BRILL | NIJHOFF

AFRICAN JOURNAL OF LEGAL STUDIES
16 (2024) 249–270

AFRICAN JOURNAL OF LEGAL STUDIES
brill.com/ajls

Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps

Ifeoma E. Nwafor | ORCID: 0000-0001-9288-2378
Senior Lecturer, Faculty of Law, Godfrey Okoye University, Enugu, Nigeria
Co-Founder/Chief Product Officer, Decybr Inc., Ontario, Canada
nwaforifeoma@gouni.edu.ng

Received 6 March 2023 | Accepted 19 May 2024 |
Published online 31 July 2024

Abstract

The investigatory framework of cybercrime is as essential as the legal and institutional framework governing cybercrime. This article argues that an effective investigation process is fundamental to the effective prosecution of cybercrime offences. Cybercrime investigation involves digital forensics, intelligence gathering, lawful interception, and use of communication data and internet networks. At its core, cybercrime investigation necessitates a comprehensive cybercrime investigation framework backed by a legal framework that ensures effective evidence collection, preservation, and analysis. This article evaluates the cybercrime investigation structure in Nigeria and highlights the gaps in Nigeria's regulatory framework. It identifies the challenges that hinder Nigeria's successful investigation and prosecution of cybercrime offences. The study adopts a comparative methodology by juxtaposing cybercrime investigation in Nigeria with the law and practice in the United Kingdom (UK). The UK has a robust cybercrime investigation framework, strengthened by its Cyber Security Strategy 2022. The findings show that, unlike the UK's Regulation of Investigatory Powers Act, 2000 and the Investigatory Powers Act, 2016, the Nigerian Cybercrimes (Amendment) Act, 2024, the Administration of Criminal Justice Act, 2015 and other laws, are silent on essential investigatory initiatives, steps and specialised powers. The study proposes a practical cybercrime investigation framework to implement Nigeria's effective prosecution of cybercrime offences.

Published with license by Koninklijke Brill BV | DOI:10.1163/17087384-12340108
 | ISSN: 1708-7384 (online)

Keywords

cybercrime – cybercrime investigation and prosecution – regulatory framework – Nigeria – United Kingdom

1 Introduction

The Nigerian cyber threat landscape is rapidly escalating with the rate and sophistication of cyberattacks and cybersecurity breaches. Emails sent from Nigerian based servers (Nigerian internet scams) are classified as one of the most common forms of fraud.[1] Nigerian legislators have argued that the lack of an adequate information communication technology (ICT) culture makes Nigeria inadequately equipped to tackle cyberattacks.[2] The Cybercrimes (Prohibition, Prevention, Etc) (Amendment) Act, 2024 (CPPA) and the Principal Act, The Cybercrime (Prohibition, Prevention, Etc) (Amendment) Act, 2015, did not substantially empower law enforcement agencies with special investigative powers to effectively investigate cybercrimes and protect individual privacy and civil liberties.

Investigating cybercrime is a highly demanding task. Such investigations have thrown up many challenges to the investigative capacity and competence of policing in various countries. This is owing to the transnational character and scope of cybercrime. Additionally, the sophistication of technology has outpaced the laws regulating cyber-related offences in Nigeria.[3] At its core, cybercrime investigation necessitates an adequate ICT culture and comprehensive cybercrime investigative framework backed by a legal framework that ensures effective evidence collection and preservation, analysis and prosecution. Arguably, this can be achieved by establishing an adequate legal framework with a structured approach that enables law enforcement to

1 Peter Grabosky, *Cybercrime: Keynotes in Criminology and Criminal Justice Series* (New York: Oxford University Press 2016) 19.

2 Samson Atekojo Usman, 'Nigeria not Ready for Cyber Attacks- Buhari' <*http://dailypost.ng/2018/06/26/nigeria-not-ready-cyber-attacks-buhari/?utm_source=DailyPost+Newsletter&utm_campaign=6ac803bc54Todays_headlines&utm_meduim=email&utm_term=0_7c25dc3ce6-6ac803bc54-227478289*> last accessed 15 February 2024.

3 Police National Legal Database (PNLD) and Andrew Staniforth, 'Blackstone's Handbook of Cyber Crime Investigation' Babak Akhgar and Francesca Bosco (eds) (London: Oxford University Press 2017).

successfully investigate and prosecute cybercrimes while upholding human rights and due process.[4]

While researchers have conducted comprehensive studies analysing the methods and challenges of cyber investigation,[5] there is little research examining how the cybercrime investigation framework in Nigeria has played out in the lawful and successful prosecutions of cybercrime in Nigeria. The question of whether a practical cybercrime investigation framework enables successful prosecution of cybercrime offences in Nigeria has been accorded little attention. To gain insights into the concept of cybercrime investigation, this study provides an in-depth analysis of the stages of cybercrime investigation, elucidating its challenges and highlighting opportunities for bridging the gaps identified. It examines the cybercrime investigation process in Nigeria viz-a-vis the United Kingdom (UK), which has a robust cybercrime investigation framework. It identified challenges in the cybercrime investigation framework in Nigeria, including jurisdiction, anonymity and encryption and proposed solutions to bridge the gaps.

The paper is divided into four sections, commencing with this introduction. Section two analyses the different approaches to cybercrime investigation. Section three provides a comparative study of cybercrime investigation in Nigeria and the United Kingdom. Section four evaluates the various limitations of cybercrime investigations, while part five provides concluding remarks.

4 Vasilios Katos and Peter M Bednar, "A Cyber-crime Investigation Framework", (2008) Computer Standards & Interfaces 30(4) 223-228. DOI: 10.1016/j.csi.2007.10.003.

5 Gargi Sarkar, Hardeep Singh, Subodh Kumar, Sandeep K. Shukia, 'Tactics, Techniques and Procedures of Cybercrime: A Methodology and Tool for Cybercrime Investigation Process'. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. (2023). https://doi.org/10.1145/3600160.3605013. Jan Gruber and Lena L. Voigt et al., 'Foundations of Cybercriminalistics: From General Process Models to Case-Specific Concretizations in Cybercrime Investigations' (2022) 44 Forensic Science International Digital Investigation. https://doi.org/10.1016/j.fsidi.2022.301438. Ayse Okutan and Yalcin Cebi, 'A Framework for Cyber Crime Investigation' *Procedia Computer Science* (2019) 158 https://doi.org/10.1016/j.procs.2019.09.054 accessed 3 February 2024. F Calderoni, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation' (2010) 54(5) *Crime Law and Social Change* https://doi.org/10.1007/s10611-010-9261-6 accessed February 2024. 'Cybercrime Investigation and the Protection of Personal Data and Privacy', Project on Cybercrime https://rm.coe.int/16802fa3a3 accessed 23 February 2024. Peter Bednar et al., 'The Complexity of Collaborative Cyber Crime Investigatives', *Digital Evidence and Electronic Signature Law Review*, 6 DOI: 10.14296/deeslr.v6i0.1894 accessed 28 February 2024.

2 Cybercrime Investigation Approaches

Cybercrime is challenging to define or conceptualise with exactitude because of the absence of a universally accepted definition and inconsistency in cybercrime regulation.[6] The term 'cybercrime' refers to illegal activities that relate to computers, the internet, technology, and network systems. It has been described as a label of convenience, as it relates to a wide range of crimes committed with the aid of digital technology.[7] Conducts that amount to cybercrime include phishing, ransomware, hacking, illegal interception of computer-mediated communications, data theft, espionage, piracy, romance scams, fraud, cyber extortion, sales and investment fraud. Cybercrime is any crime that involves a computer used as an instrument to perpetrate crime, the focus of the crime and a repository of evidence.[8] The scale, sophistication and wide-ranging impact of cybercrimes have made investigating the crime more challenging.

Different approaches, methods or processes have been discussed and canvassed by legal commentators and researchers as the appropriate technique for investigating cybercrime.[9] Cybercrime investigation is the *sine qua non* of prosecuting cybercrime and related offences. It is a mission that seeks, collects and gathers evidence of a crime for a case.[10] A criminal investigation is the collection of information and evidence relevant to identifying, apprehending and convicting suspected offenders.[11] Part II of the Criminal Procedure and Investigation Act of the UK[12] defines criminal investigation as '… an investigation conducted by police officers with a view to it being ascertained- (a) whether a person should be charged with an offence, or (b) whether a person charged with an offence is guilty of it'.[13] This paper defines it as an official

6 Ifeoma E. Nwafor, *Cybercrime and the Law: Issues and Developments in Nigeria* (Lagos: CLDS Publishing 2022) 4.

7 Grabosky, (n 1).

8 Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, (3rd edn, Academic Press 2011).

9 Roger Atsa Etoundi, 'Multi-Perspective Cybercrime Investigation Process Modelling' [2 June 2012] 2(2) *International Journal of Applied Information Systems* <*http://citeseerxist.psu.edu/viewdoc/download?doi=10.1.1.401.7951&rep=rep1&type=pdf*> accessed 11 February 2024. He proposes a multi-perspective cybercrime investigation process that can be considered as a basis for standardization.

10 'Criminal Investigation' <*https://www.pinow.com/investigations/criminal-investigations*> accessed 22 February 2024.

11 PNLD and Staniforth, (n 3).

12 1996 (CPIA) Code of Practice of UK.

13 Ibid, s 22 (1).

task carried out by law enforcement agents who assemble relevant information and evidence that would assist in the unravelling of a criminal case.

In past years, a criminal investigation was carried out to prove points of law that presupposed the commission of a crime, the arrest, interview, and prosecution of an offender.[14] The ethos of criminal investigations has significantly improved due to the miscarriage of justice and a series of public inquiries concerning police investigations. Criminal investigations now focus mainly on searching for the truth and providing a range of possible outcomes.

A cybercrime investigation is akin to a criminal investigation that seeks to unravel a particular crime committed in the cyber ecosystem. Cybercrime investigation, as with any investigation, involves determining specific elements of the crime and whether laws that give jurisdiction support the prosecution of such crimes.[15] The investigator must determine if the offence comes under a statute that provides jurisdiction to support prosecution. Some crimes under the ambit of cybercrime have not been covered by legislation due to the swift evolvement of new technologies.

Criminal investigation of conventional crime involves regular and specialised methods in some instances. In traditional crimes, numerous physical pieces of evidence are usually available at the crime scene, and collecting such evidence requires critical thinking and a reasonable amount of technical knowledge.[16] In contrast, cybercrime investigation requires thorough and special investigative skills and scientific tools. The primary approach to investigating cybercrimes is the digital investigative method.[17] Digital investigative techniques or digital/computer forensics are the acquisition, preservation, and presentation of digital evidence generated from digitally related crimes.[18] It is defined as 'the discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law'.[19] The word 'forensics' signifies that digital forensic processes are

14 PNLD and Staniforth, (n 3).

15 'Cybercrime Investigations-Law Enforcement Cyber Centre' *International Association of Chiefs of Police* <*http://www.iacpcybercenter.org/officers/cyber-crime-investigation/*> accessed 11 March 2024.

16 'Investigation in Cybercrime' <*https://www.shodganga.inflibnet.ac.in*>*bitstream*> accessed 13 February 2024.

17 It is also referred to as digital forensic investigation.

18 MO Hewling and P Saint, 'Digital Forensics: The Need for Integration' *Proceedings of Digital Forensics & Incident Analysis* (WDFIA 2011).

19 'US CERT 2008, UK Copyright Law: Summary' <*http://www.copyrightservice.co.uk/copyright/uk_law_summary*> accessed 22 February 2024.

carried out to procure evidence that may be used in a court of law.[20] Digital forensics relates to the law because the evidence obtained from such investigation may/will be used in a court of law.

The history of computer forensics can be traced to the first time a system administrator investigated what unauthorised changes occurred in his system and by whom or what medium.[21] Computer forensics was limited to law enforcement agencies and investigators in the 1990s.[22] However, with expanding technological advancements, computer forensic tools are available for public use. Individuals and organisations in developed countries can investigate any activity suspected to be a criminal element and apply auditing standards and principles.

The importance of digital forensics in investigating cybercrime cannot be overemphasised. A computer forensic analyst examines and preserves electronic evidence and uses it to investigate cybercrime. They can recover evidence from electronic communications not stored on the computer or the internet service provider's server for cybercrime investigation.[23]

2.1 *The Computer/Digital Forensic Investigation Process*

Several forensic investigative models or techniques have been proposed, revealing the process's complexity.[24] Digital forensic investigators and researchers have argued that cybercrime investigations have different steps and approaches.[25]

---

20 Moniphia Hewling and Paul Sant, 'Digital Forensics: An Integrated Approach' [September 2012] <*https://www.researchgate.net/publication/259055528_Digital_Forensics_An_integrated_approach*> accessed 22 February 2024.

21 Adel Ismail Al-Alawi, 'Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status' [2014] 8(3) *Research Journal Business Management* <*https://scialert.net/fulltext/?doi=rjbm.2014.139.156*> accessed 3 February 2024.

22 'Digital Forensics' https//www.open.edu accessed 14 February 2024. Digital forensics was commonly referred to as computer forensic up until the late 1990s.

23 Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (2nd edn, Anderson Publishing, MA 2011).Muktar Bello, 'Investigating Cybercriminals in Nigeria: A Comparative Study', (PhD thesis: University of Salford 2018).

24 Michael Kohn, Jan HP Eloff and Martin S Olivier, 'Framework for a Digital Forensic Investigation' [2006] <*https://www.researchgate.net/publication/220803284_Framework_for_a_Digital_Forensic_Investigation*> accessed 12 February 2024

25 Roger Atsa Etoundi and Achille Moyo Mboupda', Multi-Perspective Cybercrime Investigation Process Modeling' [June 2012] *International Journal of Applied Information Systems* 2(2) <*https://citeseerx.ist.psu.edu*> accessed 25 February 2024. They proposed the proactive, active and reactive components of digital forensics investigation.

Moore argued that the first stage in the computer forensic investigation is duplicating the suspect's hard drive or other digital storage media. This is followed by imaging a suspect's media, called the imaging process. Thereafter, creating a hash value for the hard disk is needed to prevent or minimise data manipulation. Subsequently, the files and file signatures are verified. This is an essential stage of the investigation.[26] The next step is forensic analysis.[27] Kohn *et al.* proposed a three-phase framework for forensic investigations. These are preparation,[28] investigation,[29] and presentation.[30] Akhgar and Bosco posit that hi-tech/cybercrime investigation embodies four components or stages characterising all cybercrime investigation's core concepts.[31] These are collection, examination, analysis, and reporting.

Holt *et al.* opine that standardising the steps for conducting a digital forensic investigation generates consistency in how law enforcement personnel handle digital evidence.[32] They described the survey/identification stage as the first stage of the digital forensic investigation. The collection/acquisition phase involves retrieving and preserving digital evidence. The goal of preserving digital evidence is to make a copy of the original data files for examination to minimise the possibility of making any changes to the original data files. The examination/analysis phase is concerned with data recovery or extraction and analysis of digital data. The report should reflect complete transparency, describing each step of the digital forensic process.[33]

Given the preceding approaches and methodologies provided, it is clear that securing the suspected computer, collecting evidence, analysing it and presenting the evidence are steps that they all have in common. The foregoing shows that there are four standard stages in digital forensic investigation, even if the terminology differs.

---

26 When a file is created or saved, the file's header will contain a signature that informs the operating system about what type of file is being created or saved.

27 Moore (n 23).

28 This stage includes: standards used in the organization/agency; policies/procedures put in place to assist in the investigation; training, legal advice; notification to the correct authorities; documentation of previous incidents; and planning (approach strategy).

29 This is the most important stage.

30 Kohn and others (n 24).

31 PNLD and Staniforth, (n 3).

32 Thomas J Holt, Adam M Bossler and Kathryn C Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd ed New York: Routledge 2018).

33 Ibid.

2.2 *Role of Digital Leads in Cybercrime Investigations*

Target cybercrimes[34] and tool cybercrimes[35] have shown that cybercrime can be committed on a large (global) scale, across countries (borders) and reaching numerous computer users. Unlike real-life crimes, there are no physical leads available when investigating targets and tools of cybercrimes. In cybercrime investigations, digital leads play a vital role. These leads are essential and should be followed by law enforcement officials in cybercrime investigations. These have been identified as (1) Internet Protocol (IP) addresses and (2) Online handles.[36] These two digital leads are the foundation on which digital investigative methods used to gather evidence are based. In most inept cybercrime cases, the offender will leave a few tracks in numerous places.[37] The communication that amounts to a crime will be traceable to an IP address whose physical location will be conspicuous. In more sophisticated cases, the offender impersonates other users across several jurisdictions and conceal their communication content by encrypting them. This poses a difficult challenge for law enforcement officials to investigate.

An IP address is 'a numerical address that is assigned to a computer, which is part of a computer network and uses the Internet Protocol to communicate'.[38] It is '... a string of numbers that uniquely identify a computer, but only at a particular time; they do not, in theory, identify a person[39] or even a particular machine permanently'.[40] It has been argued that IP addresses and time are vital ingredients that identify a suspect at the beginning of an investigation.[41]

---

34 Target cybercrimes are the crimes committed where the computer is the target of the offence. Examples of target cybercrimes are: hacking, the use of malware, the use of botnets etcetera.

35 In tool cybercrimes, computer and the internet are used in the commission of the crime. Examples of tool cybercrimes are: child pornography, online drug trafficking, online fraud etcetera.

36 Jan-Jaap Oerlemans, 'Investigating Cybercrime' [10 January 2017] *Leiden University Repository <https://openaccess.leidenuniv.nl/bitstream/handle/1887/44879/Full_text_Investigating_Cybercrime.pdf?sequence=2>* accessed 1 March 2024.

37 Grabosky, (n 1).

38 Oerlemans, (n 36).

39 Several people in a facility or household may use one computer.

40 Lilian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work?' in Lilian Edwards and Charlotte Waelde (eds) *Law and the internet* (Bloomsbury publishing 2009). This book shows that most consumers sign up to domestic ISPs which dynamically assign IP addresses according to demand. Thus, an IP address can normally only identify even a household in conjunction with date and usage logs held by the ISP.

41 Da-Yu Kao and Shiuh-Jeng Wang, 'The IP Address and Time in Cyber-Crime Investigation' [2009] <*https://www.researchgate.net/publication/235253984_The_IP_address_and_time_in_cyber-crime_investigation*> accessed 3 February 2024.

Rooney argues that an IP address is one of the core elements of the internet, and all computers or devices communicate through it on a static or dynamic basis.[42] This is why law enforcement agencies worldwide utilise IP addresses to trace an accused or cybercriminal.

An IP address is a crucial constituent of the internet and an indispensable means for tracking crime in cyberspace. However, an investigation based solely on IP address tracking cannot be relied on to convict an accused because a public IP address[43] may be used, or IP address spoofing may be involved. This shows that cybercrime investigations based on IP address tracking cannot be solely relied on to secure a conviction.

3 Cybercrime Investigation in Nigeria and the United Kingdom

Currently, in Nigeria, numerous laws and policies regulate the internet ecosystem and prosecution of cyber-related offences. The related frameworks are discussed seriatim below:

3.1 *Cybercrime Investigation in Nigeria*

3.1.1 The Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024

The Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 is Nigeria's principal legislation regulating cybercrime. It provides the legal basis for preventing, detecting, investigating and prosecuting cybercrimes in Nigeria. It also prescribes a proactive response strategy against cyber threats and attacks.[44] However, the absence of a regulatory authority or agency to oversee the enforcement of the Act's provisions hinders the fight against cybercrime in Nigeria. Accordingly, the principal Act was amended in February 2024 to address concerns and issues with the law, to enhance protection of rights, and to adapt to recent developments in the cyber ecosystem.

Section 38 of the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024 (CPPA) mandates service providers to keep and protect specific traffic data and subscriber information for two years, in accordance with certain provisions of the Nigerian Data Protection Act as may be prescribed by the

42 Timothy Rooney, *Introduction to IP address management Vol. 17* (John Wiley & Sons, 2010) 1–4.

43 This is where many individuals use a private or public network and share a IP address.

44 Adedeji Adekunle, 'A Review of the Cybercrime Act 2015' Adedeji Adekunle (ed), *Combatting Cybercrimes in Nigeria: Trends and Issues* (Abuja: NIALS Press 2017).

relevant authority responsible for regulating communication services in the country.[45] Service providers must retain non-content and content information and make such information available to an authorised officer of a law enforcement agency.[46] The Act mandates that any data retained shall be used for legitimate purposes as provided under the Act, any other legislation, regulation or an order of a court of competent jurisdiction.[47] Appropriate measures to safeguard the confidentiality of the data retained must be taken and the individual's privacy must be respected.[48]

Service providers are required to intercept electronic communications for criminal investigation or proceedings where there are reasonable grounds to suspect that such communication is required for investigation.[49] Section 45 of the CPPA provides safeguards regarding the power of arrest, search and seizure. Section 45 of the CPPA provides thus:

> (2) The Judge may issue a warrant authorising a Law Enforcement Officer to-
> (a) enter and search any premises or place if, within those premises, place or conveyance-
> (i) an offence under this Act is being committed;
> (ii) there is evidence of the commission of an offence under this Act or
> (iii) there is an urgent need to prevent the commission of an offence under this Act; ...
> (d) seize, remove and detain anything which is, or contains, evidence of the commission of an offence under this Act.
> (e) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network.
> (f) use of any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensive format; or

45 S 38(1) of the Principal Act was amended by substituting for subsection (1). It is important that the service providers keep and protect data in accordance with the appropriate data regulatory framework in Nigeria.

46 S 38(2) and (3).

47 Subsection 4.

48 S 38(5). The individual's right to privacy under the CFRN must be given due regard.

49 S 39.

(g) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.

From the preceding, section 45 does not comprehensively empower law enforcement agencies with specialised investigative powers to adequately investigate and prosecute cybercrime offences. In extreme cases, conducting electronic surveillance without contravening human rights and freedoms is necessary to investigate cybercrime offences successfully. The CPPA does not cover fundamental investigative powers that enable timely access to crucial evidence and the legal basis for cybercrime investigations and prosecutions.

Section 47 of the CPPA covers the prosecution of offences. It provides that 'Subject to the powers of the Attorney-General, relevant law enforcement agencies shall have the power to prosecute offences under this Act'. The section failed to state the relevant law enforcement agencies. This has resulted in multiple agencies overseeing the prevention, investigation and prosecution of cybercrime, which has led to investigative and prosecutorial clashes.[50]

The Act does not have a cybercrime investigative framework that guides law enforcement officials on cybercrime investigations. Understandably, the CPPA is the substantive legislation that defines cybercrimes and punishments under the Act. In contrast, the Administration of Criminal Justice Act 2015, which is the main procedural law on criminal investigation, does not comprehensively outline search, seizure procedures, data collection, and preservation.

3.1.2 The Administration of Criminal Justice Act 2015

The Administration of Criminal Justice Act 2015 provides a general framework of procedural processes applicable to all criminal investigations.[51] It does not set out the process for administering and enforcing the CPPA. It provides for arrest, bail, warrants, prevention of offences, security for good behaviour, public nuisance, place of trial or inquiry and plea bargain, amongst other things.[52] The Act is silent on essential investigatory steps and powers. It does not provide a framework for permissible surveillance and investigation of electronic communication that must be compatible with the fundamental human rights enshrined in the Nigerian Constitution and the African Charter on Human and Peoples' Rights.

50 Nwafor (n 6).

51 See ACJA, sections 15(4), 18, 37-39, 43-44, 106, 143.

52 ACJA, Parts 2, 3, 4, 6, 9 and 28.

3.1.3 The Economic and Financial Crimes Commission

The Economic and Financial Crimes Commission (EFCC) is a Nigerian law enforcement agency that investigates and prosecutes cases of corruption and financial crime. Section 6 of the EFCC Act gives the Commission the responsibility to investigate all financial crimes, including advance fee fraud, computer crime, money laundering, and fraudulent encashment. Section 6(b) of the Act provides that the Commission shall be responsible for 'the investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam etc.'[53] The powers of the Commission are further widened by sections 7(1) (a), 7(2)(f) and 13(2), which gives it the powers to investigate and prosecute offenders for any offence, whether under the EFFC Act or any other statute. The underlining requirement is that the offence relates to the commission of economic and financial crimes.[54] The synergy of sections 6 and 7 gives the EFFC the legislative impetus to prosecute cybercrimes in Nigeria, even though nothing in the Act expressly gives them an inherent cyber jurisdiction.[55]

Although the Commission has investigated numerous cybercrime-related offences for years, it is essential to state that the Act did not explicitly provide the components of cybercrime investigation that the Commission can legally carry out.

3.1.4 The Terrorism (Prevention and Prohibition) Act, 2022

The Terrorism (Prevention and Prohibition) Act of 2022 repealed the Terrorism (Prevention) Act No. 10 of 2011. It provides measures for the detection, prevention, and countering of acts of terrorism to implement international instruments and standards effectively.

Part 10 of the Terrorism Act 2022 covers the investigation and prosecution of terrorism. Section 64 of the Act provides for investigation and search without a warrant in a case of verifiable urgency or life-threatening cases. Section 65 gives an authorised officer the right to record measurements, samples, photographs or fingerprint impressions during investigations. Section 68 of the Act covers interception of communication orders. Section 68(2) provides thus:

53 EFCC Act, s 46 defines economic and financial crimes.

54 See *Dr Joseph Nwobike SAN v FRN*, SC/CR/161/2020.

55 Emmanuel Obuah, 'Combating Corruption in Nigeria: The Nigerian Economic and Financial Crimes (EFCC)' [2010] 12(1) *African Studies Quarterly* available on <*http://asq.africa.ufl.edu/files/Obuah-V12Is1.pdf*> accessed 27 February 2024.

> (2) The court to which an application is made under subsection (1) may make an order-
> (a) requiring a communication service provider to intercept and retain a specified communication, or communications of a specified description received or transmitted or about to be received or transmitted by that communication service provider, including the call record data or metadata;
> (b) authorise a relevant agency to enter any premises and to install in such premises, any device for the interception and retention of a communication or communications of specified description, and to remove and retain such a device for the purpose of intelligence gathering; or
> (c) authorise a relevant agency to execute a covert operation in relation to an identified or suspected terrorist group, entity or person for the purpose of gathering intelligence.

Section 68(3) provides that An order made under subsection (1) shall specify the period for which a communication service provider may be required to retain communication data to which the order relates. This provision is similar to section 38 of the CPPA, which mandates service providers to keep all traffic and subscriber information as may be prescribed by the relevant authority responsible for regulating communication services in the country for two years. However, the provisions of section 38 of the CPPA are not as elaborate as section 68 of the TA, which gives authorised officers the right to carry out covert operations, intelligence gathering and lawful interception.

From the preceding, the laws regulating cybercrime in Nigeria do not establish a specific body or agency with monitoring or oversight authority of cybercrime investigation and prosecution. Also, the laws do not provide for cybercrime investigation measures, including digital forensics, intelligence gathering, and lawful interception. Although some cybercrime regulatory bodies in Nigeria conduct digital forensics, intelligence gathering, and covert operations, the CPPA, which is the cyber-specific legislation in Nigeria, does not expressly empower these agencies with such investigative powers. The Terrorism Act made provisions for covert operations, intelligence gathering and lawful interception, but this enactment governs terrorism, not cybercrimes. It can be used to investigate terrorist acts tainted with cybercrime or acts of terrorism carried out using the internet or network protocols as a tool.

3.2 *Cybercrime Investigation in the United Kingdom*

The principal cybercrime legislation in the United Kingdom (UK) is the Computer Misuse Act (CMA) 1990. It sets out cybercrime offences and punishments.

Other legislation applicable to regulating cybercrime in the UK include the Communications Act, 2003; the Privacy and Electronic Communications (EC Directive) Regulations, 2003; the Data Protection Act, 2018; the Network and Information Systems Regulations, 2018; and the Malicious Communications Act. The National Cyber Security Centre is crucial in coordinating the response to cyber breaches and developing specialist investigative capabilities. The National Crime Agency's National Cyber Crime Unit leads investigations of cybercrimes in the UK.[56]

3.2.1 National Cyber Strategy 2022

The UK government developed the National Cyber Strategy 2022 (the Strategy) to maintain the country's resilience, capabilities and confidence in the rapidly moving digital ecosystem and ensure adequate protection in cyberspace. The Strategy's five pillars are:

Pillar 1: Strengthening the UK cyber ecosystem.

Pillar 2: Building a resilient and prosperous digital UK.

Pillar 3: Taking the lead in the technologies vital to cyber power.

Pillar 4: Advancing UK global leadership and influence.

Pillar 5: Detecting, disrupting and deterring adversaries. The objectives of Pillar 5 include:

(1) Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens.

(2) Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests and its citizens.

The Strategy outlines a comprehensive legal framework covering numerous cybercrimes, investigative techniques and international cooperation mechanisms.[57] Its central vision is to promote a free, open, peaceful and secure cyberspace. It has made significant impacts in strengthening the country's cybersecurity structure and capabilities.

3.2.2 The Regulation of Investigatory Powers Act

The Regulation of Investigatory Powers Act (RIPA) is the legislation that partly governs the investigative powers of law enforcement relating to the interception and use of electronic communications.[58] It recognises the legal right of

56 National Cyber Strategy 2022, https://www.gov.uk/.

57 'A Hostage to Fortune: Ransomware and UK National Security-Joint Committee on the National Security St', https://publications.parliment.uk/.

58 Regulation of Investigatory Powers Act (RIPA) 2000.

public bodies to carry out digital surveillance and digital access communication held by a person or organisation.[59] The law was explicitly introduced to consider the technological evolution and sophistication of the internet and tools used by terrorists, drug smugglers, and cybercriminals.[60] Public authorities use covert techniques to investigate crimes involving electronic communications.[61] This applies to wide-range investigations that may require obtaining the private information of persons involved. The process must be necessary, lawful and compatible with the fundamental human rights of the persons involved.

The Act regulates the process/methods of covert surveillance that public bodies can carry out. It provides a legal investigative framework authorising public authorities to conduct clandestine surveillance without breaching the Human Rights Act. It categorises covert surveillance into five heads, which are: 'directed surveillance (includes photographing people); intrusive surveillance (includes bugging); the use of covert human intelligence sources (informants and undercover officers, including watching and following people); accessing communications data (record of emails sent, telephone calls made) and intercepting communications (i.e. reading the content of emails, listening to calls)'.[62] It allows public bodies to demand the details of communication records for telephone/internet users from telephone and internet service providers.[63] It compels ISPs to install tools to enable law enforcement agents to monitor internet traffic and intercept emails.[64]

In summary, RIPA provides for covert surveillance and investigation of electronic communication. It gives law enforcement agents the legal right to carry out such investigations and provides a framework of permissible surveillance, which must be compatible with the Human Rights Act.

59 'The Regulation of Investigatory Powers Act (RIPA)' <*https://www.bbc.co.uk/bitesize guides/zpjm6sg/revision/1*> accessed 5 March 2024.

60 'Regulation of Investigatory Powers Act 2000/UK Civil Liberties/The Guardian' [19 January 2009] <*https://www.theguardian.com/commentisfree/libertycentral/2009/jan/14/regu lation-investigatory-powers-act*> last accessed 5 March 2024.

61 'Regulation of Investigatory Power Act (RIPA)' [30 November 2018] <*https://www.hinck ley-bosworth.gov.uk/info/10020/strategies_plan_and_policies/609/regulation_of_investiga tory_powers_act_ripa*> last accessed 3 February 2024.

62 'Regulation of Investigatory Powers Act 2000/UK Civil Liberties/The Guardian'.

63 This includes: the police, intelligence services, HM Revenue and Customs amongst other public bodies.

64 'Regulation of Investigatory Powers Act 2000/UK Civil Liberties/The Guardian' (n 60).

3.2.3 The Investigatory Powers Act

On 29 November 2016, the Investigatory Powers Act (IPA) received Royal Assent in the UK. It amended the RIPA and provides a framework regulating the use and oversight of investigatory powers by law enforcement and security/intelligence agencies.[65] The Act created a regulator, the Investigatory Powers Commissioner, and other Judicial Commissioners to oversee the implementation of powers provided in the Act. It made additional efforts to safeguard privacy rights.

The existence of a robust cybercrime investigation framework does not eliminate the challenges of investigating cybercrime in the rapidly evolving digital sphere. Cybercrime regulatory agencies must keep up with the fast pace of the digital ecosystem and technological changes to navigate the challenges of cybercrime investigation.

4 Limitations of Cybercrime Investigations

Many challenges in cybercrime investigation fundamentally affect the crime's investigation and prosecution. These limitations are jurisdiction, the doctrine of double criminality, anonymity and encryption. They are discussed seriatim below.

4.1 *Jurisdictional Challenge*

Jurisdiction is essential to the dispensation of criminal justice. It is a pivotal question posed in any court of law. A lack of jurisdiction by a trial court would nullify the entire adjudicatory process even if the proceedings were well conducted.[66] Jurisdiction can be based on different issues, such as the actual place where the cybercrime was committed, the offender's country of origin, and the property or person affected by the crime. In the virtual environment, the issue of jurisdiction in international and domestic laws has been raised due to cyber offences' de-territorial nature.[67]

---

65 'Investigatory Power Act', https://www.gov.uk/government/collections/investigatory-powers-bill/ accessed 22 February 2024.

66 KE Oraegbunam, 'Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea from International Law?' [2015] 6 *NAUJILI* <*https://www.ajol.info/index.php/naujilj/article/view/136262*> last accessed 27 February 2024.

67 G Shashikala, 'Problems of Jurisdiction in Cyberspace and its Impact on International and Domestic Laws' http://shodhganga.inflibnet.ac.in/bitstream/10603/113328/5/chapter%20ii.pdf accessed 6 March 2024.

The ease with which an internet user can access a website anywhere globally has led to the internet being described as multi-jurisdictional.[68] The multi-jurisdictional nature of the internet makes it problematic for courts to determine jurisdiction.[69] Questions like whether a particular event in cyberspace is controlled by the laws of the state or country where the website is located, where the internet service provider or user is located, or perhaps by all these laws together have arisen. Menthe argues that jurisdiction is the prevailing conceptual problem for domestic and foreign courts.[70] He added that cyberspace replicates all traditional conflicts-of-law principles and reduces them to absurdity unless perceived as an international space. He suggests that cyberspace should be treated as a fourth global space as this will be helpful for jurisdictional analysis. In customary international law, any other entity's evasion in a sovereign state is not allowed. The Permanent Court of Justice in the *Lotus Case*[71] held that:

> Now, the first and foremost restriction imposed by international law upon a State is that- failing the existence of a permissive rule to the contrary- it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory … except by virtue of a permissive rule derived from international custom or from a convention.

From the preceding, it is clear that the state cannot exercise jurisdiction on persons, events and things physically located in another state (territory).[72]

The transnational nature of cybercrime raises the issue of the jurisdiction in which the offender will be prosecuted. In cybercrime cases, the territorial notion of jurisdiction to prosecute is usually problematic.[73] Generally, the procedural law of the prosecuting country must be adequate to exercise

68 Gabriole Zeviar-Geese, The State of the Law on Cyberjurisdiction and Cybercrime on the Internet' [1997-1998] 1 *Gonz.J.Int'l 1999.*

69 The court in *Zippo Mfg v Zippo Dot Com, Inc*952 F Supp 119 (WD Pa 1997), stated that there is a global revolution looming on the horizon, and the progress of the law in dealing with theavailable scope of personal jurisdiction based on the internet use is in its infancy.

70 Darrel C Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces' [1998] 4(1) <*https://repository.law.umich.edu/mttlr/vol4/iss1/3/*> last accessed 4 March 2024.

71 [1927] PCIJ Ser. A No: 10 available at <*http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm*> last accessed 4 March 2024.

72 Shashikala, (n 67).

73 Susan W Brenner, 'Cybercrime Investigation and Prosecution: he Role of Penal and Procedural Law' [2001] *Murdoch University Electronic Journal of Law* <*http://www.researchgate.net/profile/Susan_Brenner/publication/240610895_Cybercrime_Innvestigation_and*

jurisdiction over cybercrimes legitimately. This is due to the difficulty in determining where the cybercrime was committed. The perpetrator and victim can be located in different countries. Also, the instrument of crime may be computer networks utilised in numerous countries in crime perpetration. Brenner argues that an approach to this problem is to 'broaden the territorial notion of jurisdiction to prosecute so that it allows the nation to prosecute whenever the offender's conduct occurred in whole or in part in the prosecuting nation's territory'.[74]

The term 'Cyber Jurisdiction' has been coined to recognise the government's power and courts' authority over internet users and their activities in cyberspace.[75] Determining cyber jurisdiction involves an application of existing rules.[76] There are two types of cyber jurisdiction. These are (1) cyber jurisdiction in national cases and (2) cyber jurisdiction in international cases.

In national cases, there is cyber jurisdiction in civil and criminal cases. Cyber jurisdiction in civil cases arises when a website or online material leads to committing a civil wrong in another state.[77] The state courts will decide whether jurisdiction exists over the defendant. Federal courts in the US apply the law of forum states subject to the limits of the due process clause.[78] This was illustrated in *Zippo Mfg v Zippo Dot Com. Inc.*[79] Cyber jurisdiction in criminal cases was not an issue until 1996 when it was raised in the *US vs Thomas* case.[80] From these cases, it is arguable that national courts can impose jurisdiction on activities (substantial or otherwise) within the state in the absence of an established cyber-jurisdiction.

4.2 *Doctrine of Dual Criminality*

The doctrine of dual criminality is not one of the significant limitations of cybercrime investigation. However, it is an important aspect worthy of

---

_Prosecution_the_Role_of_Penal_and_Procedural_Law/links/0a85e52dd8b778d095000000.pdf> last accessed 3 February 2024.

74 For example, the 1999 Revision of the Model State Computer Crimes Code, section 10.3.

75 SA Kumar, 'The Concept and Theories of Jurisdiction' <*http://shodhganga.inflibnet.ac.in/bitstream/10603/188821/7/5%20chapter3.pdf*> accessed 3 February 2024.

76 Jillian Raw, 'Cyber Jurisdiction: Where on Earth do you sue?' [2 February 2016] <*https://www.lexology.com/library/detail.aspx?g=3b74fcc1-bd4d-4cdb-aa0c-fbc337033a78*> accessed 25 February 2024.

77 Kumar, (n 75).

78 See *McDonough v Fallon Mc EillgotInc* [1996] Dist Lexis 15139, No 93-4037. *Zippo Mfg v Zippo Dot Com Inc* [1997] 92F Supp 1119 (WD).

79 [1997] 92F Supp 1119 (WD).

80 74 F 3d 701 (6th Cir 1996).

discussion, since extradition is an approach to curb jurisdictional challenges. However, extradition entails dual criminality, which is a universal condition applied to international criminal law institutions.[81]

Dual or double criminality connotes that an act or omission must be considered a crime in two countries, one of which is the country prosecuting the crime.[82] This means that the conduct alleged must constitute a crime and be punishable under the criminal laws of both the surrendering and requesting states. Extradition relating to cybercrime will be problematic if the nation requesting it has no equivalent offence.

Another problematic aspect is the wide divergences in punishment and sentencing. If the sentence in the requesting state is not commensurate with the crime, it defeats the purpose. 'Double criminality can also provide a prime example of the tension between one country's desire to enforce its laws and another country's determination to preserve its legal sovereignty'.[83] The process may be politicised by the nations involved. It is contended that the paramount goal of extradition is to prevent criminals from evading justice. Governments are encouraged to insert an extradition provision in their cybercrime laws. Section 51 of the CPPA provides that 'offences under this Act shall be extraditable under the *Extradition Act*.'[84] Adequate cybercrime punishments and extradition provisions in all nations' cybercrime laws will ease extradition hurdles in prosecuting cybercrime.

4.3 *Anonymity Challenge*

Anonymity is an advantageous medium for cybercriminals to conceal their identity online using tools such as proxy servers, spoofed email, IP addresses or anonymous emailers.[85] Using anonymising tools by offenders makes digital investigative methods of cybercrime difficult for law enforcement agents. The use of different internet access points[86] by an offender will require significant

81 Lech Gardocki, 'Double Criminality in Extradition Law' [04 July 2014] <*https://www.cambridge.org/core/journals/israel-law-review/article/abs/double-criminality-in-extradition-law/923684i068D61B41E7ACFECDC867B1F6*> last accessed 1 March 2024.

82 Fey- Constanze Blaas, Double Criminality in International Extradition Law.

83 Kim Soukieh, 'Cybercrime: The Shifting Doctrine of Jurisdiction' <*https://www.austlii.edu.au/au/journals/CanLawRw/2011/9.pdf*> last accessed 5 February 2024.

84 CPPA, 2015. See Extradition Cap E24 LHJ 2004.

85 Jonathan Clough, 'Principles of Cybercrime' (2nd ed United Kingdom: Cambridge University Press 2015).

86 For example, another person's Wi-Fi connection, a computer at a cyber café or publicly available internet connections.

efforts on the part of investigators to trace back an IP address.[87] Various anonymising services are available on the internet, making it challenging to track offenders based on their IP addresses. Some anonymising services are proxies, virtual private networks, and Tor.

Importantly, anonymity is an excellent medium for people to speak out against or criticise oppressive political regimes or government policies. So, law enforcement authorities must acknowledge the distinction between anonymity and privacy so as not to cross the line.

4.4 *Encryption Challenges*

Encryption is a technique that encodes communication preceding transmission to make such communication unreadable if intercepted.[88] Encrypting messages is 'the use of algorithms[89] to encrypt data to render it unintelligible to third parties who do not have the secret information necessary to decrypt the message'.[90] The goal is for the intended recipient with the key to the message to decode and restore it to its original form. Encryption has been widely used legitimately in electronic schemes to secure transaction data. Cybercriminals and terrorists have also used it to protect their communication from interception from law enforcement agents and investigators.

Encryption software was designed originally for government use to protect files from persons without proper security clearance. In 1991, Phil Zimmerman, a computer programmer, released a version of encryption software, Pretty Good Privacy, to the public free of charge.[91] Multiple software companies have developed encryption software programs, with businesses seeking to protect their data as their target market. The availability of encryption software has enabled individuals and criminals to abuse the tool in cyberspace.

In the US and Netherlands, law enforcement authorities have warned that their ability to read the contents of intercepted communications is declining.[92]

87 Oerlemans, (n 36).

88 Marjid Yar, *Cybercrime and Society* (2nd edn London: Sage Publications Inc 2013).

89 is a process, procedure, formula or set of rules to be followed in calculations which allows a computer to solve a problem or complete a task. See Ifeoma E. Nwafor, AI Ethical Bias: A Case for AI Vigilantism (AIlantism) in Shaping the Regulation of AI, (2021) *IJLIT* 29(3) https://doi.org/10.1093/ijlit/eaab008.

90 P Gerard and G Broze, 'Encryption: An Overview of European Policies: IT, Telecoms and Broadcasting' (1997) 3(4) *CTLR* 168.

91 Moore, (n 20).

92 There are various laws and policies on the use of encryption. For instance, the United Kingdom's WhitePaper on 'Regulatory Intent Concerning Use of Encryption on Open Networks', DTI, 10 June 1996. There is an encryption provision in the Electronic Communications Bill.

This is a result of the use of encryption. It challenges law enforcement officials in cybercrime investigations in two situations. These are encryption in transit (i.e. during the analysis of encrypted data in transit) and encryption in storage (i.e. encrypted data already stored in a computer). Encryption can be used positively to protect sensitive information or negatively when used in furtherance of cybercrime. The Nigerian Cybercrime Act is silent on the legitimate use of encryption. It should make provisions for users of encryption techniques to disclose the key to law enforcement agents if needed.

4.5 *Lessons for Nigeria*

Numerous enactments enable various institutions and agencies to investigate and prosecute cybercrime-related offences in Nigeria.[93] This leads to investigative and prosecutorial competition or clashes between the agencies and institutions. The UK's RIPA and IPA are good guidelines for an effective cybercrime investigation framework in Nigeria. The IPA created a regulator to oversee the application of the provisions of the Act. This is absent in the Nigerian scene. There is no regulatory agency or body with oversight functions on implementing the CPPA, which is the cyber-specific legislation in Nigeria. Also, the CPPA does not explicitly provide for covert surveillance and investigation of electronic communication. Lessons can be learnt from the IPA to close the gaps identified in the Nigerian CPPA. The RIPA categorised covert surveillance into five heads: 'directed surveillance, intrusive surveillance, the use of covert human intelligence sources, accessing communications data and intercepting communications'. The CPPA and ACJA did not provide such categorisation and the lawful implementation of such covert surveillance.

Additionally, the ACJA should provide for cybercrime investigation measures, including digital forensics, intelligence gathering, and lawful interception. The Act should expressly authorise law enforcement officers to conduct permissible covert operations, intelligence gathering and lawful interception relevant to practical and lawful investigation of cybercrime offences. RIPA gives law enforcement agents the legal right to carry out such investigations and provides a framework of permissible surveillance, which must be compatible with the Human Rights Act. Nigeria needs a cybercrime investigative framework that authorises the lawful investigation of cybercrime, which includes permissible and legal covert investigative processes that do not breach a suspect's human rights.

93 The EFCC Act, the Police Act, the Cybercrime Act etcetera. See Nwafor, (n 6).

5 Conclusion

This paper examined the investigative framework of cybercrime in Nigeria *vis-a-vis* the law and practice in the United Kingdom. It identified the shortcomings of Nigerian legislation in investigating cybercrime offences. The study highlights the differences between cybercrime investigation and criminal investigation and analyses the limitations of investigating cybercrime. It found that no law explicitly gives law enforcement agents the legal right to conduct digital forensics and lawful interception during cybercrime investigations in Nigeria. My investigation shows that the Nigerian legal framework does not adequately empower law enforcement agencies with specialised investigative powers to investigate and prosecute cybercrime offences. The complexity, severity and impact of cybercrime in Nigeria deserve a comprehensive and effective cybercrime investigative framework. To bridge the gaps identified, I propose that a separate investigative framework should be developed to ensure the effective investigation of cybercrime offences in Nigeria. The CPPA and the ACJA should provide a framework of legal and permissible surveillance and investigation of electronic communication that is compatible with the fundamental human rights enshrined in the Nigerian Constitution and the African Charter on Human and Peoples' Rights. The existence of an adequate legislative, institutional and investigatory framework will yield great results in prosecuting cybercrime and possibly deterring prospective cybercriminals. Lessons can be drawn from the UK's RIPA and IPA relating to investigating cybercrime and upholding the human and privacy rights of Nigerian citizens.