LEGAL AND INSTITUTIONAL FRAMEWORK FOR COMBATING CYBERCRIMES IN NIGERIA

Daudu S O[*] and Idehen S O[**]

Abstract

This article examines the current legal and institutional regime for combating cybercrimes in Nigeria. It shall in adeptly examine the Cybercrime Act in combating cybercrimes in Nigeria and also examine the laws combating cybercrime in other jurisdictions such as the UK and USA. The discussion shall also cover the effectiveness of the legal framework aimed at combating cybercrimes in Nigeria, and the challenges affecting the fight against cybercrimes in Nigeria and some selected jurisdictions. As the use of digital technologies and internet connectivity has increased in Nigeria, the incidence of cybercrimes such as hacking, software piracy, and credit card fraud has also risen. In response, the Nigerian government enacted the Cybercrime Act in 2015 to prohibit, prevent, and punish cybercrimes through a comprehensive legal framework. The key law regulating cybercrime in Nigeria is the Cybercrime Act of 2015. This Act aims to create a robust legal regime to combat cybercrimes by defining offences and prescribing penalties. Other relevant laws include the Criminal Code Act, Money Laundering Act, and the Nigerian Communications Act. Countries such as the UK and USA have also enacted laws to tackle the borderless nature of cybercrimes. In 1996, the Council of Europe drafted an international treaty on computer crimes. The US enacted laws like the USA Patriot Act, 2003 to expand law enforcement powers online. However, effectively enforcing these laws in Nigeria is still challenging due to factors like transnational nature of crimes, lack of technical capacity, and inadequate public awareness. This negatively impacts the fight against cybercrimes in Nigeria.

Keywords: Cyber, Cybercrime, Combat, Nigeria, Crime, Internet.

Introduction

This article examines transnational cybercrimes as crimes occurring several jurisdictions. The advancement of technology has brought about increase in the severity, comprehensiveness and sophistication of incidents of cybercrimes such that cybercrimes can now be effortlessly transnational. In the face of this reality, most countries have responded to this challenge by enacting legislations to address cybercrimes. In Nigeria today, the activities of cybercriminals have become a threat to the society. With the advent of information age, legislatures have been

[*]Department of Public Law, University of Benin, Benin City, Nigeria. Email: omokhudu.daudu@uniben.edu, 07035762754.

[**]Department of Public Law, Benson Idahosa University, Benin City, Edo State. Email: sidehen@biu.edu.ng, 08147415035

struggling to redefine laws with a view to criminalised cybercrimes. As a result of this, the Cybercrimes Act, 2015 was enacted for the prohibition, prevention, detection, response, and prosecution of cybercrimes and for other related matters. Aside the new Cyber Act, there are laws that indirectly relate to the prosecution of cybercriminals in Nigeria. These laws include the Economics and Financial Crimes Commission (EFCC) Establishment Act, Advanced Fee Fraud and Other Related Offences Act, the Nigeria Criminal Code, the Penal Code, the Money Laundering Act, and the Nigeria Evidence Act. Attempt shall also be made to other jurisdictions in their legislative effort to combat cybercrimes.

Legal Frameworks Combating Cybercrime in Nigeria

In Nigeria today, the activities of cyber criminals have become a threat to the society.[75] With the arrival of information age, legislatures have been struggling to redefine laws that fit crimes committed by cybercriminals.[76]Initially, there were no specific laws in Nigeria for combating computer crimes.[77]This led to the creation of an ideal environment for criminals to freely operate without any law to combat their criminal activities.[78] It is a general principle of law that an uncodified crime is not punishable, as provided in Section 36 of the 1999 Constitution of the Federal Republic of Nigeria[79] which states thus: A person shall not be convicted of a criminal offence unless that offence is defined and the penalty thereof prescribed in a written law; and a written law refers to an Act of the National Assembly or a law of a State.[80]

The factors involved in the prosecution of a crime under the Nigerian law emanates from one major source. 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

[75]Oke, R. "Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology" Journal of Philosophy, Science and Law, (2012) Vol.2, No.1, 17-22
[76]Ani, L. "Cybercrime and National Security: The Role of the Penal and Procedural Law" Law and Security in Nigeria, (2015), Vol. 10, No.7, pp. 197-232
[77]Ehimen, R. and Bola, A. "Cybercrime in Nigeria", Business Intelligence Journal, (2010) Vol.3, No.1, 93-98
[78]Ibid.
[79]Section 36 (12) of the 1999 Constitution of the Federal Republic of Nigeria
[80]Ibid.

Criminal Code, The Penal Code, Money Laundering Prohibition Act and the Nigerian Evidence Act.

Economic and Financial Crimes Commission (Establishment) Act

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).[81]

Section 5 of the Act[82]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.[83]

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.***[84]The accused in the case was reputed to have carried out the third world biggest single scam with numerous others pending in count. In this case, the accused persons were charged to the High Court of Lagos State. A57-count charge was proffered against the accused persons including the scamming to the tune of US $181.6 million and they were all found guilty and sentenced accordingly. In addition to this sentence, their assets were forfeited to the Federal Government of Nigeria and the sums of money recovered and returned to their owners.

Sections 14-18 stipulate offences within the remit of the Act. This includes offences to financial malpractices, offences in relation to terrorism, offences relating to false information and offences in relation to economic and financial crimes.[85]

Section 46 of the Act defines 'economic crime' as the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either-individually or in a group or organised manner thereby violating existing legislation governing the economic activities of

[81]Section 1 of the Economic and Financial Crimes Commission (Establishment) Act, 2002
[82]Section 5, Ibid
[83]Ehimen, Cybercrime, note 3
[84]Suit No. CA/244/05 http://www.cenbank.gov.ng/419/cases.asap(Accessed 16th March, 2021)
[85]Section 14–18of the Economic and Financial Crimes Commission (Establishment) Act, 2002

government and its administration and includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse dumping of toxic wastes are prohibited.[86]

Advanced Fee Fraud and other Fraud Related Offences Act[87]

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.[88] 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.[89]

According to Section 7, a person who conducts or attempts to conduct a financial transaction which involves the proceeds of a specified unlawful activity with the intent to promote the carrying on of a specified unlawful activity with the intent to promote the carrying on of a specified unlawful activity; or where the transaction is designed to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of a specified unlawful activity is liable on conviction to a fine of N 1 million and in the case of a director, secretary or other officer of the financial institution or corporate body or any other person, to imprisonment for a term, not more years and not less than five years.[90]

[86]Section 46, Ibid
[87]Advanced Fee Fraud and Other Fraud Related Offences Act, 2006, CAP A6, LFN 2010
[88]Chawki, M. "Nigeria Tackles Advanced Fee Fraud" Journal of Information, Law and Technology, (2009) Vol.1, No.4, 1-20
[89]Section 2 of the Advanced Fee Fraud and other Related Offences, 2006
[90]Section 7, Ibid

However, while in previous laws the onus was on the government to carry out surveillance on unlawful activities of criminals, the new law by virtue of Section 13 vests this responsibility on industry players, including internet service providers (ISPs) and cybercafé operators, among others. While the EFCC is the sub-sector regulator, the Act by virtue of Section 12 prescribes that henceforth, any user of internet services shall no longer be accepted as anonymous. Through what has been described as due care measure, cybercafés operators and ISPs will henceforth monitor the use of their systems and keep a record of transactions of users.[91] These details include, but are not limited to, photographs of users, their home address, telephone, email address, etc.

Money Laundering (Prohibition) Act[92]

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.[93]Section 17 and Section 18 of the Act also implicates any person corporate or individual who aids or abet illicit disguise of criminal proceeds.[94] 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.[95] In the same way, be acting on his own account, the financial institution shall seek from him by all reasonable means information as to the true identity of the principal.

This enables authorities to monitor and detect suspicious cash transactions and these Sections can be used against criminals who use the internet as a means of unlawfully transferring large amount of money from one account to another.

[91]Section 12, Ibid
[92]Money Laundering (Prohibition) Act Cap M18, LFN 2010
[93]Section 14 of the Money Laundering (Prohibition) Act
[94]Section 17 and 18, Ibid
[95]Section 10, Ibid

Criminal Code[96]

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 239(2) (a) and 240A of the code prohibit betting and public lotteries respectively.[97] Section 239(2)(a) provides that any house, room or place which is used for the purpose of any money or other property, being paid or received therein by or on behalf of such owner, occupier, or keeper or person using the place as or for an assurance, undertaking, promise, or agreement, express or implied, to pay or give thereafter any money or other property on any event or contingency of or relating to any horse race or other fight, game, sport or exercise, of any house, room, or place knowingly and willfully permits it to be opened, kept or used or any person who has the use or management of such business of a common betting house is guilty and liable to imprisonment for one year, and to a fine of one thousand naira.[98] This Section can be used by law enforcement agencies to regulate 'Online Betting' contravene this Section. or prosecute such persons as would contravene this section.

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. In the case of ***Esso West Africa Inc. v. T. Oyegbola***[99]the court had a foresight when it stated that:

> The law cannot be and is not ignorant of the modern business methods and must not shut its to the mysteries of computer. In modern times reproduction and inscriptions documents by mechanical process are common place and Section 37 cannot therefore only apply to books of account.

[96]Criminal Code Act CAP 38, LFN 2010
[97]Section 239-240 of the Criminal Code Act
[98]Section 239(2), ibid.
[99](1969) NMLR 194 at pp.216-217

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.[100]

Section 84(1)-(5) introduces the 'admissibility of statements in documents produced by computers.[101] 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 which it was generated and the 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.[102]

Thus, in ***R v. Spiby***[103]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. Taylor L.J. in this case confirmed that 'this was not a printout which depended in its content for anything that had passed through the human mind' and so was admissible as real or direct evidence.[104] The court also noted here that unless there was evidence to the contrary the court would assume that the electronic device generating the evidence was in working order at the material time.

Lawyers can now rely on Section 84(5)(c) to prove that information via mobile phones and other gadgets/devices are admissible. This has made it more convenient and expedient for our courts to admit computer generated evidence.

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

[100]Section 258 of the Evidence Act
[101]Section 84, Ibid
[102]Chinedu, L. Regulation of Cybercrime In Nigeria (Owerri; Imo State University Press; 2014) 69
[103](1990) 91 Criminal Appeal Review 186
[104]Ibid.

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.

The objectives of the Act are to-

Provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

Ensure the protection of critical national information infrastructure; and Promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

Before the enactment of this Act, the legal and institutional framework regulating cybercrime in Nigeria was not unified. But through this Act, the legal, regulatory and institutional framework for the combating of cybercrime would be unified. The application of the provisions of the Act would also apply throughout the Federal Republic of Nigeria.[105]

The Act looks into the position of the nation with reference to information and communication where it provides for the designation of certain computer systems or networks as critical information infrastructure.[106]And it further provides that:

The president may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well being of its citizens, as constituting Critical National Information Infrastructure.[107]

The presidential order made under subsection (1) of this Section may prescribe minimum standards, guidelines rules or procedure in respect of the protection or preservation of critical information infrastructure; the general management of critical information infrastructure; access to, transfer and control of data in any critical information infrastructure, infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national informational infrastructure; the storage or achieving of data or information regarded critical national information infrastructure, recovery

[105]Section 2 of the Cybercrime Act, 2015
[106]Section 3 of the Cybercrime Act, 2015
[107]Ibid.

plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and any other matter required for the adequate protection, management and control of data and other resources in any critical information infrastructure.

Through this aforementioned provision of the Act, national security is secured and enhanced by the protection of critical information infrastructure.

Part III of the Act discuss 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 Act provides for offences against critical national infrastructure. And any person who commits any offence against any critical national information infrastructure, pursuant to Section 3 of the Act, is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine.[108] Where the offence committed under subsection (1) of this Section results in grievous bodily injury, the offender shall be liable on conviction to imprisonment for a minimum term of fifteen years without option of fine.[109] Where the offence committed under subsection (1) of this Section results in death, the offender shall be liable on conviction to death sentence without an option of fine.[110]

Critical national information infrastructure is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on national economic strength, national image, national defiance and security, government capability to functions and public health and safety. The critical national infrastructure is therefore a major asset for the nation, and Section 5 (1) would therefore help in promoting national security.

The Act further criminalizes unlawful access to a computer and the crime is punishable with a term of imprisonment of not less than two years or to a fine of not less than five million naira or to both fine and imprisonment.[111]The Act further provides that where the crime of unlawful access to a computer was committed with the intent of obtaining and securing access to any

[108]Section 5(1) of the Cybercrime Act
[109]Section 5(2) of the Cybercrime Act, 2015
[110]Section 5(3), Ibid
[111]Section 6(1) of the Cybercrime Act, 2015

computer data, program, commercial or industrial secrets or confidential information, the offender shall be liable to a term of imprisonment of not less than three years or to a fine of not less than seven million naira or such offender shall be liable to both fine and imprisonment.[112]

The Act discusses unlawful interception of communications, where it further provides that any person, who intentionally and without authorization or in excess of authority intercepts any data from a computer to or from a computer, computer system or connected system or network commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than five million naira or to both fine and imprisonment.[113]

This Section aims to secure the internet which is a collection of information, protect data and protect the privacy of individuals in relation to the information they transfer through the net.

The Act also establish numerous other crimes, including unauthorized modification of a computer program or data,[114] system interference,[115] misuse of devices,[116] computer-related fraud,[117]identity theft or impersonation,[118]cyberstalking,[119] and cybersquatting.[120]

Section 17 of the Act also criminalizes cyber-terrorism and provides that any person who accesses or causes to be accessed any computer system for the purpose of committing a terrorist act as defined under Terrorism (Prevention) Act 2011 as amended commits a cyberterrorism offence and he is thus liable to life imprisonment upon conviction.

The Act also criminalizes child pornography and creates two classes of offenses under this category. The first involves the use of a computer network for the purpose of, among other activities, the possession, production, and/or distribution of materials depicting a minor, a person appearing to be a minor, or images representing a minor engaged in sexually explicit conduct.[121]

The second involves the use of 'information and communication technologies' to engage in such acts as luring and meeting (here the crime requires two elements to exist: communicating with a child online followed by an in person meeting) with s child for the purpose of engaging in sexual

[112]Section 6(2), Ibid
[113]Section 7, Ibid
[114]Section 8, Ibid
[115]Section 9, Ibid
[116]Section 10, Ibid
[117]Section 12, Ibid
[118]Section 13, Ibid
[119]Section 15, Ibid
[120]Section 16, Ibid
[121]Section 14, Ibid

activities or recruiting a child to participate in a pornographic performance.[122] The penalties for the offences would range from a five to ten year prison term or fines ranging from ten to twenty million naira, or both, depending on the particular offense.[123]

Institutions Regulating Cybercrime in Nigeria

There are certain bodies in Nigeria set up by the Nigerian government mainly involve the setting- up of special bodies by the Nigerian government to deal with cybercrime.[124]And they include the Economic and Financial Commission (EFCC) and the Nigerian Cybercrime Working Group.

Economic and Financial Crimes Commission (EFCC)

The EFCC is a Nigerian law enforcement agency that investigates financial crimes such as advance fee fraud and money laundering. The commission is empowered to investigate, prevent and prosecute offenders who engage in *'money laundering, embezzlement, bribery, looting and any form of corrupt practices, illegal arms deal, smuggling, human trafficking, and child labour, illegal oil bunkering, illegal mining, tax evasion, foreign exchange malpractices include counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes, and prohibited goods'*.[125]

The commission is also responsible for identifying, tracing, freezing, confiscating, or seizing proceeds derived from terrorist activities. For example, in 2005, the EFCC confiscated at least hundred million dollars from spammers and other defendants.[126]

Nigerian Financial Intelligence Unit (NIFU)

This is an operative unit in the office of EFCC and was established under EFCC Act 2004 and Money Laundering (Prohibition) Act of 2004, as amended.[127] The unit is a significant component of the EFCC.[128]It complements the EFCC's directorate of investigations but does not carry out its

[122]Ibid.
[123]Ibid.
[124]Chawki, supra note 14
[125]Ibid, p.12
[126]Olukanmi, A. "Expert Group Meeting on Cybercrime", Journal of Law and Policy, Vol.2, pp. 17-21
[127]Saulawa, M., Marshal, J. "Cyberterrorism: A Comparative Legal Perspective", Journal of Law, Policy and Globalization, (2015), Vol.3, No. 1, pp. 11-22
[128]Chawki, Nigeria Tackles Advanced Fee Fraud, note 14

own investigation.[129] The unit's coordinating objective is receipt and analysis of financial disclosure of Currency Transaction Report and Suspicion Transaction. All financial institutions and designated non-financial institutions are required by law to furnish the NFIU with details of their financial transactions.[130] The NFIU has access to records and databanks of all government and financial institutions, and it has entered into memorandums of understandings (MOUs) on information sharing with several other financial intelligence centres.[131]

Nigerian Cybercrime Working Group

The Nigerian Federal government in 2004 set up the Nigeria Cybercrime Working (NCWG) to realize the objectives of National Cybersecurity Initiative (NCI).[132] The objectives of the NCI include public enlightenment of the Nigerian populace on the nature and danger of cybercrime, criminalization through new legislation of all on-line vices, establishment of legal and technical framework to secure computer systems and Networks, and protection of critical information infrastructure for the country.[133] The group was created to deliberate on and propose ways of tackling the malaise of internet fraud in Nigeria.

Legal Framework on Cybercrimes in other Jurisdictions

Canada

Canada was one of the first countries to enact criminal laws in the area of computer crime.[134]According to a study by a United Nations-sponsored network of internet policy officials, Canada is ahead of nearly two-thirds of the 52 countries surveyed in enacting laws to crack down on cybercrimes.[135]

[129]Ibid.
[130]Ibid.
[131]Ibid.
[132]Maska, M. "Building National Cybersecurity Capacity in Nigeria: The Journey so Far" (2009) Regional Cybersecurity Forum for Africa and Arab States, Tunis, available at http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity(Accessed 28th May, 2021)
[133]Ibid.
[134]Kowalski, M. "Cybercrime Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics", Canadian Centre for Justice Statistics, http://www.publications.gc.ca/collection/statcan/85-558-x85-558(Accessed 3rd June, 2021)
[135]Ibid.

Canada is a signatory to the Convention on Cybercrime. It requires that each state party prosecute cybercrimes committed within its territory.[136] This translates that a country could claim territorial jurisdiction in a case where the computer system attacked is on its territory, even if the perpetrator of the attack is not.

In Canada, if a crime falls under Section 430 or 342.1 of the Canadian Criminal Code that is where a computer or data is object of the crime. The code makes provision for mischief in relation to computer data. It provides for computer sabotage which include destruction of hardware, erasure or alteration of data, logic bombs. The Section provides that everyone commits computer data or mischief who willfully destroys or alters computer data; renders computer data meaningless, useless or ineffective; obstructs, interrupts or interferes with the lawful use of obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it is liable to imprisonment for life if the mischief committed caused actual danger to life or to a term of ten years or two years depending on the degree of crime committed.[137]

Thus, under Section 430(1.1), an offence occurs when viruses are used to cause mischief to data. Under the code, there is no law expressly prohibiting the creation or dissemination of computer viruses. Although under Section 430(5.1) of the criminal code, distribution of virus might constitute an offence even if the virus has yet to be activated. The Section provides for that an act or omission is an offence if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or computer data.[138]

The Criminal Code also provides for computer fraud and other economic crimes. These include misuse of credit or bank cards, breach of trust or abuse of confidence, forgery and related offences.[139] Canadian courts have held that anything that can be considered property can be the object of theft or fraud. In the case of ***Regina v. Stewart,***[140] the Ontario Court of Appeal held that copying a confidential list of hotel union employees from a computer printout constituted theft of property. In the most recent Canadian case involving computer-related crime, *Turner and the Queen*,[141] the Ontario High Court reconciled the absence of Parliamentary action with judicial

[136]Article 22 of the Budapest Convention on Cybercrime,,(year)
[137]Ibid.
[138]Section 430 of the Criminal Code of Canada
[139]Ibid.
[140]42 Ontario 2d 225 (1983)
[141]13 Criminal Code of Canada 3d 430 (1984)

expansion of the definition of property.[142] In Turner, the defendants had accessed computer tapes and tampered with the program stored on the tapes so that other users were unable to use the program without first obtaining the new program code. The court found that the defendants, by their actions, had interfered with the retrieval of data off the tape, making it impossible for other users to process their work. If the Turner case is followed, Canadian courts will treat alteration or destruction of computer data specifically as an interference with property.[143]

Combating cybercrime in Canada comes under the jurisdiction of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) a division of Public Safety Canada.[144] Under the OCIPEP umbrella is the Cyber Security division responsible for the Canadian Cyber Incident Response Centre (CCIRC), Canadian Cyber Incident Response Centre Partners, Cyber Security Technical Advice and Guidance, and Cyber Security in the Canadian Federal Government. OCIPEP facilitates communication and networking amongst Canadian organizations and businesses, provides updates and advisory tools, provides training and workshops, and acts in conjunction with similar departments of foreign government.

United States

The United States (US) has certain federal laws that relate to computer crimes.[145] In the early 1980s, law enforcement agencies in the US faced the dawn of the computer age with developing issues about the lack of criminal laws available to fight emerging computer crimes.[146] Although there existed in the federal criminal code, provisions relating to the wire and mail fraud, they were incapable of combating the new computer crimes.[147] This led to the enactment of laws to deal with computer crimes. In doing so, Congress opted not to add new provisions regarding computers to existing criminal laws, but address federal computer-related offences in a single, new statute.[148]

[142]Ibid. at p.434
[143]Menelly, L. "Prosecuting Computer-Related Crime in the US, Canada and England", Boston College International and Comparative Law Review, http://www.lawdigitalcommons.bc.edu/iclr/vol8/iss2/9(Accessed 26th May, 2021)
[144]Duke, S. "Cybercrime in Canada: Strategies, Reforms and Amendments in the Canadian Judicial Law Enforcement Systems" http://www.academia.ed/documents/3397373508/cybercrime-strategies(Accessed 3rd June, 2021)
[145]Jarie, M. and Balie, M. "Prosecuting Computer Crimes" http://www.justice.gov/sites/default/files/criminal-cips/egacy(Accessed 20th June, 2021)
[146]Ibid.
[147]Ibid.
[148]Ibid.

In some situations, the Act allows victims who suffer specific types of loss or damage as a result of violations of the Act to bring civil actions against the violators for compensatory damages and injunctive or other equitable reliefs.[149] The situations in which a victim could bring an civil action for any equitable relief include physical injury to any person; a threat to public health or safety; damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defence, or national security; loss to one or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the US only, loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000 in value; the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; and damage affecting one or more protected computers during any one- year period.[150] As long as a victim is able to prove that he has suffered any type of loss or damage aforementioned, such will suffice for a victim to bring a civil action against the violator.

Another US federal law used for combating computer crimes is the Wiretap Act[151]. The federal Wiretap Act, as amended in 1986 by the Electronic Communications Privacy Act, protects the privacy of wire, oral, and 'electronic communications', a broad term that includes computer network communications.[152] It is both procedural and substantive.[153] It prohibits not just law enforcement, but 'any person' from making an illegal interception or disclosing or using illegally intercepted material.[154]

The prohibition crux of the Wiretap Act is found in Section 2511(1)(a), which prohibits 'any person' from intentionally intercepting, or attempting to intercept, any wire, oral or electronic communication. From the aforementioned Section, it must be shown that the interception of the communication be intentional.

While the Wiretap Act has provided for wide prohibitions in Section 2511(1), it has also provided for many exceptions in subsection 2511(2). The exceptions that are particularly relevant in the context of network crimes would be briefly discussed here. One exception is where the

[149]Subsection 1030(g) of the CFAA
[150]Subsection 1030(c) of the CFAA
[151]Section 2510 – 2522 of the Federal Wiretap Act, 18 USC
[152]Title 18 of the United States Code SS 2510-2522, The Wiretap Act
[153]Jarie, supra note 96
[154]Section 2511(1) of the Wiretap Act

consent of a party has been given.[155] Thus an interception is lawful if the interceptor is a party to the communication or if one of the parties to the communication consents to the interception.

England

In England, criminal law generally applies to illegal acts regardless of the medium used to commit the act. An exception however, is the Computer Misuse Act (CMA) 1990 (and now amended by the Police and Justice Act 2006) which its main focus is on computers. The CMA is the only legislation that explicitly and mainly focuses on computer crime. The Act creates three main offences: (i) unauthorized access to computer material,[156] (ii) unauthorized access to a computer system with intent to commit or facilitate further offences,[157] and (iii) unauthorized modification of computer material.[158] Maximum sentences for these offences range from six months imprisonment and/or a 500 Euros fine to ten years imprisonment and/or an unlimited fine. The current Police and Justice Act[159] contains amendment to the CMA under the Section called Miscellaneous Part 5 Computer Misuse amendments'. For example, Clause 39 doubles the maximum jail sentence for hacking into computer systems from five years to ten years.

Also, the Obscene Publications Act 1964 makes it illegal to publish material that tends to deprave and corrupt those viewing it. The law's approach to child pornography is that it is so offensive that possession as well as circulation of offending images is criminalized. The primary legislation consists of the Protection of Children Act 1978 and the Criminal Justice Act 1988. It is an offence to possess indecent images involving children.

Incitement to racial and religious hatred is also governed by Section 21 of the Public Order Act 1986 which states that it is an offence for a person to publish or distribute material which is threatening or abusive or insulting if it is intended thereby to stir up racial hatred, or having regard to all the circumstances, racial hatred is likely to be stirred thereby. The Racial and Religious Hatred Act 2006 gained Royal Assent on 16 February 2006.[160] The Act makes it illegal

[155]Section 2511(2) of the Wiretap Act
[156]Section 1 of the CMA
[157]Section 2, Ibid
[158]Section 3, Ibid
[159](Commencement No.9) Order 2008
[160]John, J. "Computer Misuse Overview"http://www.jisclegal.ac.uk/legalareas/computermisuse(Accessed 23rdJune, 2021)

to threaten people because of their religion, or to stir up hatred against a person because of their faith.[161]

LOOPHOLES OF THE CYBERCRIME ACT, 2015

The Nigeria Cybercrimes Act 2015, made to contain the growing spate of Internet offences by seeking to arrest, prosecute and sentence anyone found guilty of committing cybercrime and allied offences, lacks what it takes to adequately combat the menace. Though the new law was expected to make the Internet a safer place, this may not be unless the loopholes in the Act are blocked.

The Cybercrimes Act, though long in coming and beset with certain challenging components, may be applied to effectively tackle Nigeria's cybercrime and cyber security challenges. But deliberate efforts have to be made by the key players; Office of National Security Adviser and the Office of Accountant General of the Federation working with stakeholders to make this a reality."

The definitions provided in the Act are "too specific" and may give room for offenders to devise other means of committing crimes outside the specific definitions of the law. There is a danger of confusion when we use specific definitions. For example, if we say someone commits a crime with an ATM machine and in the future we have another machine that is not called ATM to commit fraudulent act, that means, by definition, the person has not committed any offence or done anything wrong." There is nothing that defines what those funds are used for. There is need for the government to fully articulate all these issues and collaborate with the citizens to have a proper framework as to the workings of the Act.

The law is no doubt a welcome development but more needs to be put in place if we most win the war against cyber-attacks in Nigeria but with the new Cybercrime Act in place, which spells out various degrees of punishment for cybercrime offenders, Nigerians will be fully-protected and be able to freely transact online businesses without further fear or intimidation, since there is a law in place.

The issue of the expertise of the Local Enforcement Agents in prosecuting cybercrime and related cases is also suspect and I foresee that according to Section 7 of the Act, the Federal High

[161]Ibid.

Courts will be overburdened as they have been made the exclusive court to handle issues arising from cybercrime offences."

Comparative Analysis of the Nigerian Legal Framework on Cybercrime with some Selected Jurisdictions

Under this section, this study would use the Nigerian Cybercrime Act 2015 as the basis for its comparison. This is because the Cybercrime Act covers virtually everything provided for by other Nigerian statutes dealing with cybercrime. Though the Cybercrime Act adequately provides for the prevention and prosecution of cybercrimes in Nigeria, there are however certain shortcomings.[162]

Unlike the Canadian Law on Cybercrime, the Nigerian Cybercrime Act does not specifically provide for email spam. Section 15 of the Act only provides for the crime of sending messages that are grossly offensive, indecent, obscene, false for the purpose of causing annoyance or with intent to harm any person, property, reputation or with intent to extort. Section 42, which is the interpretation Section, defines cyberstalking to include: '(i) the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass; (ii) sending multiple e-mails, often on a systematic basis, to annoy, embarrass, intimidate, or threaten a person or to make the person fearful that she or a member of her family or household will be harmed.'[163]This does not extend to email spam. Email spam involves sending large amount of unsolicited commercial email, which could occur even in the absence of any intent to annoy, threaten or annoy the receiver. In our current age, spam could even contain various malware threats that the sender of the mail might not even know about. Therefore, it is suffice to say that the Cybercrime Act is not comprehensive enough, compared to the Canadian Cybercrime Law, in relation to cyberstalking as opposed to the American legal regime that specifically provides for email spam by virtue of its CAN SPAM Act under Section 1037.

The Cybercrime Act also provides for sanction that ranges from one to five years, depending on aggravating factors and prior convictions. Also, the Cybercrime Act as opposed to the American

[162]Ani, L. Law and Security in Nigeria (Lagos: Legal Studies Press; 2016) pp. 15-27
[163]Ladan, M.T. Cyber Law and Policy in ICT in Nigeria (Zaria: ABU Press; 2015) p.14

Computer Fraud and Abuse Act (CFAA), in the United States, as it does not allow victims who suffer specific types of loss or damage as a result of violations of the Act to bring civil actions against the violators for compensatory damages and injunctive or other equitable reliefs. Section 31 of the Cybercrime Act only provides for the forfeiture of the assets to the Federal Government of Nigeria. Under the CFAA, by virtue of Subsection 1030(g), a victim could bring a civil action for any equitable relief in certain situations. The Cybercrime Act thus neglects the interests of victims that are affected by the acts of cybercriminals and does not provide them with adequate protection.

Furthermore, although Section 24(3) of the Cybercrime Act provides that law enforcement, security and intelligence agencies should undergo training programmes, the fact that the judges are not included among the people required to undergo training programmes would likely affect the effective implementation of the Act. For instance, Section 27(3)(d) of the Cybercrime Act provides that a court may not issue a warrant under subsection 2 of the Section unless the court is satisfied that there are reasonable grounds for believing that the person named in the warrant is preparing to commit an offence under this Act. If the judge in question is not well vast in matters of computer crimes and cyber security, the judge might not know exactly what constitute enough 'reasonable ground' to believe that a person named in the warrant is preparing to commit an offence under this Act. Thus, without adequate knowledge on the part of the judges about computer crimes and cyber security, the Act would not be effectively implemented.

More so, although Sections 8 and 9 of the Cybercrime Act prevent the modification of computer data and computer system through malicious codes such as viruses, they do not prevent the creation and distribution of computer viruses among people.

In view of these gaps identified in the legal framework, there is a need to properly amend the Cybercrime Act so as to cover these lapses, by "borrowing a leaf" from the above stated countries. This would go a long way in enhancing the legal framework on cybercrime by way of enhancing the legal mechanisms available for the effective eradication of cybercrime in Nigeria.

Challenges Faced in the Combating Cybercrime in Nigeria

Despite the legal framework of the Cybercrime Act in Nigeria, the menace has still prevailed in many parts of the country. The following challenges militate against effective fight against cybercrime in Nigeria:

i. Technical Challenges

When a hacker disrupts air traffic control at a local airport, when a child pornographer sends computer files over the Internet, when a cyberstalker sends a threatening e-mail to a school or a local church, or when credit card numbers are stolen from a company engaged in e- commerce, investigators must locate the source of the communication. Everything on the Internet is communications, from an e-mail to an electronic heist. Finding an electronic criminal means that law enforcement must determine who is responsible for sending an electronic threat or initiating an electronic robbery.[164] To accomplish this, law enforcement must in nearly every case trace the "electronic trail" leading from the victim back to the perpetrator. Tracing a criminal in the electronic age, however, can be difficult, especially if we require international cooperation, if the perpetrator attempts to hide his identity, or if technology otherwise hinders investigation.[165]

As networked communications and e-commerce expand around the globe, businesses and consumers become more and more vulnerable to the reach of criminals. The global nature of the Internet enables criminals to hide their identity, commit crimes remotely from anywhere in the world, and to communicate with their confederates internationally. This can happen in nearly any type of crime, from violent crime, terrorism, and drug-trafficking, to the distribution of child pornography and stolen intellectual property, and attacks on e-commerce merchants.[166]

Criminals can choose to weave their communications through service providers in a number of different countries to hide their tracks. As a result, even crimes that seem local in nature might require international assistance and cooperation. For example, a computer hacker in Oslo might attack the computers of a corporation located only a few miles away. Yet, it is very possible that the enforcement agents might have to go to U.S., French, or Danish law enforcement officials for help in finding this criminal. This would happen if the hacker routes his communications through providers in New York, Paris, and Copenhagen before accessing his victim's computer.

Naturally, criminals like these, who weave communications through multiple countries, present added complexities to governments trying to find criminals. Mutual legal assistance regimes between governments anticipate sharing evidence between only two countries, that is, the

[164]Ibid.
[165]Kristine, M.F. "Cybercrime: Conceptual Issues in Nigerian Law Enforcement" <http://www.fas.org/sgp/r425.pdf>(Accessed 21st June, 2021)
[166]Ibid.

victim's country and the offender's country. But when a criminal sends his communications through a third, or fourth, or fifth country, the processes for international assistance involve successive periods of time before law enforcement can reach data in those latter countries, increasing the chances the data will be unavailable or lost, and the criminal will remain free to attack again.

While the Internet may be borderless, national boundaries exist for law enforcement and we must respect the sovereignty of each other's countries. We increasingly are dependent on mutual cooperation from other countries in investigating and prosecuting computer crimes. Simply stated, cybercriminals know no national boundaries, and the multi-jurisdictional nature of cybercrimes requires a new multilateral approach to investigations and prosecutions.

To succeed in identifying and tracing global communications, there is need to work across borders, not only with our counterparts throughout the world, but also with industry, to preserve critical evidence such as log files, e-mail records, and other files, and must be able to do so quickly, before such information is altered or deleted.[167]

ii. Operational Challenges

In addition to technical and legal challenges, law enforcement agencies in Nigeria and around the world face significant operational challenges. The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications. The complexity of these technologies, and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions.[168]

It is wise to suggest that every country should have dedicated high-tech crime units that can and will respond to a fast-breaking investigation and assist other law enforcement authorities faced with computer crimes.

To effectively combat cybercrime, there is a need for proper training of investigators and prosecutors on how to investigate acts or omissions which constitute cybercrimes. This affects how they prosecute crimes in law courts.

[167]Ibid.

[168]Benedict, B., "Consensus on Cybercrime" <https://www.pressreader.com/nigeria/thisday/20150826/281900181961981> Accessed 4th April, 2021

The emergence of new technologies is compounding the efficacy of the legal and institutional efforts geared towards combating cybercrimes in Nigeria. This is more so because of the borderless and transnational nature of cybercrimes generally. Cybercrimes, such as cyber terrorism, fraud-identity theft, drug trafficking deals, cyber stalking, spam, wiretapping, logic bombing, password sniffing, privacy and child pyrography still raised their ugly heads despite the concerted legal efforts aimed at nipping the menace on the board. The growing trend of cyber crime is allegedly attributable to weak enforcement of the legal and institutional instruments put in place to fight the upsurge. The article concludes that the institutionalisation of a task force to monitor and enforce compliance to the relevant legal and institutional frameworks will be the antidotes needed to nip cyber criminalities to the kneels