PROSPECTS OF CYBERCRIME INVESTIGATION AND PROSECUTION IN NIGERIA AND THE ROLE OF SECURITY AND INTELLIGENCE AGENCIES IN CURBING CYBERCRIME*

Abstract
Cybercrime has emerged as a significant threat to Nigeria's national security, economy, and social fabric. The country's increasing reliance on digital technologies has created vulnerabilities that cybercriminals exploit, resulting in substantial financial losses and reputational damage. Effective investigation and prosecution of cybercrimes are crucial to mitigating these threats. However, Nigeria's law enforcement agencies face challenges in tackling cybercrime due to limited expertise, inadequate legislation, and poor inter-agency collaboration. This study examines the prospects of cybercrime investigation and prosecution in Nigeria, with a focus on the role of security and intelligent agencies in curbing cybercrime. The research employs a qualitative approach, combining case studies, and documentary analysis to identify the strengths and weaknesses of Nigeria's cybercrime investigative and prosecutorial framework. The findings highlight the need for enhanced capacity building, specialized training, and improved inter-agency cooperation among security and intelligent agencies. The study recommends the establishment of a dedicated cybercrime unit, the development of comprehensive cybercrime legislation, and the adoption of international best practices in cybercrime investigation and prosecution. This research contributes to the discourse on cybercrime and cybersecurity in Nigeria, providing insights for policymakers, law enforcement agencies, and stakeholders engaged in combating cybercrime. By identifying the prospects and challenges of cybercrime investigation and prosecution in Nigeria, this study aims to inform strategies that strengthen the country's cybersecurity posture and foster a safer digital environment.

Keywords: Cybercrime, Investigation and Prosecution, Security and Intelligence Agencies, Role, Nigeria

1. Introduction

The advent of the digital age has brought about unprecedented opportunities for economic growth, social connectivity, and access to information. However, this digital revolution has also created a new frontier for criminal activity, with cybercrime emerging as a significant threat to individuals, businesses, and governments worldwide. Nigeria, with its rapidly growing digital landscape, has become an attractive target for cybercriminals, resulting in substantial financial losses, reputational damage, and compromised national security. Cybercrime investigation and prosecution are critical components in the fight against cybercrime. Effective investigation and prosecution require specialized skills, advanced technologies, and robust legal frameworks. However, Nigeria's law enforcement agencies face significant challenges in tackling cybercrime, including limited expertise, inadequate legislation, and poor inter-agency collaboration. The role of security and intelligent agencies is crucial in curbing cybercrime. These agencies possess the expertise, resources, and mandate to investigate and prosecute cybercrimes. However, their effectiveness is hindered by various factors, including inadequate funding, lack of specialized training, and poor coordination among agencies.

This study seeks to explore the prospects of cybercrime investigation and prosecution in Nigeria, with a focus on the role of security and intelligent agencies in curbing cybercrime. The research aims to: examine the current state of cybercrime investigation and prosecution in Nigeria; identify the strengths and weaknesses of Nigeria's cybercrime investigative and prosecutorial framework; investigate the role of security and intelligent agencies in cybercrime investigation and prosecution; analyze the challenges faced by security and intelligent agencies in curbing cybercrime and propose recommendations for enhancing the effectiveness of cybercrime investigation and prosecution in Nigeria. By examining the prospects and challenges of cybercrime investigation and prosecution in Nigeria, this study aims to contribute to the development of a comprehensive strategy for combating cybercrime, ensuring a safer digital environment, and protecting Nigeria's national interests.

2. Legal and Institutional Framework for Cybercrime Investigation and Prosecution in Nigeria

The aim of this section is to discuss briefly the legal and institutional framework on cybercrime in Nigeria. The various statutes as well as the institutions regulating cybercrime in Nigeria would be discussed below.

Legal Framework for Cybercrime Investigation and Prosecution in Nigeria

Cybercrime Act 2015[1]**:** 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.

***By R. O. ISHIGUZO, PhD, BL,** Law Officer of the 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.

[1] Cybercrime (Prohibition, Prevention, ETC.) Act 2015.

Economic and Financial Crimes Commission (Establishment) Act[2]: 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. 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*[3].

***Advanced Fee Fraud and other Fraud Related Offences Act[4]*:** 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 therewith. Advance fee fraud is a vexing threat and a major problem in Nigeria today.[5] The Act provides for ways to combat cybercrime and other related online frauds.

***Money Laundering (Prohibition) Act[6]*:** 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.

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.[7]

Criminal Code[8]: 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.

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.

Communication Act 2003: The main objective of the Act was to create and provide a regulatory framework for the Nigerian Communications Industry and all matters related thereto. The Act provides a regulatory framework for the communications industry in Nigeria. This industry includes computer databases, telegraphs, television and radio broadcasting, publishing, advertising, motion pictures, telecommunications and other information industries.[9]

National Information Technology Development Agency Act: The National Information Technology Development Agency (NITDA) Act was established by the National Assembly in 2007 with the mandate to oversee the overall development of the ICT industry in Nigeria in order to ensure a steady growth of the sector and the agency has since its inception, embarked on several programs to expand the reach of IT across rural and under-served communities through inclusive development[10].

Institutional Framework for Cybercrime Investigation and Prosecution in Nigeria

Office of the President of the Federal Republic of Nigeria: The law[11] empowered the President of Nigeria upon receipt of a recommendation from the National Security Adviser, by designation of Order published in the Federal Gazette, designate certain computer systems or networks, whether physical or virtual the computer programs, computer data or networks as traffic data to this country that the incapacity or destruction of or interference with such systems and assets

[2] Economic and Financial Crimes Commission (Establishment) Act 2002, Cap E1 Laws of the Federation of Nigeria, 2010.
[3] Suit No: CA/245/05. Retrieved online from http://www.cenbank.gov.ng/419/cases.asap. Accessed on 20th July, 2024.
[4] Advanced Fee Fraud and other Fraud Related Offences Act 2006, CAP A6, Laws of the Federation of Nigeria, 2010.
[5] Chawki M, Nigeria Tackles Advance Fee Fraud, *Journal of Information, Law & Technology,* Vol. 1, 2009, *pp.* 1-20 at p. 4.
[6] Money Laundering (Prohibition) Act Cap M18, Laws of the Federation of Nigeria, 2010.
[7] A Awopeju, 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 July, 2024.
[8] Criminal Code Act CAP 38, Laws of the Federation of Nigeria, 2010.
[9]Communication Industry, Retrieved online from https://www.infoplease.com/encyclopedia/social-science/economic/business/communication-industry. Accessed on 25th July, 2024.
[10] P O Jack, National Information Technology Development Agency NITDA), *Nigeria Computer Society (NCS) International Conference*, July 2015. Retrieved online from http://www.ncs.org.ng/wp-content/uploads/2015/08/NITDA-presentation.pdf. Accessed on 25th July, 2024.
[11] Cybercrime (Prohibition, Prevention, ETC.) Act 2015, Section 3.

would have a debilitating impact on security, national or economic security national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.

Office of the National Security Adviser (NSA): The Office National Security Adviser is responsible for making recommendation to the President of Nigeria to designate certain computer systems or network, computer programs, computer data as traffic data vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure and to audit and inspect any critical national information infrastructure at any time on the directive of the President.[12]

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[13]. The Cybercrime Act[14], like the Nigerian Constitution[15], 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.

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 include 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

Nigerian Financial Intelligence Unit: The Nigerian Financial Unit (NFIU) is the Nigerian arm of the global Financial Intelligence Units (FIUs).[16] 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.[17] The EFCC Act of 2004 and the Money Laundering (Prohibition) Act 2011 (as amended in 2012) confer powers on the NFIU.

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.[18] The group was created to seek ways of tackling the menace of 419 fraud in Nigeria.[19]

Cybercrime Advisory Council**:** As part of efforts to combat cybercrime in Nigeria, the Act established Cybercrime Advisory Council which consists of a representative of different ministries and agencies listed under the first schedule to the Act. The functions and powers of the council includes: to advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues; among others.

Computer Professionals' Registration Council**:** The Cybercrime Act,[20]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 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.[21]

National Information Technology Development Agency (NITDA): Following the approval of the National Information Technology Policy in March 2001, the National Information Technology Development Agency (NITDA) was

[12] Ibid, Sections 3 & 4.
[13] Ibid, Section 41(2).
[14] Cybercrime Act, Section 47.
[15] Constitution of the Federal Republic of Nigeria, 1999 (As Amended), Cap 23, Laws of the Federation of Nigeria, 2004. Section 174.
[16] On information about the NIFU, See http://www.nifu.gov.ng/index.php/nifu. Accessed on 25th July, 2024.
[17] Ibid.
[18] A E Ezeoha, 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 July, 2024.
[19] Chawki, op. cit.
[20] Ibid, Sections 7(1)(a)
[21] Ibid, Section7(1) (b) (2-4)

established. The agency is the body responsible for facilitating ICT growth for development in Nigeria. The agency is the clearing house for Information Technology projects in the public sector.

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 sub-unit of the Nigerian Police Force called Special Fraud Unit (SFU)[22] is charge with the responsibility of apprehending and carrying out forensic investigation of cybercriminal activities in Nigeria.

3. The Role of Security and Intelligence Agencies in Curbing Cyber Crime

The specialized criminal groups to commit cybercrime develop their activities through computer viruses against individual users of internet and above all with sophisticated operations aiming to block the official addresses of private and public institutions such as banks, in order to unlawfully obtain the data or to infiltrate to classified information so to exchange them. Therefore, state institutions both national state agencies as well as international agencies specific role in combating crimes in general and cybercrime in specific are discussed below.

Nigeria Cybercrimes Working Group (NCWG): The Nigeria Cybercrimes Working Group (NCWG) is an inter-agency body comprising law enforcement intelligence, security as well as information and communications technology (ICT) agencies of government and key private sector ICT organizations[23]. It was established in 2004 by the Federal Executive Council (FEC) on the recommendation of the President. The group was created to deliberate on and propose ways of tackling the malaise of cybercrimes in Nigeria[24]. This includes; educating Nigerians on cybercrimes and cyber security; undertaking international awareness programs for the purpose of informing the world of Nigeria's policy on cybercrimes and to draw global attention to steps taken by the Nigerian government to rid the country of cybercrimes; providing legal and technical assistance to National Assembly on cybercrimes and cyber security in order to promote general understanding of the subject matter among the legislators[25].

National Information Technology Development Agency[26]: In 2001, the National Policy on Information Technology was put in place by the Nigerian government with the view to among others utilize information technology for sustainable national development, global competitiveness, education, wealth/job creation, poverty eradication, as well as guarantee that the country benefits maximally and contributes meaningfully by providing global solution to the challenges of the information age[27]. The policy also seeks to protect and promote the interest, assets and safety of Nigeria by developing knowledgeable manpower with commensurate discipline and IT skills-set capable of efficiently generating and effectively utilizing information in a timely manner for national decision making[28] Specifically, the National IT Policy's objectives with respect to national security and law enforcement are to safeguard life and property of all Nigerians both at home and abroad and NITDA's mission is to make Nigeria IT capable country as well as using IT as an engine for sustainable development[29]. It is also NITDA's mandate to ensure the safety of the Nigerian cyber space and a successful implementation of an electronic government program. In this regard, NITDA formulates the National Information Systems and Network Security Standards and Guidelines in January, 2013. Draft Guidelines on Data Protection in September, 2014. Guidelines on Nigeria Content Development in Information and Communication Technology (lCT) in December, 2013 and the Standard for Digital and Computer Forensics in Nigeria in March, 2014.

Nigerian Communications Commission (NCC): The Nigerian Communications Commission (NCC) was established under the Nigerian Communications Act. The NCC is the independent national regulatory authority for the telecommunication industries in Nigeria. The Commission is responsible for creating enabling environment for competition among operators in the industry as well as ensuring the provisions of qualitative and efficient telecommunications services throughout the country. In furtherance of its mandate, the Commission has put in place guidelines for the provisions of Internet Service Providers (ISP) and other internet protocol-based telecommunication services. The Guidelines require ISPs to ensure that users are informed of any statement of cybercrimes prevention or acceptable internet use published by the Commission or any other authority and that failure to comply with these acceptable use requirements may lead to criminal prosecutions. Internet Service Providers are further required to

[22] Retrieved online from www.specialfraudunit.org.ng. Accessed on 25th of July, 2024.
[23] Chawki M, Nigeria tackles Advance Fee Fraud*; in Journal of Information, Law and Technology* (JILT), May 28, 2009. Retrieved online from http://go.warwick.ac.uk/jilt/2009-/chawki on 9/7/2016, p.13
[24] Ibid.
[25] Ibid; Abubakar Is'haq, *An examination of the institutional Framework for Combating Cybercrimes in Nigerian*: Being a Seminar Paper Presented at the Faculty of Law, Ahmadu Bello University, Zaria, 2016.
[26] Established by the National Information Technology Development Agency (NITDA) Act 2007
[27]See Paragraphs 2, 3 and 4 of the National Information Technology Policy. Retrieved online from http://www.nitda.gov.ng/document/nigeriaitpolicy.pdf. Accessed on 28th September, 2023.
[28] See Ibid, Chapter 12, para 12.1.
[29] Ibid.

cooperate with enforcement and regulatory agencies investigating cybercrimes or other illegal activity and must provide any service related information requested by the Commission or any other legal authority. These include information regarding particular users and the content of their communications; while contacting the Commission in the event they became aware of any complaint or activity indicating internet use for the commission of an offence. March 15, 2009 was the deadline for all cyber cafe operators and Internet Service Providers in Nigeria to register with the NCC of face the wrath of the commission. The Commission gave the deadline in a notice titled 'Final Warning to Illegal Telecom Operators and Service Provides.' The notice stated that the decision was necessary in order to curb cybercrimes and bring security to Telecom sector[30].

Economic and Financial Crimes Commission (EFCC): The Economic and Financial Crimes Commission (EFCC) was established by the EFCC (Establishment) Act, 2004 and was charged with the responsibility for the enforcement of all economic and financial crimes laws[31]. The EFCC is vested with the powers to investigate, prevent and prosecute financial crimes such as the Advance Fee Fraud and corrupt practices among others. It was established in response to pressure from the Financial Action Task Force (FATF) which named Nigeria as one of the 23 non-cooperative countries in the international community's efforts to fight financial crimes. The Commission is also responsible for identifying, tracing, freezing, confiscating and seizing proceeds of economic crimes. EFCC also host the Nigerian Financial Intelligence Unit (NFIU) vested with the responsibility of collecting suspicious transaction reports from financial and designated non-financial institutions, analyzing and disseminating them to relevant government agencies and other financial intelligent units all over the world. The NFIU complements the EFCC's Directorate of Investigations but does not carry out its own investigations. It has access to records and data banks of all government and financial institutions and has entered into agreement on information sharing with several financial intelligence centres. The case of *Amadi v FRN*[32]is one of the cases where the apex court in Nigeria pronounced on internet or computer related crimes in Nigeria. In 2013, the EFCC recorded 177 convictions in different courts across the country[33].502 Of the 117 convictions recorded by the EFCC, 57 of which are in relation to offences of obtaining by false pretences and possession of documents containing false pretences under the Advance Fee Fraud Act 2006, which is the principal enactment now in place for combating cybercrimes in Nigeria. This represents 49 percent of the total convictions secured by the EFCC in the year 2013. In its bid to combat cybercrimes the EFCC is collaborating with foreign anti-crime enforcement agencies such as the London Metropolitan Police, US FBI, Royal Canadian Mounted Police, and the Anti- Fraud Squad of the Western Australian Police.

Nigeria Internet Group (NIG): Nigeria Internet Group (NIG) was founded in 1995 as non-profit, non-governmental organization principally saddled with the responsibility of promoting the internet in Nigeria. To achieve its mandate, the Group engages in a number of activities which include; policy advocacy, awareness creation and education through conferences, seminars, exhibitions, workshop and newsletter publication[34]. The advocacy activities of the Group let to the licensing of the first set of internet service providers in Nigeria. The Group has made positive and impactful contributions to virtually all government policies and legislation that are related to the internet and the ICT sector in general. Such policies and legislation include; the National IT Policy, the NITDA Act, the EFCC (Amendment) Act, the Cyber Security Bill, the National Policy on Telecoms and the Telecoms Act.

Nigeria Computer Society: The Nigeria Computer Society (NCS) is the umbrella organization of all information technology professionals, interest groups and stakeholders in Nigeria. Formed in 1978 as Computer Association of Nigeria (COAN) and transformed into NCS as a result of harmonization with other stakeholders and interest groups. The NCS is a national platform for the advancement of information technology science and practice in Nigeria[35]. Part of the NCS strategic objectives include the promotion of the education and training of computer and information scientist, computer engineers, information and communication systems professionals; encourage research in the advancement of computer and information science among others. It is not in doubt that the NCS has contributed to policy formulation with respect to cybercrimes in Nigeria, hence its membership of the Nigeria Cybercrimes Working Group (NCWG).

Internet Service Providers Association of Nigeria (ISPAN): The Internet Service Providers Association of Nigeria (lSPAN) is an independent body and voluntary association acting in the interest of internet service providers and generally dealing with matters related to the provision of internet service in Nigeria. ISPAN's mission is to provide a forum in which internet service providers can address issues of common interest and interface with industry stakeholders so that end users receive world class service and industry participants earned a fair return on their investments. Recently, ISPAN

[30] Nigerian Communications Commission, Final Warning to Illegal Telecom Operators and Service Providers in Nigeria, Press Release, February 17, 2009. Retrieved from https://ncc.gov.ng/

[31] Section 6 of the Economic and Financial Crimes Commission Act

[32] *Amadi v Federal Republic of Nigeria* [2013] 16 NWLR (Pt. 1384) 611 (SC)

[33] Economic and Financial Crimes Commission (EFCC). (2013). *Annual Report 2013*, p. 12. Abuja, Nigeria: EFCC.

[34] Nwachukwu, C. C. (2013). The Role of Nigeria Internet Group in the Development of Internet in Nigeria. *International Journal of Computer Science and Information Security,* 11(1), 1-6.

[35] Nigeria Computer Society, About Us, 2024. Retrieved from https://www.ncs.org.ng

urged cyber cafe operators to join the government in the fight against cybercrimes in Nigeria. In its efforts at combating cybercrimes, ISPAN has blocked many sites because they were used to facilitate internet scams otherwise known as 419. Perhaps, that was why many cyber cafe operators do not want to use the connection of the ISPs hence they own their private connections known as Very Small Aperture Terminal (VSAT) which makes tracking, apprehension and prosecution of offenders more challenging to enforcement institutions.

Department of State Security: The Department of State Security was established by the National Security Agencies Act[36]. Section I of the Act provides that, for the effective conducts of national security there shall be established the State Security Service, which shall be charged with the responsibility for the prevention and detection within Nigeria of any crime against the internal security of Nigeria; the protection and preservation of all non-military classified matters concerning the internal security of Nigeria; and such responsibilities affecting internal security within Nigeria as the National Assembly or the President may deem necessary[37]. In furtherance of its general duties of crime prevention and detection, the Directorate for Cyber Security was created as a permanent autonomous body within the office of the National Security Adviser (NSA) to take over all the assets and liabilities of the Nigerian Cybercrimes Working Group (NCWG), including all uncompleted projects. The main mandates of the Directorate for Cyber Security (A Directorate in the Department of State Security) are to develop and implement a National Cyber Security Policy for Nigeria; drafting and/or proposing all relevant laws required to be enacted by the National Assembly for the security of computer systems and networks in Nigeria pursuant to the National Strategies on Cyber Security; and establishing a National Computer Emergency Readiness and Response Mechanism with Early Warning System (EWS) and alerts for all cyber related emergency in the country. The mandate also includes establishing a National Computer Forensics Laboratory and coordinating the training and utilization of the facility by all law enforcements, security and intelligence agencies on cybercrimes and cyber security: developing effective framework and interfaces for inter-agency collaboration on cybercrimes and cyber security among others.527

Nigeria Intelligence Agency (NIA): The Nigeria Intelligence Agency (NIA) is a vital part of security section. Its primary role is the collection and analyzing of information for threats against the state and the population. The NIA is established as necessity of obtaining the information on time for intelligence, counter-intelligence, internal and external threats, international and national terrorism, organized crime, cybercrime, sabotage and all other issues related to intelligence and Nigeria security. Apart from its role to gather information, the NIA performs the counter-intelligence activities. This activity covers the encountering and obstruction of cyber espionage and foreign intelligence services that are against the interests of the state[38].

The agency is responsible of information protection and state information system, dealing with verification of security for all employees of the state institutions that have access to classified information. The essential role of NIA is to protect the state and its population. Preventing various crimes, including cybercrimes, terrorism and other threats against national security, the NIA contributes in the security and welfare of the society. It analyzes foreign and internal information, electronic communication through internet and gathers the information for un-information issues such as, propaganda, terrorism, sabotage, espionage etc. The NIA collects information from persons and members of the groups that threat national security with their incriminatory action including cybercrime.

Nigeria Police Special Fraud Unit: The Special Fraud Unit of the Nigeria Police is responsible for the investigation of high profile, local and international fraud cases particularly the advance fee fraud (419), cybercrimes and information technology frauds. The section is headed by a Commissioner of Police[39]. The Nigeria Police (NP) applies high standards of preserving the classified information. The data-center of NP is used for creating and functioning of entire service infrastructure such as servers, memory disks, network services etc. The sector receives considerable number of requests from other states involving various cybercrime cases such as: web-page attacks, unlawful profit though services provided by webpage companies, use of unauthorized credit cards (identity theft) etc. Apart from the mentioned activities of the police regarding the fight against cybercrime, an important role has the co-operation with the prosecution office, the court and internet providers with bank representatives, customs and other institutions, depending on their needs. The close cooperation between relevant institutions is a primary or leading condition that cybercrime be prevented and fought efficiently and effectively. In regard to the international co-operation, we can assess it as positive but with intent to further develop it.

[36] National Security Agencies Act Cap N74 Laws of the Federation of Nigeria 2010.
[37] Ibid, Section 1.
[38] Wikipedia, *National Intelligence Agency (Nigeria)*, 2024. Retrieved online from https://en.wikipedia.org/wiki/National_Intelligence_Agency_(Nigeria)#:~:text=The%20National%20Intelligence%20Agency%20(NIA,foreign%20intelligence%20and%20counterintelligence%20operations.
[39] Retrieved online from https://www.specialfraudunit.org.ng/en.

Computer Crime Prosecution Unit, Federal Ministry of Justice: As part of its commitment to combating cybercrimes, the Federal Government in Nigeria approved the establishment of the Computer Crime Prosecution Unit (CCPU) under the supervision of the Public Prosecution Department of the Federal Ministry of Justice[40]. The CCPU is to collaborate with agencies such as the EFCC, the Telecoms and banking sectors in its bids to combat cybercrimes in Nigeria. At best, the CCPU is still in its infancy but was established to help in combating cybercrimes in Nigeria.

The International Police (Interpol): The International Criminal Police Organization, otherwise known as the Interpol, is an organization that facilitates the collaboration between all the police forces around the world[41]. The Interpol supports and facilitates international collaboration among the police forces in combating worldwide crimes such as cybercrimes. Interpol's work on combating cybercrimes are designed to assist cooperation between the member countries via a list of contact officers reachable for cybercrimes investigation; enhance the exchange of information on cybercrimes between member countries; support member countries in the incidence of cybercrimes investigation attack; build up partnerships with other international and private organizations[42]. Interpol has also established collaborative work with the private sector in countering the spread of cybercrimes.

Financial Action Task Force (FATF): The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 by the ministers of its member jurisdictions. The objectives of FATF are to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system[43]. In collaboration with other international stakeholders, the FATF also works to identify national level vulnerabilities with the aims of protecting the international financial system from misuse. It is a well-known fact that terrorists have been using the internet to communicate, extort, intimidate, raise funds and coordinate operations. Hostile states have highly developed capabilities to wage cyber wars. They have capabilities to paralyze large parts of communication networks, cause financial meltdown and socio-economic and political unrest. In a bid to counter multi-national crimes, FATF introduced a number of changes to strengthen the measures to combat money laundering, terrorist financing and other offences in the financial sectors. These include the adoption of a stronger standard for money laundering offences, detailed customer due diligence requirements, extension of customer due diligence and record keeping requirements to designated non-financial businesses and professions such as Accountants, Lawyers, Service Providers and Casinos.

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:

Jurisdiction: Jurisdiction presents a significant challenge to the effective investigation of cybercrime in Nigeria, complicating efforts to combat the growing threat posed by cybercriminals. This issue arises due to the inherently transnational nature of cybercrime, where activities often span multiple countries, making it difficult to determine which jurisdiction has the authority to investigate, prosecute, or enforce laws. Cybercrimes, such as hacking, phishing, and financial fraud, frequently involve perpetrators, victims, or both across different countries. A cybercriminal operating from one country can target victims in Nigeria, using servers located in a third country. This global spread creates a complex web of legal jurisdictions, leading to confusion about which country's law enforcement has the authority to investigate and prosecute the crime. For Nigeria, this means that even when cybercrimes are detected, local authorities may face significant difficulties in gathering evidence or apprehending suspects if those suspects are located abroad.

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 cyber-criminals opportunity to operate freely without been checkmated for their illicit activities. Even with the promulgation of the Cybercrime Act, cybercrime is still on the rise in Nigeria due to loopholes in the Act that still makes it possible for cyber criminals to circumvent the laws.

Inadequate Resources: The success or failure of the Law Enforcement agencies in the performance of their Constitutional duties is dependent on the available resources at their disposal. The law enforcement agencies are often

[40] Ahuraka Yusuf Isah, Nigeria: Cybercrime - FG Approves Prosecution Unit, 18th August, 2010. Retrieved online from https://allafrica.com/stories/201008190229.html.
[41] Retrieved online fromhttps://www.interpol.int/en/Who-we-are/Member-countries/Africa/NIGERIA
[42] Ibid.
[43] Retrieved online from https://www.fatf-gafi.org/en/home.html

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: Most of the officers involved in the investigation of cybercrime are computer illiterates as they have not attended any further training apart from there training at the police college. They are not trained 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 these 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.

Enforcement Issues: Even where laws exist, enforcement is often weak. The Nigerian legal system faces challenges such as corruption, lack of expertise among law enforcement officials, and inadequate resources to effectively combat cybercrime.

Technological Challenges: The technological landscape in Nigeria presents both opportunities and challenges in the fight against cybercrime.

Lack of Infrastructure: Many parts of Nigeria lack the necessary digital infrastructure to support robust cybersecurity measures. This includes inadequate internet penetration, limited access to modern cybersecurity tools, and poor technological literacy among the population.

Rapid Technological Change: The fast pace of technological innovation means that new cyber threats are constantly emerging. Nigerian businesses and government agencies often struggle to keep up with these changes, leaving them vulnerable to attacks.

Limited Cybersecurity Expertise: Nigeria faces a shortage of cybersecurity professionals, which hampers the country's ability to defend against cyber threats. Training and retaining skilled cybersecurity personnel is a significant challenge, as many experts are lured abroad by better opportunities.

*Cultural and Socioeconomic Factors***:** Cultural and socioeconomic factors also play a role in the prevalence of cybercrime in Nigeria.

High Youth Unemployment: The high rate of unemployment among Nigerian youth is often cited as a contributing factor to cybercrime. With limited opportunities for legitimate employment, many young people turn to cybercrime as a means of making money.

Cultural Tolerance of Corruption: Corruption is deeply entrenched in various aspects of Nigerian society, including law enforcement and the judiciary. This cultural tolerance of corrupt practices can hinder efforts to combat cybercrime effectively.

Lack of Public Awareness: There is a general lack of awareness among the Nigerian population about cybercrime and cybersecurity practices. Many people are unaware of how to protect themselves online, making them easy targets for cybercriminals.

*High Cost of Investigation***:** Cost of investigation is another serious aspect that affecting the investigators from conducting a detail discreet investigation in criminal cases most especially in cybercrime cases that evidence required for effective prosecution often comes from different sources and jurisdictions.

5. Prospects of Cybercrime Investigation and Prosecution in Nigeria

Cybercrime investigation and prosecution are critical components in the fight against cybercrime in Nigeria. As the country's digital landscape continues to evolve, the need for effective investigation and prosecution of cybercrimes has become increasingly important. Despite the challenges faced by law enforcement agencies, there are prospects for improving cybercrime investigation and prosecution in Nigeria. Below are some of the prospects of cybercrime investigation and prosecution in Nigeria.

Law Enforcement in Combating Cyber Crime (Skills, Knowledge, Techniques for Effective Investigation): Law-enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures[44]. It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously, the hash value is stored in a database and the picture that was analyzed has not been modified[45]. Forensic software is able to search

[44] See: Giordano/Maciag, (2005) Cyber Forensics: *A Military Operations Perspective, International Journal* of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632BFF420389C0633B1B.pdf

[45] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, Vol. 119, p. 531.

automatically for child-pornography images by comparing the files on the hard disk of suspects with information about known images. For example, in late 2007, authorities found a number of pictures of the sexual abuse of children. In order to prevent identification of offender had digitally modified the part of the pictures showing his face before publishing the pictures over the Internet. Computer forensic experts were able to unpick the modifications and reconstruct the suspect's face[46]. Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child-pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.

Use of ICTs and the Need for New Investigative Instruments: Offenders use ICTs in various ways in the preparation and execution of their offences. Law enforcement agencies need adequate instruments to investigate potential criminal acts. Some instruments (such as data retention) could interfere with the rights of innocent Internet users. If the severity of the criminal offence is out of proportion with the intensity of interference, the use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries. The introduction of investigative instruments is always the result of a trade-off between the advantages for law-enforcement agencies and interference with the rights of innocent Internet users. It is essential to monitor ongoing criminal activities to evaluate whether threat levels change. Often, the introduction of new instruments has been justified on the basis of the 'fight against terrorism', but this is more of a far-reaching motivation, rather than a specific justification *per se*.

Establishment of Fraud Detection Departments in the Various Financial Institutions: In order to reduce the scourge of cybercrime in the country, it is pertinent that financial institutions in the country should establish fraud detection departments. The Evidence Act has become grossly inadequate to cover the present advancement in technology with the concomitant sophistication employed in the commission of economic and financial crimes as it relates to computer-generated evidence should be amended to incorporate medium on how to authenticate an internet public device to ease the admissibility of electronically generated evidence in our court system. There is a need to reconsider the prohibitive aspects of our laws. The inadequacy of our legislation turns out to be even more serious when we consider the lack of analogy between most cybercrimes and their conventional network. There is a need to develop a comprehensive internet legislation to regulate electronic financial transactions and prevent electronic crimes. As long as there is an absence of a centralized electronic databank containing specific information on each individual resident and visitor to Nigeria, exposure of criminal intentions before they are executed and the effective investigation of crimes committed would continue to pose a serious challenge to security agencies.

***Serious Legislative Reforms and Amendment of Legislations Combating Cybercrime*:** It is also pertinent that legislative reforms be carried out and amendment of legislation in combating cybercrime and full harmonization with international legislation in order for legislation on cybercrime in Nigeria to keep pace with e-crime, especially as it becomes more prevalent and sophisticated hence there is the need to develop a common platform to address cyber security since cybercrime crosses borders and cannot be fought by one country. There is need for the National Assembly to amend the cybercrime Act by inserting a provision prescribing punishment under section 7 that relates to operation of cybercafés to make effective and efficient, the law making body should also expedite action to pass necessary Bills, that could help in curbing internet related crimes including the Economic and Financial Crimes Commission Act (Amendment) Bill 2010, Electronic Transactions Bill, 2015 and Payment System Management Bill 2015 all these are yet to become law and it relates to Cybercrimes.

Need to Organize Media Debates, Workshops and Seminars with Organizations for Security and Civil Society: Lastly, it is further, recommended that in order to advance the knowledge for applicable laws, the protection of privacy right and intellectual property, with intent to sensitize the methods and measures to prevent and combat the cybercrimes, there is a need to organize media debates, workshops and seminars with organizations for security and civil society. Education is the most vital weapon for literacy, as such seminars and workshops should be organized from time to time with emphasis on cyber safety so that the individuals, law enforcement agencies and service providers, will learn to keep their personal and customer information safe cybercrime criminals. We therefore, recommends that curriculum which will include courses on cybercrime, cyber management and its prevention should be introduced to both tertiary and secondary schools to take care of the present social changes. The internet services providers should not just provide broadband connection to their subscribers especially the home users, but they should also monitor effectively what the subscribers are doing on the net, at what time and where. They should provide their customers, especially financial institutions and cyber cafes with well-guided security codes and packages in order to protect their information and software from hackers and publishers.

[46] See: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007. Retrieved online www.nytimes.com/ 2007/10/09/ world/europe/09briefs-pedophile.html?_r=1&oref=slogin. Accessed on 28th September, 2023.

6. Conclusion

In conclusion, this study has extensively explored the prospects of cybercrime investigation and prosecution in Nigeria, with a focus on the role of security and intelligent agencies in curbing cybercrime. The findings of this research have highlighted the challenges faced by Nigeria's law enforcement agencies in tackling cybercrime, including limited expertise, inadequate legislation, and poor inter-agency collaboration. The study has also emphasized the critical role of security and intelligent agencies in cybercrime investigation and prosecution. These agencies possess the expertise, resources, and mandate to effectively combat cybercrime. However, their effectiveness is hindered by various factors, including inadequate funding, lack of specialized training, and poor coordination among agencies. To enhance the effectiveness of cybercrime investigation and prosecution in Nigeria, this study recommends: capacity building and specialized training for law enforcement agencies; development of comprehensive cybercrime legislation; improved inter-agency collaboration and coordination; establishment of a dedicated cybercrime unit and adoption of international best practices in cybercrime investigation and prosecution. By implementing these recommendations, Nigeria can strengthen its cybersecurity posture, reduce the incidence of cybercrime, and protect its national interests. The study's findings and recommendations are intended to inform policy decisions, guide law enforcement agencies, and contribute to the development of a comprehensive strategy for combating cybercrime in Nigeria. Ultimately, this research aims to contribute to the creation of a safer digital environment, where individuals, businesses, and governments can operate with confidence and security. By working together, Nigeria can harness the benefits of the digital age while minimizing the risks associated with cybercrime.