LEGAL AND INSTITUTIONAL FRAMEWORK FOR CYBERCRIME INVESTIGATION AND PROSECUTION IN NIGERIA: THE NEED TO STRENGTHEN THE EXISTING STRUCTURES*[1]

Abstract

The investigation and prosecution of cybercrime in Nigeria rely on a legal and institutional framework that faces numerous challenges. Nigeria, like many other countries, has witnessed a significant increase in cybercrimes due to the rapid growth of information and communication technologies. To address this growing concern, Nigeria has enacted legislation such as the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, which provides a legal framework for combating cybercrimes. However, the effectiveness of this legislation is hindered by several shortcomings. This study highlights the critical challenges in the legal framework for cybercrime investigation and prosecution in Nigeria. It examines the existing structures for cybercrime investigation and prosecution in Nigeria, identifies the weaknesses within them, and emphasizes the imperative to strengthen these structures to effectively combat cybercrimes. In carrying out this research, the researcher employed the doctrinal method of research wherein the descriptive and analytical approaches were adopted. Also, the primary sources of legislation, books and judicial authorities as well as secondary sources of journal articles, publications etc. were used. This work found that there is a need for comprehensive legislation that covers emerging cyber threats and addresses gaps in existing laws. Also, the institutional framework for cybercrime investigation and prosecution in Nigeria requires significant enhancement. This includes the allocation of adequate resources, both human and technological, to law enforcement agencies responsible for cybercrime investigations. Furthermore, coordination and collaboration among different agencies involved in cybercrime investigation and prosecution need improvement and lastly, public awareness and engagement play a crucial role in combating cybercrimes. This article ended on the note that Nigeria's legal and institutional framework for cybercrime investigation and prosecution requires significant strengthening to effectively combat the rising threat of cybercrimes. Enhancing the legal framework, investing in resources and training, improving coordination among agencies, and fostering public awareness are crucial steps towards building a robust cybersecurity ecosystem. By addressing these challenges, Nigeria can mitigate the risks posed by cybercrimes and safeguard its digital infrastructure and citizens against evolving threats.

Keywords: Cybercrime, Investigation and Prosecution, Legal and Institutional Framework, Nigeria

1. Introduction

The rise of cybercrime in Nigeria has necessitated the development of a legal and institutional framework to combat these illicit activities effectively. The proliferation of information and communication technologies has led to an increase in cybercrimes globally, and Nigeria is not exempt from this trend. Online fraud, identity theft, hacking, and other forms of cybercriminal activities pose significant threats to individuals, businesses, and the overall security of the digital ecosystem in Nigeria. In response to this growing concern, Nigeria has taken steps to establish a legal framework for addressing cybercrimes. The Cybercrimes (Prohibition, Prevention, etc) Act of 2015 serves as the primary legislation governing cybercrime investigation and prosecution in Nigeria. This Act criminalizes various cyber offenses and provides the legal basis for law enforcement agencies to investigate and prosecute cybercriminals. However, despite the existence of this legislation, several critical challenges hamper its effectiveness. One of the primary challenges is the need for a comprehensive and up-to-date legal framework that adequately addresses emerging cyber threats. The rapid evolution of cybercriminal techniques necessitates proactive legislation that can keep pace with these advancements. The current legislation may have gaps or inadequacies that cybercriminals exploit, requiring regular reviews and amendments to strengthen the legal framework. In addition to the legal challenges, the institutional framework for cybercrime investigation and prosecution in Nigeria requires significant strengthening. Adequate allocation of resources, both financial and technological, is crucial to equip law enforcement agencies with the necessary tools and infrastructure to effectively combat cybercrimes. Insufficient funding, limited access to advanced technologies, and a shortage of trained personnel pose significant obstacles to successful investigations and prosecutions. It is against this background that this article examined the legal and institutional frameworks for cybercrime

[1] ***By EOC OBIDIMMA, BA, LLB, LLM, PhD, BL**, Professor of Law, Faculty of Law, Associate Provost (Humanities) College of Postgraduate Studies, Nnamdi Azikiwe University, Awka. Tel: 08034003436, 08090255555. Email: eocobidimma@gmail,com;

***Richard Onyekachi ISHIGUZO, PhD Candidate,** Faculty of Law, Nnamdi Azikiwe University, Awka; Law Officer, Nigerian Police Force attached to Legal/Prosecution Unit, Delta State Police Command, Asaba, Delta State, Tel: 08068515729, 08058237739. Email: rich4just@yahoo.com, rich4just12@gmail.com.

investigation and prosecution in Nigeria with a view to recommending how the existing frameworks can be strengthened for efficiency, effectiveness and maximum productivity

2. Legal Framework for Cybercrime Investigation in Nigeria

In Nigeria today, the activities of cyber criminals have become a threat to the society.[2] With the arrival of information age, legislatures have been struggling to redefine laws that fit crimes committed by cyber criminals.[3] Initially, there were no specific laws in Nigeria for combating computer crimes.[4] This led to the creation of an ideal environment for criminals to freely operate without any law to combat their criminal activities.[5] It is a general principle of law that an uncodified crime is not punishable, as provided in Section 36 (12) of the 1999 Constitution of the Federal Republic of Nigeria[6]. The factors involved in the prosecution of a crime under the Nigerian law emanates from one major source: legislation.[7] As a result of this, the Cybercrime Act 2015 has been enacted for the prohibition, prevention, detection, response and prosecution of cybercrimes and for other related matters. Aside the new Cybercrime Act, there are laws that indirectly relate to the prosecution of cybercriminals. These laws include Economic and Financial Crimes Commission (Establishment) Act 2004, Advanced Fee Fraud and other Fraud Related Offences Act, Nigerian Criminal Code, Money Laundering Prohibition Act and the Nigerian Evidence Act. These and other laws regulating cybercrime in Nigeria would be discussed below.

Cybercrime Act 2015: This is an Act that provides for the prohibition, prevention, detection, response and prosecution of cybercrimes and other related matters. The Act is divided into eight parts. Part I provides for the objectives and application of the Act, Part II provides for the protection of critical national infrastructure, part III provides for offences and penalties, Part IV provides for duties of service providers, Part V provides for administration and enforcement, Part VI of the Act provides for search, arrest and prosecution, Part VII provides for jurisdiction and international co-operation and Part VIII provides for miscellaneous. Part III of the Act discusses the offences and penalties in relation to cybercrimes. Through these provisions, crimes committed through computer and computer networks are codified and thus punishable under Nigerian law. Before the enactment of these provisions, only internet related fraud was actually a punishable cybercrime. But this Part of the Act provides for offences and penalties in relation to cybercrimes. The legislation also affords law enforcement officers broad search, arrest, and seizure powers, including some that do not require judicial oversight[8]. Section 33 of the Act also vests authority on the Federal High Courts to try and sanction offences committed under this Act.

Economic and Financial Crimes Commission (Establishment) Act[9]: This Act was enacted to repeal the Financial Crimes Commission (Establishment) Act, 2002. Section 1 of the Act establishes a body known as the Economic and Financial Crimes Commission (EFCC). Section 5 of the Act charges the commission with the responsibility of the enforcement and the due administration of the Act, the investigating of all financial crimes including advance fee fraud money laundering, counterfeiting, illegal charge transfers and also the prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney-General of the Federation. Criminal activities that would come under these economic crimes would include the activities of the 'Yahoo boys' whose activities are sabotage on the economy of the country.[10] Section 5 has been the basis for various actions of EFCC including Emmanuel Nwude (the accused) in the case of *Federal Republic of Nigeria v. Chief Emmanuel & Ors*[11] wherein the accused was convicted of cybercrime.

Advanced Fee Fraud and other Fraud Related Offences Act[12]: The Act was enacted to prohibit and punish certain offences pertaining to advance fee fraud and other fraud related offences and to repeal other Acts related

[2] Oke R, Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT), *The Journal of Philosophy, Science and Law,* vol. 12, 2012.
[3] Ani L, Cybercrime and National Security: The Role of the Penal and Procedural Law, *Law and Security in Nigeria,* pp. 197-232 at p. 197.
[4] Ehimen R & Bola A, Cybercrime in Nigeria, *Business Intelligence Journal,* Vol. 3(1), 2010, pp. 93-98.
[5] Ibid.
[6] Cap C23, Laws of the Federation of Nigeria, 2004.
[7] Ashaolu D, Combating Cybercrimes in Nigeria, *McAsh's Thoughts,* 24 December, 2011. P. 1. Retrieved online from http://blogs.law.harvard.edu/mcash/2011/12/24/combatingcybercrimesinnigeria. Accessed on 20th April, 2023.
[8] Ibid, Section 28.
[9] Economic and Financial Crimes Commission (Establishment) Act 2002, Cap E1 Laws of the Federation of Nigeria, 2010.
[10] Ehimen O & Bola A, Cybercrime in Nigeria, *Business Intelligence Journal*, 3(1) 2010, pp. 93-98 at p. 95.
[11] Suit No: CA/245/05. Retrieved online from http://www.cenbank.gov.ng/419/cases.asap. Accessed on 20th April, 2023.
[12] Advanced Fee Fraud and other Fraud Related Offences Act 2006, CAP A6, Laws of the Federation of Nigeria, 2010.

therewith. Advance fee fraud is a vexing threat and a major problem in Nigeria today.[13] The Act provides for ways to combat cybercrime and other related online frauds. The Act provides for a general offence of fraud with several ways of committing it, which are by obtaining property by false pretence, use of premises, fraudulent invitation, laundering of fund obtained through unlawful activity, conspiracy, aiding among other crimes. Section 2 makes it an offence to commit fraud by false pretence. This Section can be used to prosecute criminals who commit cybercrimes like computer related fraud, where the offender uses an automation and software tools to mask criminals' identities, while using the large trove of information on the internet to commit fraud.

Money Laundering (Prohibition) Act[14]: Another related law regulating internet scam is the Money Laundering (Prohibition) Act 2004. It makes provisions to prohibit the laundering of the proceeds of crime or an illegal act. Section 14 (1) (a) of the Act prohibits the concealing or disguising of the illicit origin of resources or property which are the proceeds of illicit drugs, narcotics or any other crime. Section 17 and Section 18 of the Act also implicates any person corporate or individual who aids or abet illicit disguise of criminal proceeds. Section 10 makes life more difficult for money launderers by mandating financial institutions to make compulsory disclosure to National Drugs Law Enforcement Agency in certain situations prescribed by the Act.

Independent Corrupt Practices and Other Related Offence Act 2000: The Independent Corrupt Practices (ICPC) and Other Related Offences Act seek to prohibit and prescribe punishment for corrupt practices and other related offences. The ICPC has the mandate to combat corruption, including bribery, fraud and other related offences.[15] The connection between the ICPC Act and cybercrime is that some offences outlined in the Act are perpetuated using the internet or electronic device as a medium[16]. The Independent Corrupt Practices and Other Related Offences Commission (ICPC) Act of 2000 is primarily focused on combating corruption and related offenses in Nigeria. While it does not specifically address cybercrime in great detail, it does contain provisions that can be applied in the fight against cybercrime.

Criminal Code[17]: This Act was enacted to establish a code of criminal law in Nigeria. The criminal code criminalizes and sanctions any type of stealing of funds, in whatever form and also false pretences. Although, cybercrime is not specifically mentioned here, crimes such as betting, theft and false pretences performed through the aid of computers and computer networks is a type of crime punishable under the criminal code. Section 418 defines false pretence as any representation made by words, writing, or conduct of a matter of fact, either past or present, which representation is false in fact and which the person making it knows to be false or does not believe to be true.' Cybercrime that would fall under this Section would mainly bother on computer related fraud. By their fraudulent action, cybercriminals deceive their victims by pretending to have abilities or skills which ordinarily they do not have or possess. Most of the activities of these cyber criminals bother on false pretences and cheating which Section 419 and 421 of this Act prohibit respectively. Section 419 states that 'any person who by any false pretence, and with the intent to defraud, obtains from any other person anything capable of being stolen or induces any other person deliver to any person anything capable of being stolen, is guilty of a felony and is liable to imprisonment for three years.'

Nigerian Evidence Act: This Evidence Act repeals the old Evidence of 1945. As opposed to the old Evidence Act, this Act allows for admissibility of digital and electronic evidence. Before the enactment of the Act, electronically generated evidence was not admissible in Nigerian courts, thereby creating a serious impediment in the prosecution of cybercrimes. This Act is therefore a big step in the right direction towards the prosecution of cybercrime activities in Nigerian courts. Following age-long need for review of evidence laws to become age compliant, digital evidence is now admissible on Nigerian courts. The Act provides for the definition of a computer which was not included in the 1945 Evidence Act. Under the Act, a computer is defined as 'as any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison or any other process'.[18] Section 84(1)-(5) introduces the admissibility of statements in documents produced by computers. The Section has now made it possible for facts for which direct oral can be given to be equally evidence by a computer-produced document containing such facts, subject however to condition precedents as to the document, the computer from

[13] Chawki, M, Nigeria Tackles Advance Fee Fraud, *Journal of Information, Law & Technology,* Vol. 1, 2009, *pp.* 1-20 at p. 4.
[14] Money Laundering (Prohibition) Act Cap M18, Laws of the Federation of Nigeria, 2010.
[15]Awopeju, A, An Appraisal of Nigerian Independent Corrupt Practices and Other Related Offences Commission (ICPC), 2001-2013, Review of Public Administration and Management, 3(7) July 2015. Retrieved online from https://www.arabianjbmr.com/pdfs/RPAM_vol_4_7/6.pdf. Accessed on 20th April, 2023.
[16] Nwafor, IE *Cybercrime and the Law: Issues & Developments in Nigeria* (Lagos: CLDS Publishing, 2022) p.44.
[17] Criminal Code Act CAP 38, Laws of the Federation of Nigeria, 2010.
[18] Evidence Act, Section 258.

which it was generated and the person who generated it or manages the relevant activities captured in the document, for instance cybercafé managers, secretaries, ATM card users or experts – the list is endless.[19] Thus, in *R v. Spiby*[20] the English Court of Appeal held that the trial judge had properly admitted evidence of computer printouts of a machine which had monitored hotel guests' phone calls.

3. Institutional Framework for Cybercrime Investigation and Prosecution in Nigeria

The enactment of the Cybercrime Act and other extant laws and the National Cybersecurity Policy and Strategy framework as a tools to fight the menace of cybercrime in Nigeria is not sufficient as what makes a good society is not only the enactment of good laws, but also the ability to enforce the laws, coupled with the willingness of the populace to embrace them and for any country in the world to effectively actualize the objectives of its laws, certain institutions and persons have to be put in place under the laws and this juncture, this article will now proceed to consider some of Cybercrime Institutions in Nigeria.

Office of the Attorney-General of the Federation: The Attorney-General of the Federation is responsible for strengthening and enhancing the existing legal framework to ensure the followings: conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards; maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security; and effective prosecution of cybercrimes and cyber security matters[21]. The Cybercrime Act[22], like the Nigerian Constitution[23], clothed the Attorney-General powers with respect to prosecution of cybercrime offences and granting of approval before certain offences under the Cybercrime Act can be prosecuted. The office of the Attorney-General is also solely responsible for ensuring that any assets or property of a convict forfeited to the Federal Government are effectively transferred and vested in the Federal Government of Nigeria[24].

Economic and Financial Crimes Commission (EFCC): The Economic and Financial Crimes Commission (EFCC) is one of the Nigerian Law enforcement agencies that investigates and prosecutes corruption and financial crime cases. The agency has extensive special and police powers which includes the power to investigate persons and/or properties of persons suspected of breaching the provision of the EFCC Establishment Act of 2022 and any other law or regulation relating to financial and economic crimes in Nigeria. It is also empowered to enforce all the pre & post 1999 anti-corruption and anti-money laundering laws. It has recorded considerable success in investigating and prosecuting financial and economic crimes that can be classified as cybercrimes.[25] It has recovered monies and assets derived from crime worth over billions of dollars and has made restitution to victims of 419 fraud after successful investigations.

Nigerian Financial Intelligence Unit: The Nigerian Financial Unit (NFIU) is the Nigerian arm of the global Financial Intelligence Units (FIUs).[26] It seeks to adhere to international standards on combating money laundering, financing of terrorism and proliferation. It was established in 2005 by the EFCC and domiciled as an autonomous unit operating in the African Region.[27] The EFCC Act of 2004 and the Money Laundering (Prohibition) Act 2011 (as amended in 2012) confer powers on the NFIU.[28] The Unit was established based on the requirements of Recommendation 29 of the Financial Action Task Force (FATF) Standard and Article 14 of the United Nations Convention Against Corruption (UNCAC).[29] It formulates coordinated policies that aim to combat money laundering, terrorist financing and serious financial crimes. In 2018, President Muhammadu Buhari signed the Nigerian Financial Intelligence Unit bill (NIFU) 2018 into law.[30] The signing of the new Act makes NIFU independent of EFCC. The Act creates NIFU to be domiciled in the Central Bank and work autonomously and independently.[31] The Act establishes the NIFU as the central body in Nigeria responsible for

[19] Chinedu L, Regulation of Cybercrime in Nigeria: A Critical Appraisal, (Unpublished, LLB Thesis) Imo State University, Owerri, 2014.
[20] (1990) 91 Criminal Appeal Review, p. 186.
[21] Ibid, Section 41(2).
[22] Cybercrime Act, Section 47.
[23] Constitution of the Federal Republic of Nigeria, 1999 (As Amended), Cap 23, Laws of the Federation of Nigeria, 2004. Section 174.
[24] Cybercrime Act, Section 48 (2) & (3).
[25] Examples of these cases are the case of *FRN v. Odiawa* (2010) LPELR-CA/L/124/2008*; Amadi v. FRN* CA/L/389/2005.
[26] On information about the NIFU, See http://www.nifu.gov.ng/index.php/nifu. Accessed on 25th April, 2023.
[27] Ibid.
[28] Nwafor, op. cit. p. 35.
[29] Ibid.
[30] Nseyen, N, Buhari signs Nigerian Financial Intelligence Unit Bill into Law (12 July 2018). Retrieved online from http://www.dailypost.ng. Accessed on 25th April, 2023.
[31] Nigerian Financial Intelligence Unit Act 2018, Section 2(3)

requesting, receiving, analyzing and disseminating financial intelligence reports and other information to all law enforcement, security and intelligence agencies and other relevant authorities.

Nigerian Cybercrime Working Group: The Nigerian Cybercrime Working Group (NCWG) is an establishment of the Federal Executive Council (FEC) on the recommendation of the then President of Nigeria on 31st March 2004. It is an inter-agency body comprising all key law enforcement, security, intelligence, and ICT and ICT agencies of government and key private sector ICT organizations.[32] The group was created to seek ways of tackling the menace of 419 fraud in Nigeria.[33]

Cybercrime Advisory Council: As part of efforts to combat cybercrime in Nigeria, the Act established Cybercrime Advisory Council which consists of a representatives of different ministries and agencies listed under the first schedule to the Act and the representative required from each of the ministries and agencies shall be an officer not below the Directorate Cadre in the Public Service or its equivalent and the functions and powers of the council includes the followings: (c) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues; (d) establish a program to award grants to institutions of higher education to establish Cyber Security Research Centers to support the development of new cyber security defences, techniques and processes in the real-world environment; [e] promote Graduate Traineeships in cyber security and computer network security research and development.[34]

Computer Professionals' Registration Council: The Cybercrime Act,[35]empowers the Computer Professionals' Registration Council to register all operators of a cybercafé as a business in addition to a business name registration with the Corporate Affairs Commission and in way of checkmating the activities that goes on at cybercafé, the operators are also mandated in addition the above-mandatory registration, to maintain a register of users through a sign-in register and such register must be made available to law enforcement personnel whenever needed and to further keep the operators alive to their responsibility of ensuring that internet fraudsters do not use their cybercafé as base for their heinous activities, the law provides that in the event of prove of connivance by owner of the cybercafé by the prosecutor in the case of online fraud using a cybercafé, such owners shall be liable to a fine of $42,000,000.00 or imprisonment for a term of 3years or both.[36]

Nigeria Police Force (NPF): Section 214(1) of the constitution (1999) provides that "there shall be a police force for Nigeria which shall be known as the Nigeria Police Force (NPF). The NPF is responsible for the prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the protection of lives and property and the enforcement of all laws and regulations made by the Federal and State Government as well as bye-laws made by the Local Government authorities. The researcher is interested in this population set because there is a sub-unit called Special Fraud Unit (SFU)[37] which is charge with the responsibility of apprehending and carrying out forensic investigation of cybercriminal activities in Nigeria. It will also provide understanding into the approaches adopted by the Law Enforcement Agencies in combating cybercrime activities.

Financial Institutions: The financial institution by the contractual duty of safety policy the owes to their customers' are under obligation to ensure that effective counter-fraud measures are put in place to safeguard customers' sensitive information, where there is failure on the part of any financial institution to put in place effective counter-fraud and security breach take place, the financial institution would be held for negligence subject to proof by the customer.[38] The Act further mandate the financial institution to verify the identity of its customers carrying out electronic financial transaction by requiring the customers to present document bearing their full details by applying the principle of known your customer in documentation of customers proceeding execution and the law further prescribed punishment for any organization that fails to obtain proper identity of customer before executing customer electronic instructions.[39]

---

[32] Ezeoha, AE, Regulating Internet Banking in Nigeria: Some Success Prescriptions - Part2, *11(2) Journal of Internet Banking and Commerce.* Retrieved online from http://www.icommercecentral.com/open-access/regulating-internet-banking-in-nigeria-some-success-prescriptions-part-1-12.pdf. Accessed on 25th April, 2023.
[33] Chawki, op. cit.
[34] Cybercrime Act, Sections 42 & 43.
[35] Ibid, Sections 7(1)(a)
[36] Ibid, Section7(1) (b) (2-4)
[37] Retrieved online from www.specialfraudunit.org.ng. Accessed on 25th of April, 2023.
[38] Ibid, Section 19 (3)
[39] Ibid, Section 37(1) & (2).

4. Challenges to Effective Investigation of Cybercrime in Nigeria

There is no gainsaying that criminal investigation generally is cumbersome and investigation of cybercrime is more complex because these are crimes committed in virtual scene where criminals are undercover and investigating crimes that took place in virtual scene will a lot of technical skill and expertise for investigators to effectively and efficiently a detail discreet investigation and some of the factor inhabiting effective cybercrime investigation in Nigeria includes the followings:

Inadequacy of Legal Framework: Before the advent of Nigeria Cybercrime (Prohibition, Prevention ETC) Act, 2015 there is no direct law for curbing of cybercrime, most of the existing laws only made allusion one way of the other to some of the offences under the cybercrime Act and the vacuum gave most of the cybercriminals opportunity to operate freely without been checkmated for their illicit activities. The success or failure of the Law Enforcement agencies in the performance of their Constitutional duties of detecting crime, preventing crime, apprehending offenders, investigating crime and prosecuting offenders with sole aim of maintaining law and order is wholly dependent on the existing on the existing adequate legal framework in place.

Inadequate Resources: The success or failure of the Law Enforcement agencies in the performance of their Constitutional duties of detecting crime, preventing crime, apprehending offenders, investigating crime and prosecuting offenders with sole aim of maintaining law and order is also dependent on the number of resources at their disposal. The law enforcement agencies are often incapacitated by inadequate resources in carrying out their mandates in investigating cybercrimes. Investigation of complex crimes like cybercrimes requires collection and preservation of data evidence that will be used in court for effective prosecution of offenders involve and collection and storage of data evidence which most times requires traveling asides the shores of Nigeria involves huge amount of money which our Nigeria investigators involved in cybercrime investigation do not have and this lack of adequate resources limit them to conducting armchair investigation that made of efforts to effectively prosecute cybercrime offender an effort in futility.

Lack of Skilled Personnel: One of the challenges with cybercrime investigation in Nigeria is that aside the fact that most of the officers involved in the investigation of cybercrime are computer illiterates, majority of them as the training they had during their six months/below two years college training, they have not attended any further training especially on how to investigate crimes like cybercrime that usually occur on virtual world cutting across many countries with most of the offender's identity remaining anonymity and investigating these crimes by most of this officers without the requisite professional training on prevention and investigation of transnational crime and with little or no computer training makes them unable to efficiently conduct a detail discreet investigation in such cases. These unskilled officers also lack the proficiency requires to obtain data evidence from the virtual scene of cybercrime and preserve such digitally obtained data evidence against virus attacks and even if a direct and accurate information is provided to the unskilled investigating officer, he will still not achieve any positive result duo his ignorant on the applications of the information and this made tracing criminals online in real time can be difficult to investigating officers who have little or no knowledge or mechanism to obtain traffic information.

Extradition or Doctrine of Dual Criminality: The doctrine of dual criminality becomes a serious in cybercrime investigation when investigation of such crime involves extradition of the offender and this is because the act or omission necessitating the extradition must have been considered a crime and punishable under the criminal laws of both the surrendering and requesting state because if same act or omission does not constitutes a punishable crime in the two countries, extradition relating to cybercrime will be problematic and as such, a person who commits an offence in Nigeria may not be extradited if his offence is not criminalized in the other state.

Anonymity Challenge: Most times the cybercriminals usually conceal their identity using different apps which may include: proxy servers, spoofed email or IP addresses and the use of anonymity tools by offenders makes digital investigative method of cybercrime difficult for law enforcement agents. The use of different internet apps by cybercriminals to hide their identity will require serious efforts on the part of skilled investigators to trace back the hidden identity. It is always difficult for investigators to unearth the true identity of the criminals who operate in virtual world. Various anonymity services are available on the internet, making it challenging to track down offenders based on their IP addresses. Some anonymity service includes: proxy, virtual private network, and Tor.

Encryption Challenges: Encryption is a technique used to encode communications proceeding transmission to make such communication unreadable if intercepted.[40] Encrypting messages means the use of algorithms to encrypt data to render it unintelligible to third parties who do not have the secret information necessary to decrypt the message.[41] The goal is for the intended recipient who has the key to the message to decode and restore it to its original form.[42] While companies and organizations have legitimately used encryption to secure their transaction data in electronic scheme, cybercriminals and terrorist have also taken advantage of it to guide their fraudulent communication from law enforcement agents.

Jurisdictional Challenge: Cybercrime is an offence that mostly cut across borders. A fraudster in Nigeria may target a victim in Canada and use a cohort based in Turkey to facilitate and finalize the crime and in situation like the one presented above, jurisdiction can be based on different issues such as the actual place the cybercrime was committed, the offender's country of origin, the property and/or person affected by the crime. In the virtual environment, the issue of jurisdiction in international and domestic laws has been raised owing to the de-territorial nature of cyber offences[43]. The ease with which an internet user can access a website anywhere globally had led to the internet being described as multi-jurisdictional. The multi-jurisdictional nature of the internet makes it problematic for courts to determine jurisdiction. Question like whether a particular event in cyberspace is controlled by the laws of the state or country where the website is located, or perhaps by all these laws arises.

Prosecution of Cybercrime: The law provides that relevant law enforcement agencies shall have power to prosecute offences under the Act[44] subject to powers of the Attorney-General.[45] Criminal Prosecutions are under the control of the Attorney General of the Federation. That explain why he can take over and continue criminal proceedings or discontinue them even if they were instituted by any other authority or person.[46] The full panel of the Nigerian Apex court has held that: institution of proceedings against any person before any court in Nigeria other than a court martial is not exclusive preserve of the Attorney-General of the Federation and/or his counter in the State. There are several agencies, bodies and institutions, beyond the Attorney-General of the Federation and/or his counterpart in the state, with powers to prosecute specific offences. This becomes more compelling given the provision of the Economic and Financial Crimes Commission (Establishment) Act Cap. E1, Laws of the Federation of Nigeria, Vol. 5, 2004. The Provisions of Sections 7(1) and (2) and 13 (1), (2) and (3) of the Act empowers the prosecutors in the Legal and Prosecution Unit of the EFCC to prosecute any person who commits any of the offences that the Commission is empowered to prosecute under the Act.[47] The court with the requisite jurisdiction to entertain any cybercrime charge in Nigeria is the Federal High Court located in any part of Nigeria, regardless of the location where the offence is committed.[48]

5. Conclusion and Recommendations

In conclusion, Nigeria's legal and institutional framework for cybercrime investigation and prosecution requires strengthening to effectively address the growing menace of cybercrimes. Enhancing the legal framework, investing in resources and training for law enforcement agencies, improving coordination among different agencies, and fostering public awareness are critical steps towards building a robust cybersecurity ecosystem in Nigeria. By addressing these challenges, Nigeria can mitigate the risks posed by cybercrimes and ensure the security and integrity of its digital infrastructure and citizens in the face of evolving cyber threats. Below are the discussions of the various recommendations towards addressing the challenges identified above:

1. The Cybercrime Act should also provide for compensatory damages and other form of reliefs to victims who suffer from the acts of these cybercriminals, just as it is provided for in the American jurisdiction, under Subsection 1030(g) of the Computer Fraud and Abuse Act.
2. Although Part VI of the Act provides for the search, arrest and prosecution of cybercriminals by law enforcement officers, it is in the opinion of this writer that these provisions are not enough in the

[40] Yar, M, *Cybercrime and Society* (2nd Edn., London: Sage Publication Inc. 2013) p. 58.
[41] Gerard, P & Broze, G, Encryption: An Overview of European Policies: IT, Telecoms and Broadcasting (1997) 3(4) *CTLR,* 168.
[42] Ibid.
[43] G Shashikala, G, Problems of Jurisdiction in Cyberspace and its Impact on International and Domestic Laws. Retrieved online from http://shodhganga.inflibnet.ac.in/bitstream/10603/113328/5/chapter%20ii.pdf. Accessed on 20th May, 2023.
[44] Cybercrime Act 2015 s.47 (1)
[45] *See* sections 174 & 211 of the 1999 Constitution of the Federal Republic of Nigeria that give the Attorney-General of Federal of the Federation & States powers to institute, take-over and discontinue criminal cases.
[46] *Ezekiel v A-G Federation* (2017) Vol. 266 LRCN 1
[47] *Shema v FRN* (2018) 9 NWLR Part 1624 337, see also section 66 of the Police Act, 2020 which empowers a Legal Officer with the Police to Prosecute before superior courts.
[48] Cybercrime Act, s.50 (1-4)

prosecution of cybercriminals. Provisions should be made to provide for how information technology professionals can get involved at the investigative level as consultants to law enforcement agencies.

3. Section 24(3) of the Cybercrime Act which provides for the training of the law enforcement agencies should also be extended to cover judges in the training so as to aid the effective implementation of the Act.
4. Furthermore, Section 15 of the Cybercrime Act which provides for cyber stalking should be made to extend to email spam that is, sending large amount of unsolicited commercial emails.
5. It is recommended that before anybody enters into any kind of financial deals in Nigeria with anyone through the internet he/she should use any of the search engines to verify the identity of the unknown.
6. The government of Nigeria should set up National Computer Crime Resource Centre, which should comprise experts and professionals to establish rules, regulations and standards for network security protocols.
7. Establishment of an institutional agency in Nigeria that will be responsible for the monitoring of the information security situation, dissemination of advisories on latest information security alerts and management of information security risks including the reporting of information security breaches and incidents.[49]
8. Governments, the private sector and non-govern- mental organizations should work together to bridge the digital divide, to raise public awareness about the risks of cybercrime and introduce appropriate countermeasures and to enhance the capacity of criminal justice professionals, including law enforcement personnel, prosecutors and judges. For this purpose, national judicial administrations and institutions of legal learning should include comprehensive curricula on computer related crime in their teaching schedules.[50]
9. The Nigerian police should be educated on Internet policing capability. Nigerian law enforcement agencies are basically technology illiterate; they lack computer forensics training and often result to conducting police raids on Internet service site mainly for the purpose of extortion.[51]
10. Forensics commission should be established, which will be responsible for the training of forensics personnel.[52]
11. Improving awareness and competence in information security and sharing of best practices at the national level through the development of a culture of Cyber-security at national level.
12. Develop, foster and maintain a national culture of security standardize and coordinate cyber security awareness and education programme at all levels of education- primary, secondary and tertiary.[53]
13. Formalize the coordination and prioritization of cyber security research and development activities; disseminate vulnerability advisories and communications;

[49] Ibid
[50]Ibid
[51] Ehimen OR & Bola A., 'Cybercrime in Nigeria', *Business Intellectual Journal*. 2010 Vol.3(1):pp.26-37 p.31
[52] Ibid
[53] Ibid