility to companies for the actions of their employees or agents during their official duties. The Computer Misuse Act of 1990 in the United Kingdom requires the aforementioned provisions.

To summarise, the Nigerian Cybercrime Act 2015 and the UK Computer Misuse Act 1990 addressed cybercrime. However, notable distinctions exist between the two in their respective coverage, penalties, jurisdictional reach, evidentiary and investigatory provisions, and corporate accountability measures.

The following are supplementary particulars regarding the fundamental distinctions between the Nigerian Cybercrime Act of 2015 and the UK Computer Misuse Act of 1990:

4.1 Scope

The Nigerian Cybercrime Act of 2015 exhibits greater comprehensiveness concerning the range of offences that it encompasses. Apart from conventional computer-related offences such as hacking and malware, the scope of cybercrime encompasses a range of other unlawful activities, including cyber stalking, child pornography, and cyber-terrorism[40]. In contrast, the Computer Misuse Act of 1990 in the United Kingdom has a more specific scope, cantering on computer systems' unauthorized manipulation and entry[41].

---

36 Section 4 CMA Section 3ZA
37 ibid
38 Section 38 of the Cybercrime Act 2015
39 Section 40(3)(4) of the Cybercrime Act 2015
40 Section 18, 23 and 24 of the Cybercrime Act 2015
41 Section 1 of the Computer Misuse Act 1990

The Nigerian Cybercrime Act of 2015 stipulates comparatively harsher penalties for certain offences[42] in contrast to the UK Computer Misuse Act 1990. The Nigerian legal system stipulates a potential sentence of 10 years of incarceration for acts of cyberterrorism[43]. In contrast, the UK legal system prescribes a maximum sentence of 2 years imprisonment for most related offenses[44].

It is widely acknowledged that the Nigerian Cybercrime Act of 2015 is more extensive and stringent in its approach to combating cybercrime than the UK Computer Misuse Act of 1990. However, both laws have the same objective. Notably, the United Kingdom has recently implemented supplementary legislation to combat cybercrime, including the Computer Misuse Act 2018 and the Data Protection Act 2018[45]. These statutes may offer additional safeguards for both UK citizens and enterprises. The following elucidates the fundamental distinctions between the Nigerian Cybercrime Act of 2015 and the UK Computer Misuse Act of 1990:

4.2 Jurisdiction

The Nigerian Cybercrime Act of 2015 provides legal provisions for the indictment of foreign nationals who engage in cybercrime activities that affect Nigeria's computer system[46]. This implies that individuals not geographically situated within Nigeria may still be susceptible to legal prosecution per Nigerian jurisprudence. By comparison, the Computer Misuse Act 1990 in the United Kingdom lacks similar measures for indicting individuals who are not citizens of the United Kingdom.

---

42 Section 24C(ii) 3(b) Cybercrime Act 2015

43 Section 18 of the Cybercrime Act 2015

44 Section (1) of the Computer Misuse Act

45 The Act was assented to in the 16th of May 2018 and commenced on 30 May 2018. The Act is aimed to protect the confidentiality, integrity and availability of the computer systems programs and data as well as facilitated the prevention, detection, investigation, prosecution and punishment of cybercrimes. Indokhomi D., and J.Syekei . The computer Misuse and Cybercrimes Act. (2020)www.bownanslaw.com. >accessed 11 June 2023.

46 Section 53(ii) of the cybercrime Act 2015.

The Nigerian Cybercrime Act of 2015 provides a range of defences that defendants may invoke[47]. These defences include situations where the conduct was legally authorised or the defendant lacked the necessary intent to commit an offence. The Computer Misuse Act of 1990 in the United Kingdom does not contain explicit defences. However, the defendant may assert that their behaviour did not satisfy the elements of the offence for which they were being prosecuted.

4.3 Collaboration

The Nigerian Cybercrime Act of 2015 incorporates clauses that pertain to global collaboration and support in the context of cybercrime inquiries and litigations, which encompass the processes of extradition and mutual legal aid[48]. The Computer Misuse Act of 1990 in the United Kingdom provides for international collaboration in criminal affairs, albeit lacking explicit clauses about cybercrime.

4.5 Penalties and Remedies

The Nigerian Cybercrime Act of 2015 provides civil remedies in conjunction with criminal penalties, including compensation for those affected by cybercrime[49]. The Computer Misuse Act of 1990 in the United Kingdom lacks comparable provisions for civil remedy.

In general, the Nigerian Cybercrime Act of 2015 and the UK Computer Misuse Act of 1990 are significant legislative measures designed to address cybercrime. Although certain overlaps exist in the types of offences they address and in the permissibility of digital evidence, there are also discernible distinctions in their range, sanctions, territorial authority, and additional provisions. However, as technology continues to evolve and new threats emerge, there is an ongoing debate about whether CSA needs to be updated to better address emerging risks to information security.

5 Comparative Analysis of Cybercrime Laws in Nigeria and the United States.

---

47 Section 31 of the Cybercrime Act 2015.
48 Ibid (53) Section 54
49 Computer Misuse Act Section

Conducting a comparative assessment of cybercrime legislation in Nigeria and the United States would entail scrutinising the similarities and distinctions between the respective legal frameworks governing cybercrime in both nations. The examination could encompass various aspects, including the delineation of cybercrime, classification of cyber offences, sanctions imposed on cybercrime, and strategies implemented to avert and scrutinise cybercrime.

A salient distinction between the cybercrime laws of Nigeria and the United States pertains to their degree of advancement and implementation. The United States has implemented a comprehensive set of laws on cybercrime for several decades, whereas Nigeria's legislation on cybercrime was only established in 2015. Consequently, the United States possesses a more developed legal infrastructure and law enforcement mechanism to tackle cybercrime. An additional contrast pertains to the extent of legal regulations. Although both nations acknowledge various types of cyber offences, the United States possesses a broader spectrum of offences and more stringent sanctions for cybercrime. The Computer Fraud and Abuse Act (CFAA) is a legislative measure in the United States that criminalizes a broad spectrum of computer-related transgressions, such as unlawful entry into a computer system and the misappropriation of confidential information[50]. The Cybercrime Act in Nigeria proscribes to activities such as hacking, identity theft, and cyberstalking. However, there are concerns among some quarters that legislation requires more precision and clarity. Both countries have implemented measures to prevent and investigate cybercrimes. However, the effectiveness of these approaches may vary. The United States has well-established authorities dedicated to investigating cybercrime, such as the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS). In contrast, Nigerian law enforcement agencies are strengthening their ability to combat cybercrime efficiently.

Comparing the cybercrime legislation in Nigeria and the United States highlights the importance of Nigeria in continuously

[50] ibid (n150)

improving its legal infrastructure and law enforcement capabilities to effectively combat cybercrime. Given that cybercriminals often operate across national borders, it is crucial to prioritise international cooperation and collaboration in order to effectively address cybercrime[51].

To conduct a comprehensive analysis of Nigerian cybercrime legislation in comparison to that of the United States, it is essential to examine the explicit provisions and implementation of legal frameworks in both jurisdictions.

The Nigerian Cybercrime Act enacted in 2015 proscribes various cyber offenses, including hacking, identity theft, cyberstalking, cyberbullying, and cyberterrorism[52]. The legislation additionally stipulates the formation of a Cybercrime Advisory Council, which will guide the government on cybercrime issues[53]. Furthermore, it mandates the establishment of a Cybercrime Investigation Agency, which will be responsible for the examination and litigation of cybercrime incidents[54].

Nonetheless, the legislation has been censured due to its excessive scope and inadequate lucidity and exactitude in delineating cyber transgressions. These circumstances have elicited apprehensions regarding the possibility of exploitation and the need for more precise delineations and directives.

In comparison, the United States has implemented comprehensive laws on cybercrime that have been in place for several decades. The Computer Fraud and Abuse Act (CFAA) enacted in 1986 is a significant legislative measure that renders a broad spectrum of computer-related transgressions as criminal offences. These offences encompass, but are not limited to, unauthorised entry into a computer system, misappropriation of confidential information, and dissemination of malicious code.

The United States possesses established agencies and departments, namely, the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), and the Department of Homeland

---

51 A. Peters and A. Hindocha, US Global Cooperation: A Brief Explainer. Third Way www.thirdway.org>accessed on the 23 June 2023.

52 First schedule (Section 42) Computer Fraud and Abuse Act

53 ibid

54 ibid

Security (DHS), which are committed to the investigation of cybercrime and the legal pursuit of perpetrators. These entities collaborate closely with private enterprises to exchange information and mitigate cyber risk. The divergence in the execution and imposition of cybercrime legislation between the two nations is noteworthy. There have been apprehensions in Nigeria regarding the ability and proficiency of law enforcement entities in conducting investigations and litigating instances of cybercrime. In certain instances, there have been accounts of malfeasance and instances of misuse of authority.

The Computer Fraud and Abuse Act (CFAA) have faced censure in the United States due to its perceived lack of specificity and excessive scope, resulting in contentious legal proceedings and apprehensions regarding its susceptibility to exploitation[55]. There have been apprehensions regarding the efficacy of law enforcement agencies in thwarting and probing cybercrime, particularly in instances that involve transnational perpetrators.

To sum up, it can be observed that although Nigeria and the United States have implemented legislation to address cybercrime, disparities exist in terms of the comprehensiveness, lucidity, and efficacy of these legal frameworks. Sustained enhancement and refinement of legal infrastructure and law enforcement competencies are imperative for tackling cybercrime proficiently in both nations.

The United States typically imposes more severe penalties for cybercrime than Nigeria[56]. The Computer Fraud and Abuse Act (CFAA) in the United States stipulates a maximum penalty of 10 years' imprisonment for unauthorised access to computer systems. In contrast, Nigeria's corresponding law provides a maximum penalty for 5 years' imprisonment for the same offence.

An additional contrast pertains to the extent of global collaboration in tackling cyber-crime. The United States has entered into multiple bilateral and multilateral agreements with other nations to collaborate on deterrence, examination, and litigation of cybercrime. Nigeria has faced criticism for its perceived lack of

---

[55] L. Johnson, Computer Fraud and Abuse Act, Security Control Evaluation Testing and Assessment Handbook (second edition) pages 9-25 www.sciencedirect.com>accessed on the 23 June 2023.

[56] Iibid

cooperation with other nations in tackling cybercrime, potentially impeding the efficacy of the investigative and prosecutorial efforts.

Both nations have implemented measures to prevent and detect cybercrime, although with varying degrees of efficacy. The cybersecurity landscape in the United States is characterised by a well-developed ecosystem encompassing established standards, guidelines, best practices for cybersecurity, and a thriving cybersecurity industry. The Nigerian context requires increased investment in cybersecurity infrastructure and capabilities and robust public-private partnerships to foster cybersecurity awareness and collaboration.

It is imperative to acknowledge that cybercrime is a dynamic and ever-changing hazard, necessitating Nigeria and the United States to continually modify their legal and law enforcement structures to effectively tackle emerging vulnerabilities and complexities. The concerns above encompass the resolution of matters regarding encryption, safeguarding data privacy, and the utilisation of nascent technologies such as artificial intelligence and blockchain in cybercrime. Although Nigeria and the United States have implemented legal frameworks to tackle cybercrime, variations exist in their comprehensiveness, lucidity, and implementation. Sustained investment in cybersecurity infrastructure and capabilities, coupled with enhanced international cooperation, is imperative to adequately tackle the worldwide threat of cybercrime.

To delve deeper into the comparative evaluation of cybercrime legislation in Nigeria and the United States, it is imperative to consider certain intricacies of laws and their execution.

The Nigerian Cybercrime Act enacted in 2015 delineates a spectrum of cyber transgressions, including hacking, identity theft, cyberstalking, and cyberterrorism[57]. The legislation also renders the creation, distribution, and utilisation of technological tools and computer programs intended for the commission of cyber offences unlawful. Furthermore, the legislation stipulates the creation of a National Cybersecurity Fund that aims to provide monetary assistance to prevent and probe cyber offences.

---

[57] Section 18 and section 25 Cyber Crime Act 2015

There have been apprehensions regarding the execution of the legislation, particularly regarding the ability and proficiency of law enforcement entities to conduct investigations and litigate instances of cybercrime. Critiques have been raised regarding the imprecise delineation of certain cyber transgressions and the possibility of their exploitation.

The Computer Fraud and Abuse Act (CFAA) in the United States encompasses a variety of computer-related transgressions such as unlawful entry into a computer system, misappropriation of confidential information, and dissemination of harmful code. Using a computer to perpetrate fraudulent activities, gain unauthorised entry into financial data, and participate in cyber espionage is also illegal.

6. Comparison of the Legal Frameworks against Cybercrime with Nigeria and South Africa.

Nigeria and South Africa passed comprehensive laws to establish a legal framework for cybercrime. South Africa's Cybercrimes and Cybersecurity Bill aims to update and streamline cybercrime laws, whereas Nigeria's Cybercrime Act 2015 criminalises multiple online activities. As defined by statutes, cybercrime is an illegal act committed using a computer or an electronic device. The Cybercrimes and Cybersecurity Bill in South Africa provides a comprehensive definition of cybercrimes, including cyber terrorism, espionage, and cyber fraud.

Both laws criminalise various Internet activities, such as unauthorised hacking, data theft, online fraud, cyberstalking, and the spread of computer viruses. While South Africa's Cybercrimes and Cybersecurity Bill covers cyber espionage and extortion, Nigeria's Cybercrime Act 2015 addresses cyber terrorism and child pornography.

Both statutes sanctioned cybercrime offences. Infractions in Nigeria's Cybercrime Act 2015 and South Africa's cybercrimes and cybersecurity bills are punishable by fines, imprisonment, asset forfeiture, and jail. Both statutes provide jurisdiction over cybercrime offences committed within the nation's borders or by nationals, regardless of where they were committed. The Cybercrimes and

Cybersecurity Bill of South Africa includes clauses that permit the prosecution of cybercrimes committed outside its borders.

Both pieces of legislation authorise law enforcement to investigate and prosecute cybercrime cases. Concerns have been raised about the effectiveness of law enforcement organisations in both countries when investigating and prosecuting cybercrime.

Nigeria and South Africa have enacted comprehensive cybercrime laws that criminalise various online behaviours and have established a framework for addressing cybercrime. Despite some similarities with other legislation, South Africa's cybercrimes and cybersecurity bills are more comprehensive and cover a broader range of online behaviours. The effectiveness of these laws relies on their application and enforcement. To enhance the fight against cybercrime, it is crucial to raise awareness, build capacity, and foster international cooperation between both countries.

The 2015 Cybercrime Act in Nigeria includes data protection and privacy regulations. Organisations are required to prevent the unauthorised access, use, and disclosure of personal information and data. The statute also specifies penalties for data breaches. The Protection of Personal Information Act (POPIA) 2013 in South Africa is a law that safeguards personal data and imposes obligations on organisations to securely collect, handle, and store such information.

South Africa's Cybercrimes and Cybersecurity Bill grants jurisdiction over cybercrime offences committed within the country's borders, as well as internationally. In addition, the bill includes provisions for extraterritorial jurisdiction, allowing South Africa to prosecute cybercrime offences committed abroad. Owing to the global nature of cybercrime, this clause is crucial. Nigeria and South Africa are committed to international collaboration in combating cybercrime. The African Union Convention on Cyber Security and Personal Data Protection aims to promote collaboration among African nations to fight cybercrime. Both nations signed conventions. South Africa is a member of the Southern African Development Community (SADC) Cyber Security Advisory Committee. Nigeria is a member of the ECOWAS Cyber Security Working Group.

Both nations recognise the importance of developing capabilities to combat cybercrime. The National Cybersecurity Centre in Nigeria is responsible for coordinating nationwide cybersecurity operations and providing training and capacity building to law enforcement organisations and partners. The Cybersecurity Hub was founded in South Africa. It coordinates cyber security efforts, training, and capacity building for law enforcement organisations and other stakeholders.

Significant problems still need to be solved despite the efforts of both nations to combat cybercrime. These difficulties include a lack of understanding of the dangers of cybercrime among the general public and business community, a lack of resources and knowledge within law enforcement agencies to investigate and prosecute cybercrime, and the requirement for greater international cooperation and coordination in tackling cybercrime across borders.

Although Nigeria and South Africa have passed comprehensive cybercrime laws that establish a legal framework for dealing with the problem, more needs to be done to improve awareness, capacity building, and international cooperation in the fight against cybercrime. Both nations must continue to engage in capacity building and international cooperation in order to address the growing nature of cybercrime.

7. Lessons for Nigeria

Nigeria can learn much from international efforts to combat cybercrime. The lessons that Nigeria must learn are:

The global nature of cybercrime requires cooperation among international partners. Nigeria should actively engage in international initiatives to combat cybercriminal activities by sharing its intelligence, best practices, and resources.

Enactment of robust and all-encompassing legislation. It is imperative for Nigeria to enact contemporary and all-encompassing legislation to combat cybercrime effectively. It is of utmost importance for legislative bodies to precisely delineate cybercrime offences, institute suitable sanctions, and remain adaptable to the constantly evolving realm of cyber danger.

Nigeria should prioritise investment in law enforcement agencies' training and capacity development to enhance their technical skills and investigative capacities. This entails furnishing essential resources and tools for the investigation and legal pursuit of cybercrimes.

Public-private partnerships (PPPs) collaborate with government agencies, private sector entities, and civil society organisations. Nigeria should establish collaborative partnerships to effectively address cybercrime and facilitate the exchange of information, expertise, and resources. This collaboration can enhance efforts to prevent, detect, and mitigate cyberthreats.

Nigeria should focus on conducting cybersecurity awareness campaigns to educate the general public, enterprises, and government entities about cyber risks and best practices for online safety. This involves educating users about secure online behaviour, preventing phishing attacks, and emphasising the importance of using strong passwords.

Developing a robust incident response mechanism and encouraging the reporting of cybercrimes are essential. Nigeria should establish formal mechanisms that allow individuals and organisations to confidentially report cyber incidents in a secure manner. This enables prompt action and aids in gathering the data required to understand the threat landscape.

Nigeria can benefit from adopting international best practices for cybersecurity and cybercrime prevention. Organisations can enhance their cybersecurity posture by implementing established frameworks such as the NIST Cybersecurity Framework and ISO 27001. Additionally, security measures can be strengthened by adopting multifactor authentication, encryption, and regular security assessments.

Collaboration with technology companies is a significant aspect of modern business practice. Collaboration with technology companies offers advantages in combating cybercrime. Nigeria should establish strong partnerships with technology companies to foster the development of creative solutions, exchange information on potential threats, and effectively tackle vulnerabilities in software and systems.

Nigeria should effectively enhance its judicial processes in handling cybercrime cases through appropriate strengthening measures. This entails the establishment of cybercrime tribunals that possess specialised jurisdiction and appoint trained prosecutors and judges who possess a comprehensive understanding of cyber-related matters.

The dynamic nature of cyber threats necessitates Nigeria's ongoing adaptation of strategies, laws, and technological defences to effectively counter emerging threats. Regular evaluations, revisions, and improvements to cybersecurity frameworks are necessary.

By implementing these lessons, Nigeria can enhance its cybersecurity posture and combat cybercrime.

8. Challenges in Combating Cybercrime

Nigeria, the United Kingdom, the United States, and South Africa encounter distinct challenges in their efforts to combat cybercrime. Below are some of the key challenges faced by each of these countries.

1. The legal framework in question is characterised by its limitations. The absence of comprehensive legislation pertaining to cybercrime in Nigeria poses obstacles to the successful prosecution and deterrence of such offences.
2. Nigeria has garnered infamy in the realm of internet fraud due to its involvement in Advance Fee Fraud, usually referred to as "419 scams," as well as other forms of online scams. Consequently, this has resulted in significant harm to a country's reputation. Fraudulent activities are frequently orchestrated by well-structured criminal syndicates.
3. Law enforcement agencies frequently encounter challenges stemming from constrained resources, insufficient technical proficiency, and inadequate interagency cooperation. This impeded the promptness of investigations and apprehensions.
4. Cross-border issues arise because of the regular activity of cybercriminals from foreign jurisdictions, emphasising the significance of extradition and international collaboration. Nonetheless, the absence of bilateral agreements with other nations is a barrier to achieving successful partnerships.

5. The United Kingdom is confronted with a growing number of intricate and highly developed cyber threats encompassing state-sponsored attacks as well as ransomware activities. The dynamic and ever-changing nature of the threat landscape presents difficulties for proactively countering criminal techniques.
6. The United Kingdom is facing increasingly complex cyber threats, including state-sponsored and ransomware activities. The ever-changing threat landscape makes it challenging to combat criminal techniques proactively. The United Kingdom is experiencing an absence of skilled cybersecurity professionals, making establishing a strong defense against cyber criminals difficult.
7. Fragmented law enforcement is observed in the realm of cybercrime investigations when multiple authorities, including but not limited to the National Crime Agency (NCA), the Metropolitan Police, and regional police forces, bear the responsibility for addressing such criminal activities. Fragmentation presents difficulties in effectively coordinating endeavours and facilitating the exchange of information.
8. The concept of jurisdiction in cyberspace is complex because of the absence of geographical boundaries. The United Kingdom (UK) encounters difficulties in addressing cybercriminal activities beyond its territorial authority.
9. The United States possesses a significant presence of cybercriminals within its jurisdiction because of its expansive dimensions, sophisticated technological infrastructure, and extensive digital interconnectedness. Addressing cybercrime on a large scale presents several challenges.
10. The United States faces an ongoing issue in reconciling the necessity for law enforcement agencies to obtain information with the protection of citizens' privacy rights, giving rise to legal and privacy concerns. Achieving optimal equilibrium and ensuring that legal structures remain in step with technological advancements can provide a multifaceted challenge.
11. International cooperation is a crucial aspect that warrants consideration. The task of apprehending cybercriminals

residing in other nations is often complicated by the existence of divergent legal systems and diplomatic obstacles, necessitating collaboration with international law enforcement organisations.

12. Rapid technological breakthroughs pose a significant difficulty in keeping pace with progress. The exploitation of developing technology by cybercriminals poses a significant challenge to law enforcement agencies as it necessitates continuous efforts to remain up-to-date and respond efficiently.
13. South Africa's limited resources directly impact the development of robust cybersecurity infrastructure and the nurturing of talent in this field. A significant portion of the population lacks knowledge of cybercrime risks. This knowledge gap allows cybercriminals to exploit those who are unaware of the best strategies to protect their digital presence.
14. Coordination and information sharing among authorities responsible for preventing and prosecuting cybercrime remain a significant issue. Foreign collaboration presents challenges for South Africa in engaging with foreign law enforcement authorities, hindering timely and effective responses to cybercrime threats.

Nigeria, the United Kingdom, the United States, and South Africa face various challenges in their fight against cybercrime. These challenges arise from factors, such as differences in laws, available resources, skill gaps, international collaboration, and public awareness. Resolving these difficulties requires collaboration between government bodies, law enforcement, commercial enterprises, and global cooperation. Together, they can develop comprehensive plans and countermeasures to combat the constantly evolving cyber-threat environment effectively.

10 Recommendations

In light of the above discussion and analysis, as encapsulated in this paper, it is recommended that

1. The Cybercrime (Prohibition, Prevention, etc.) The 2015 Act should be revised to include a

clear definition of cybercrime offences, penalties, novel forms of digital crimes, and procedures as well as to resolve existing gaps and prevent potential misuse.

2. There is a need to provide comprehensive training and resources to law enforcement agencies to enhance their ability to effectively investigate and prosecute cybercriminals.
3. There is a need to foster collaboration with the United Kingdom, the United States of America, and South Africa, among other countries, to facilitate information-sharing and the expansion of cybercriminals.
4. There is a need to conduct campaigns to increase public awareness of cybercrime risks, prevention measures, and reporting mechanisms.
5. There is a need to establish specialised courts to handle cybercrime cases and ensure swift and effective trial processes.
6. There is a need to establish a specialised institution to aid in the fight against cybercrime in Nigeria.

By implementing these recommendations, Nigeria can strengthen its cybercrime legislation and effectively combat cyber threats within its borders.

9. Conclusion

Nigerian cybercrime law has several shortcomings compared to the legal frameworks in the United Kingdom, the United States of America, and South Africa. Although the law acknowledges significant aspects of cybercrime such as identity theft and hacking, it unfortunately contains inconsistencies, inadequacies, and ambiguities. Furthermore, enforcement and prosecution efforts should be improved threats within its borders.