CYBERCRIME AND YOUTH UNEMPLOYMENT IN NIGERIA: THE DRIFT TOWARDS AN INTERNATIONAL ECONOMIC LAW

Nwosu, Uchechukwu Wilson, PhD*
Alinnor Ezinne Madonna, PhD**

Abstract
Cybercrime has been the bane of the financial sector and indeed every other facet of human existence from commerce to leisure. This research paper evaluates the nature and advent of cybercrime as well as its scope and recent trends. Using the doctrinal legal research method, the authors evaluate the recent foray of a significant population of Nigerian youth into this mode of crime. It was revealed that the paucity of employment opportunities for the teeming youth population, lack of effective legislation, hurdles regarding jurisdiction, extradition procedures, and conflict of law situations arising from diversities in legal systems have altogether been the driving force that attracts these impressionable generation of young people into embracing this online criminal activity. It was equally observed that given the trans-boundary nature of this crime, especially the fact that it is usually committed online within the cyberspace with the victims and perpetrators being in different locations, domestic legal frameworks are ineffectual for cybercrime regulation. It was further revealed that the weak laws and institutional frameworks in some developing countries such as Nigeria makes these destinations safe havens for these cybercriminals who take advantage of such lapses to strike their victims from remote locations undetected. It was concluded that in the face of the obvious shortcomings and manifest ineffectiveness of the domestic legal and institutional frameworks of most countries, an International Economic Law regime remains the only practical way to go using proactive methods particularly mutual legal assistance and cooperation among both the judicial and law enforcement authorities of countries across the globe. It was recommended inter alia that priority should be given to the ratification and domestication of international Conventions and Treaties regarding cybercrime, while state parties are encouraged to align their domestic legislations with these international legal instruments for greater effectiveness.

Keywords: Cybercrime, International Conventions, International Economic Law, Mutual Legal Assistance, Safe Havens, Unemployment.

Introduction
The concept of cybercrime has a peculiar history. Historical antecedent shows that unauthorized access, damage to property, theft, and distribution of obscene and indecent materials online are all considered as familiar cybercrimes.[1] The Nigerian cybercrime history started as a variant of the "advance fee fraud" tailored in line with the Spanish Prisoner S cam[2] which historically dates back to the late nineteenth century during which businesses were contacted by individuals pretending to be trying to smuggle an inmate belonging to a wealthy family out of prison in Spain. In exchange for this, the scammer promised to share a

*Faculty of Law, University of Calabar, Calabar – Nigeria. uchey2000@yahoo.com; uchey2014@gmail.com - +2348037050009
**Email*: ezinnealinnor@gmail.com* +2348036773203.

1 Nwosu, U. W., "Cybercrime and Nigeria's Receding Economy: The Role of the Legal System", *Institute of Public Policy & Administration [IPPA], Unical Book Series*, Lagos, Advanced Publishers Limited, 2018, 133-155.

2 Wikipedia, "Spanish Prisoner", https://en.wikipedia.org accessed, 22nd August, 2024.

huge amount of money with the victim who was however required to invest a small amount of money to bribe prison guards which usually turned out to be his initial exposure or loss.[3] The proliferation of the e-payment system following the Federal Government's adoption of the cashless policy actually led to massive increase in mobile and online transactions in recent times and by extension a resultant increase in financially related cybercrimes. Cyber-criminals have continued to develop new strategies to circumvent cyber-security models, regardless of their sophistication. Cyber-attacks or breaches of information security is increasing in frequency, and future attacks could have much more severe consequences than what has been observed till date. It has thus become perhaps the most critical issue on the global development agenda for all governments[4] since globalization has apparently given rise to activities and transactions increasingly conducted via Information and Communications Technology[5] and internet.

According to Ibikunle[6], Cyber-security has grown to become a global issue to be taken more seriously. In view of this, Nigeria's National Assembly in 2015 passed a Bill to provide a comprehensive legal framework for the evaluation and implementation of punitive response and preventive measures in the fight against Cybercrime and other related frauds in line with international best practices. The Cybercrime Act, 2015 was passed to combat Cybercrimes and redeem Nigeria's global image which had been battered by the high incidence of such crimes by providing a legal framework for the prohibition and punishment of online and electronic fraud, promoting e-government services, electronic communications, and transactions between public and private entities, institutions and individuals.

Most cybercrimes entail an attack on the personal information of individuals, corporate organizations, or government establishments. Although these attacks may not target a physical body, they often impact on the virtual essence of these persons or corporate entities, thus compromising the basic informational attributes which define these entities on the cyberspace[7] such as their National Identification Number[8], Bank Verification Number[9], the Integrated Payroll and Personnel Information System[10], *et cetera*, which are all computer codes bearing their vital personal data. In this digital age, these virtual identity codes have become essential characteristics of daily life. We are thus a collection of mathematical figures and identification codes in various computer databases belonging to government agencies and corporate organizations.[11]

The principal Cybercrime Act was unfortunately fraught with several shortcomings some of which clearly repress freedom over the Nigerian cyberspace and civil liberties.[12] Thus, the provision regarding lawful interception of communication for instance is clearly in conflict with, and as such a violation of the provision of Chapter IV of the 1999 Constitution of the

---

3 Nwosu, U. W., "Cybercrime and Nigeria's Receding Economy: The Role of the Legal System", *Op. cit.*

4 *Ibid.*

5 Hereinafter called ICT.

6 Ibikunle, F., 'Approach to Cyber-security Issues in Nigeria: Challenges and Solution', *International Journal of Cognitive Research in Science, Engineering, and Education*, Vol. 1, No.1, 2013.

7 Britannica, "Cybercrime – Identity Theft, Privacy Invasion", [2024], https://www.britannica.com , accessed, 22nd August, 2024.

8 NIN

9 BVN

10 IPPIS

11 *Ibid.*

12 Punch Online, "How Nigerian Authorities use Cybercrime Act to silence free press", [June, 2024], www.punchng.com Last accessed, 16th September, 2024.

Federal Republic of Nigeria regarding the right to privacy[13], and other international laws such as the Universal Declaration of Human Rights, 1948.[14] Although the principal Act granted limitless powers to the President, curiously it does not address the need to prevent cybercrimes, but only makes provision regarding punishment. *Section 8* thereof for instance criminalizes the act of unlawfully interfering with a computer system and goes ahead to fix punishment upon conviction for so doing without criminalizing the actual manufacturing of viruses, which are mostly used for such interference.

Paradoxically, despite some laudable provisions of the Cybercrime Act, when viewed from a domestic perspective, the menace of cybercrime has increased in volume as more young people have recently veered into various forms of internet crimes despite the existence of this law. The reason for this curious development is that cybercrimes, given their cross-border nature cannot effectively be tackled in isolation by any country via domestic legislations *simpliciter* but requires international cooperation by way of mutual legal assistance and cooperation.

Regarding institutions framework, Nigeria has been criticized for dealing with the issue of cybercrime inadequately due to enforcement agencies not being well equipped or having the necessary manpower training and skills, intelligence, and infrastructure to enforce these laws on cybercrime.[15] This includes the Police, Economic and Financial Crimes Commission, and even the Courts. This scenario led scholars like Okorie[16] to conclude that existing legal framework against cybercrime is inadequate and ineffective having regard to their dynamic and cross-border nature. Indeed, it was predicted that cyber-security spending will exceed one trillion Dollars from 2017 to 2020, while annual damages occasioned by same will reach six trillion Dollars by 2021[17] thus accentuating the need for developing countries to embrace global best practices.

The aim of this Paper is to evaluate the impact of the advent of Cybercrime on the Nigerian youth, the potency of the legal framework, and the need for reforms. Specifically, the objectives of this paper are to evaluate: the meaning, nature, and advent of Cybercrime into Nigeria; the causes of the recent foray of several Nigerian youths into various forms of Cybercrimes; the state of the law in Nigeria regarding Cybercrime with emphasis on the Cybercrime Act, 2015 and its recent 2024 amendment; the degree of effectiveness of Law enforcement agencies; and to consider a more practical way forward, given the shortcomings of the domestic legal framework.

Previous studies in this area of our law concentrated on various earlier legislation such as the Economic and Financial Crimes Commission (Establishment) Act, 2004; the Criminal Code Cap. C.38, Laws of the Federation of Nigeria, 2004; the Independent Corrupt Practices and Related Offences Commission Act, 2000; and the Advance Fee Fraud and other Related Offences Act, 2006. By way of a paradigm shift, this paper is based on not just the above legislations, but more recent ones such as the Cybercrime Act, 2015 and its recent

---

13 Section 37.

14 Article 12.

15 Oho, S.O., "A Critical Analysis of the Cybercrime Law in Nigeria", Unpublished Undergraduate Long Essay submitted to the Faculty of Law, Baze University Abuja, 2017, 33.

16 Okorie, C.K., 'Cybercrime in Nigeria: Issues and Challenges', *Orient Law Journal*, Vol. 4, 2021, 19-34.

17 Mbachu, G., & Nazeef, B., "Cybercrime: Nigeria's Losing Battle Against Unrelenting Enemies", https://leadership.ng Accessed, 25th October, 2023.

Amendment Act of 2024; and other Mutual Legal Cooperation Agreements, with their very apt and proactive provisions regarding the fight against Cybercrimes.

Criminals who engage in cybercrimes or perform such illegal computer related activities are often referred to as Cyber-criminals. They include, internet scammers, cyber-terrorists, and identity thieves who usually attempt to gain access to money, assets, or the personal data and information of their targets, or otherwise harm them or their business using computer devices. Cybercriminals routinely make use of computer technology to harvest personal information, business and trade secrets, and also use the internet for other exploitative or malicious activities.

This led Nwosu[18] to conclude that cybercrimes in an interconnected world have become pervasive and require immediate and robust legislation with emphasis on mutual legal assistance and cooperation. They include all crimes imaginable which can now be achieved with the use of computer networks as a tool such as: threat to lives and property; disruption of critical services; terrorism and economic sabotage; propaganda; theft of information, identity, and credit cards, among others. The Nigerian situation targets e-government services, e-Commerce, Electronic activities of the Nigeria Stock Exchange, Cashless banking services, and other Electronic Identification Systems such as the Independent National Electoral Commission[19] Card Reader system, *et cetera*.

According to Cerezo[20], all this put together creates challenges for the public sector particularly as it concerns legislation and investigative as well as prosecutorial capacity and reach. The situation equally affects the private sector which must address technical vulnerabilities in the system it designs and operates, which sometimes traverse many national jurisdictions. The cyberspace brings cybercriminals together to share information, commit crimes, and avoid detection, thereby adding a new dimension to the status of organized crime.[21] Increasingly, therefore, successful attacks are founded on knowledge, cooperation, and deals created and shared between networks of individuals and groups as offenders seek and exploit any weak links or vulnerable locations.[22]

The Current State of Cybercrime Laws in Nigeria

Prior to 2015 when the principal Cybercrime Act[23] was passed into law by the National Assembly, there was no clear and comprehensive Nigerian legislation that targeted cybercrime. Thus, where offences amounting to cybercrimes were committed, the law enforcement agencies and the courts usually relied on several other extant Nigerian legislations that had a bearing on such infractions including, but not limited to: the Economic and Financial Crimes Commission (Establishment) Act of 2004, as revised; the Criminal Code[24]; the Advance Fee Fraud and Other Related Offences Act, 2006; *et cetera*.

---

18 *Supra.*
19 INEC
20 *Supra.*
21 Nicole Mills, "Cyber-security: Why we are Stronger together", [August, 2022], www.cyberdefensemagazine.com Last accessed, 16th September, 2024.
22 *Ibid*.
23 Cybercrime (Prohibition and Prevention) Act, 2015.
24 Cap. C38, Laws of the Federation of Nigeria, 2004 (as revised).

The advent of the Cybercrime Act in 2015 as a specific legislation by the National Assembly targeted at the menace of cybercrime however heralded a paradigm shift in the Nigerian *corpus juris* on the basis of which the war against cybercriminals found renewed impetus. This piece of legislation thus became a turning point in the legal framework for regulating cybercrime in the country. Indisputably, the need for cyber laws in Nigeria is not unconnected with the fact that cybercrime has expanded in the country in direct response to the reality that the digital world itself has grown significantly, leading more people to spend more time online.

The Cybercrime Act 2015 therefore can be referred to as a Cyber law. This refers to any legislation that deals with the internet and similar technology, otherwise referred to as "Law of the Internet" or "IT Law". It presupposes a legal framework for addressing infractions relating to the internet, computing, cyber space, and other associated matters.[25] The need for this evolving branch of law is predicated on the rapid advancement in internet resources and technology. The rationale is premised on the realization that individuals and organizations who use the internet deserve legal safeguards. The scope of Cyber law covers intellectual property, contract, jurisdiction, data protection laws, privacy, and freedom of expression. It thus oversees the distribution of software, information, online security, and e-commerce through the internet. By this channel, e-documents are given legal validity, while establishing a framework for e-commerce and e-filing.[26]

Cyber laws act as a shield over the cyber space, their aim being to confront and possibly prevent cybercrimes. It is thus the government's positive move to erect legal and regulatory frameworks to combat illicit cyber-activities. The Cybercrime Act therefore has a significant impact on other regulations in Nigeria, since it creates a comprehensive legal, regulatory, and institutional framework to prohibit, prevent, detect, prosecute, and punish cybercrimes.[27] The Act thus encourages cyber-security and the protection of both private and public computer systems and their networks, electronic communications, data and computer programs, intellectual property, and privacy rights, as well as important national information infrastructure.[28]

Regarding the administration and actual enforcement, under the Cybercrime Act 2015, the office of the National Security Adviser acts as the coordinating unit for both the security and enforcement authorities, while the Attorney-General of the Federation is charged with the responsibility of reinforcing and improving the country's existing legal framework on cybercrime. As such, the various law enforcement, security, and intelligence agencies are mandated to develop necessary institutional architecture required for effectively implementing the provisions of the Act by collaborating with the office of the National Security Adviser to initiate, develop, or facilitate training programs for personnel saddled with such responsibilities as are directly concerned with cybercrime, both at the domestic and international levels.

---

25 Olisa Agbakoba, "Cybercrimes and Cyber Laws in Nigeria: All you need to know", [July, 2021], https://oal.law Last accessed, 16th September, 2024.

26 *Ibid.*

27 Uba, J., "Nigeria: Cybercrimes And Cyber Laws in Nigeria: All You Need To Know", [2021] https://www.mondaq.com/nigeria/security/108 Accessed, 13th September, 2021.

28 *Ibid.*

The Nigerian government equally set up a Cybercrime Advisory Council, to assume responsibility for handling issues relating to the prevention and combating of cybercrimes, cyber-threat, computer related cases, and the promotion of cyber-security in Nigeria. The Council comprises representatives from various Ministries, Departments, and Agencies of government as well as the private sector business community.[29] The objective is primarily to provide an effective implementation structure for the Cybercrime Act 2015, and enhance punishment of cybercrimes in Nigeria.

Paradoxically, Nigeria's Cybercrime Act 2015, which is the extant Cyber law in the country was more frequently used against journalists, political activists, and critics of the various states and federal government.[30] Thus, the law, since it was passed by the National Assembly ostensibly to secure online security, privacy, and to tackle cyber-fraud while boosting Nigeria's digital economy, became notorious for its frequent manipulation by these authorities to silence criticism and dissent online until it was amended just recently via the Cybercrime (Prohibition, Prevention, etc.) (Amendment) Act 2024 to cure certain defects observed in the principal Act by introducing some novel provisions that are significant to Nigeria's cybercrime regulation.[31] The aim was to improve on, and further strengthen the principal Act. This, it has done by enlarging the scope of the Act against various forms of cybercrimes, ensuring that no financial institution or any public or private person takes advantage of the inadequacies in the principal Act to endanger Nigeria's cyber ecosystem, thus making for a safer and more secure cyberspace.[32]

The following are the most significant of the provisions of the 2024 Amendment Act: the introduction of certified true copies of valid electronic signatures[33]; establishment of Sectoral National Computer Emergency Response Teams[34] or Security Operation Centres[3536]; rephrasing of the wordings of *Section 24* of the principal Act to achieve clarity and certainty[37]; prescription of the use of the National Identification Number (NIN) as a requirement for Electronic Financial Transactions[38]; recognition of the Nigeria Data Protection Act[39]; prescription of a Cyber-security levy payable by certain designated businesses and punishment for default[40]; and, the complete removal of Section 48(4) of the principal Act which hitherto prescribed the cancellation (in case of a Nigerian citizen) or withholding (in case of a foreigner) of the International Passport of any person convicted of an offence under the principal Act.[41]

---

29 Channels Television, "National Security Adviser Sets Up Cybercrime Advisory Council", [2016], https://www.channelstv.com Last accessed, 17th September, 2024.

30 The Africa Report, "Nigeria: Cybercrime law still used to harass citizens despite amendment", [May, 2024], www.theafricareport.com Last accessed, 17th September, 2024.

31 FOLEGAL, "A Review of the Cybercrime (Amendment) Act, 2024", [2024], https://blog.folegal.net , accessed, 23rd August, 2024.

32 *Ibid.*

33 Section 2(b).

34 CERTs

35 SOCs

36 Section 3.

37 Section 5.

38 Section 8.

39 Section 9.

40 Section 11(a) & (b).

41 Section 12.

Challenges in combating Cybercrime

Human beings have become cyber-creatures often spending a significant proportion of their time online. As the cyberspace expands, cybercrimes equally develop across the globe. The need to confront these seemingly uncontrollable phenomena has given rise to cyber laws in virtually every country to act as a shield over the cyberspace and prevent cybercrimes from occurring. Every government is thus committed to developing and enforcing legislation to confront illicit online activities and these legislation or legal frameworks which vary from country to country are known as a Cyber laws. It is an emerging aspect of the global legal system that evolved as a response to the rapid advancement of internet technology to provide legal safeguards for both individuals and corporate organizations who use the internet.

The principal legislation that addresses cybercrimes in Nigeria is the Cybercrime Act, 2015[42] and recently its 2024 Amendment Act. This law regulates the distribution of software, information, online security, and e-commerce over the internet. In conjunction with the revised Evidence Act[43], e-documents are now given legal validity in the field of cyber law, while establishing a dependable framework for e-commerce and e-filing; hence, their importance cannot be overemphasized. Individuals and organizations that are exposed to risks over the cyberspace as a result of an inefficient cyber-security system and who do business or social transactions online thus have an obligation to adhere to peculiar cyber-security guidelines, legislations, policies, and regulations in order to minimize their exposure in terms of risks.

Being an emerging area, issues and questions regarding cyber laws are consistently evolving, while legislators and business leaders are constantly debating how stakeholders should safely use the internet. The federal government through the various law enforcement agencies and the judiciary is expected to partner with the business community to prioritize the raising of awareness of these cybercrime policies and legislations. The need for information security is no longer a matter for the technical and computer savvy alone, but everyone who now engage these new media daily for business, communication, and leisure. It is thus pertinent that a suitable regulatory framework be put in place to ensure safe use of the cyberspace. Unfortunately, there have been several challenges in so doing ranging from the lack of effective legislation to hurdles regarding jurisdiction, slow judicial process, and actual enforcement of available legislation. As at 2010, Nigeria had already been branded one of the major hubs of cybercrime in the world according to the Internet Crime Complaint Centre.[44]
With particular reference to the Cybercrime Act 2015, it is noteworthy that while s*ections 52(2)* and *52(4)* thereof provide for international mutual legal assistance and cooperation using the office of the Attorney-General as the coordinating unit, the said sections are curiously silent on the requirement of the existence regarding countries in question of multilateral or bilateral agreements to facilitate this collaboration. This underscores the necessity of further legislative action to address the need for dual criminality as a prelude to mutual cooperation and collaboration, as well as extradition.

Ordinarily, at international law, in line with the principles of sovereignty and State independence, countries have no obligation to return cybercriminals for trial and this has been a major challenge to the enforcement of cyber laws across the globe.[45] The only exception

42 Cybercrimes (Prohibition and Prevention) Act, 2015.
43 Evidence Act, 2011.
44 IC3 Report, 2010. Available at https://www.ic3.gov , accessed, 23rd August, 2024.
45 Chatham House, "What is the UN Cybercrime Treaty and why does it matter?", [August, 2023], www.chathamhouse.org Last accessed, 17th September, 2024.

then will be where there is an extradition treaty between the countries involved. Curiously however, the principle of jurisdiction is sometimes invoked by some countries as a basis to deny such extradition requests especially countries that have legislations in their *corpus juris* providing for jurisdiction to conduct trials over their nationals for cybercrimes committed abroad including Austria[46], France[47], Germany[48], *et cetera*. Furthermore, extradition of criminals has been legally fettered by cumbersome, time consuming, and expensive nature of the process itself.

Equally significant is the provision of *Section 6* of the Cybercrime Act, 2015 regarding unauthorized access to a computer for fraudulent purpose and for obtaining data vital to national security. While this is clearly criminalized under the said section, the provision curiously raises the difficult issue of proving intent especially given the position of the Evidence Act on facts bearing on the question whether an act is accidental or intentional.[49] The Act also places a high burden of proof on the prosecution where the State seeks to prove connivance between a cybercriminal and the owner of a cybercafé to perpetrate an electronic fraud or online fraud.[50]

Ironically, the onus of proving negligence rests on the affected customer where there is a fraud case, once the financial institution shows that they had put in place, counter-fraud measures to safeguard their information.[51] This may compromise the scale of justice and so strict liability is advocated in all such instances since more often than not, the prosecution and even the judge do not have the requisite computer expertise in terms of forensic knowledge to effectively engage cybercriminals given their computer literacy thus making strict liability a safer option for the state in terms of the burden of proof.

Another important issue is that of jurisdiction.[52] The court must first of all be competent by way of possessing jurisdiction before it can go ahead with any adjudication.[53] Prior to the passing of the Cybercrime Act, there was a lingering uncertainty as to which court had jurisdiction to handle cybercrime offences. From the commencement date of the Act however, this issue has now been settled. The Federal High Court is the court conferred with special jurisdiction to try all cybercrimes in Nigeria.[54] Consequently, all cybercrime cases now enjoy speedy trials devoid of the usual interlocutory applications and appeals regarding jurisdiction.

The Act equally provides for cross-jurisdictional cooperation which ensures that the investigation of such cybercrimes now enjoys mutual legal assistance from foreign countries. The issue however appears to have been settled only at the domestic or intra-territorial level. Indeed, until recently, it was almost unheard of to talk about international consensus on combating cybercrime especially in its trans-boundary shape. Nevertheless, there is now a

46 *Section 12*, Austrian Extradition and Legal Assistance Act.
47 *Articles 696-1* to *696-7* Code of Criminal Procedure (Legislative Part).
48 *Article 16(2)* Basic Law for the Federal Republic of Germany.
49 *Section 12*, Evidence Act, 2011.
50 *Section 7*, Cybercrime Act, 2015.
51 *Section 19*, Cybercrime Act, 2015.
52 *Oloba v. Akereja*, (1988) 1 NWLR (Part 84), 587.
53 Uchechukwu, W. Nwosu, *The Practice of Administrative Law in Nigeria*, (2nd edn), Owerri: Zubic Infinity Concepts Printers, 2018, 201.
54 *Section 50*, Cybercrimes Act 2015.

positive moral climate for enforcement action, whether by civil, criminal, or administrative measures and this trans-boundary cooperation is commendable.

In view of the time-honoured principle of state independence and the authority of each nation state to make laws regulating individuals and things within its territory, conflict of laws situations in cybercrime cases have become inevitable. Indisputably, jurisdiction is ordinarily structured on territorial basis.[55] Consequently, every country guides its sovereignty jealously. Paradoxically, the fact that sovereignty is one of the fundamental principles of statehood has become a major shield that cybercriminals take advantage of to shield themselves from detection, and to conceal the evidence of their crimes which are usually domiciled in different jurisdictions.

The significance of extra-territorial jurisdiction usually comes to the fore particularly in instances where a judgment is sought to be enforced outside its geographical location of origin. This scenario is commonplace in view of the fact that cybercrimes transcend States and jurisdictions being trans-national crimes by default. Besides, in instances where the court cannot try the cybercriminal owing to lack of jurisdiction, the resort to extradition as an option is not automatic since it has its own peculiar challenges apart from the requirements of double criminality and the need for bilateral or multilateral agreements to that effect regarding cooperation.

Another challenge is the anonymous nature of the identity of cybercriminals.[56] Given the unfettered freedom of information and communication, the identities of cybercriminals is usually difficult to trace. This poses a major hurdle regarding both trial and enforcement of a judgment, since according to Lord Denning, in *Macfor v. United African Company*, you cannot put something on nothing and expect it to stand.[57] No law, however well-crafted or intended can be implemented in a vacuum, so if the cybercriminals are not identifiable, any laws passed by the legislature will amount to a nullity. Cybercrime laws have equally been further rendered nugatory by the campaign by human rights activists that putting an end to anonymity in the use of the internet amounts to a violation of privacy rights.[58]

Equally significant is the challenge regarding the nature of evidence available to the prosecution and the admissibility thereof in cybercrime trials which is typically forensic,[59] and was previously perceived as tenuous at best. Unfortunately, physical evidence is rare in cybercrime cases leaving the prosecution, and the courts with only electronic or digital evidence which is usually sensitive and often located in different jurisdictions thus requiring legally compliant procedures for its collection and preservation. Despite the overwhelming advantages of electronic evidence, there are inherent challenges, principal among which is its admissibility given its vulnerability to damage or manipulations, and the propensity of willful destruction of such evidence, or intentional impersonation of innocent individuals to steer off the trail of investigation regarding the real identity of cybercriminals.[60]

---

55 Uchechukwu, W. Nwosu, *The Practice of Administrative Law in Nigeria*, *Supra.*

56 George F. Du Pont, 'Criminalization of True Anonymity in Cyberspace', The Michigan Telecommunications And Technology Law Review, Vol. 7., Issue 1, 2001, 191.

57 (1962) AC 152. See also: *Nwosu v. Imo State Environmental Sanitation Authority (1990) 2 NWLR (Pt. 135) 688; Nyavo v. Zading (YL 124 of 2015) [28th July, 2016] NGCA 10.*

58 UNODC, "Obstacles to Cybercrime Investigations", https://sherlocc.unodc.org Lastaccessed, !7th September, 2024.

59 Microsoft Encarta Dictionary, [2017], https://answers.microsoft.com , accessed, 23rd August, 2024.

60 Cybersource, "2023 Global Fraud Report", [2023], https://www.cybersource.com , accessed, 23rd August, 2024.

There is also the problem of lack of effective reporting and dearth of data in the course of cybercrime regulation.[61] Although several countries across the globe have enacted cyber laws and policy, these regulations often do not achieve the intended results owing to a clear lack of effective reporting of incidences of cybercrime to relevant authorities thereby obviating the need to bring the exact extent of the cybercrime menace to the attention of law enforcement authorities. This obvious lack of cooperation on the part of victims towards law enforcement due to the cost implication, time consuming nature, and damage to the reputation and goodwill of corporate victims all add up to sabotage cybercrime investigation especially since the lack of reporting leads to, and indeed causes a dearth of data, and by extension a lack of awareness.[62]

Regarding the cost, time, and effort required to investigate and prosecute cybercrimes, the high-tech equipment, materials, and expertise required to investigate and obtain forensic evidence is huge since the world is a global village.[63] Given the universality of the cyberspace, investigators and other law enforcement agents in cybercrime cases go through arduous tasks to break encrypted codes and unravel clues that can lead to the arrest and possible prosecution of cybercriminals. The same herculean process is faced in the identification of the perpetrators especially when such cybercriminals are in a different country. In such instances, the investigators usually incur additional costs associated with their mandate such as travel costs, accommodation, telephone bills, cost of hiring interpreters where there are language barriers, estacodes, actual cost of hiring lawyers and associated litigation costs, *et cetera*.

The drift towards an International Economic Law

It is now indisputable that given the fact that cybercrime investigations by default require extensive cross-border cooperation and coordination, both domestic and international legal frameworks need to be brought up to speed with this reality. The existing legal framework for cooperation on cybercrime appears fragmented without a uniform governance architecture. This situation complicates the investigation and prosecution of culprits and equally sets the stage for cybercriminals to escape justice. Perpetrators therefore take advantage of these legislative gaps by taking refuge in countries that have insufficient, or inefficient cybercrime laws as safe havens[64] thus accentuating the need for the development of International Economic Law.

Understandably therefore, the United Nations Office on Drugs and Crime[65] has posited that due to the global nature of Information and Communications Technology, it is difficult to prescribe a national jurisdiction for cybercrime. The international community must therefore coordinate and cooperate in order to sufficiently address cybercrime in relation to both online transactions and intellectual property.[66] Cybercrime is multifaceted and so, the importance of collaboration between States, the private sector, civil society, and law enforcement in order to

---

61 World Economic Forum, "Why We Need Global Rules to Crack Down on Cybercrime", [2023], https://www.weforum.org accessed, 22nd August, 2024.

62 *Ibid*.

63 Mchuan, M., *The Gutenberg Galaxy: The Making of Typographic Man*, London: University of Toronto Press, (16th edn.), 2011, 132.

64 Nwosu, U. W., "Cybercrime and Nigeria's Receding Economy: The Role of the Legal System", *Supra*.

65 UNODC.

66 UNODC, "Comprehensive Study on Cybercrime", *http://www.unodc.org/documents/organized-crime/UNODC* , CCPCJ EG.4 2013/CYBERCRIME STUDY 210213.pdf Accessed, 3rd September, 2024.

create a comprehensive approach to the issue cannot be overemphasized. The challenges include: attacks against information infrastructure and internet, as well as all other forms of cyber-threats.

International Economic Law is an increasingly seminal field of International law that involves the regulation and conduct of States, international organizations, private firms, and recently individuals operating in the international economic arena. It encompasses a broad range of disciplines touching on Public International law, Private International law, and Domestic law applicable to international business transactions, commerce, and leisure. For several decades, it was most often associated with international trade, largely because of the fact that trade had developed the most mature multilateral legal institutions such as the General Agreement on Tariffs and Trade[67] and later the World Trade Organization[68] for governing international commerce.[69] Today however, a range of other disciplines are routinely acknowledged as being as impactful and relevant to the field, including international monetary law, international financial regulation, international investment law, *et cetera*.[70]

International Economic Law in general is therefore concerned with the governance of international economic relations between two or more States as they affect individuals in a state, especially and in particular their relations *inter se* across national boundaries.[71] Where such a regulation applies to just two States, it is called a bilateral economic regulation, while a regulation applying to more than two States is referred to as a multilateral economic regulation. Its sources include treaties, customary international law, general principles of law recognized by civilized nations, and recently the concept of International cooperation.[72]
International Cooperation, otherwise referred to as Mutual Legal Assistance and Cooperation in the context of cybercrime regulation implies the voluntary coordinated action of two or more countries occurring under a legal regime and serving a specific objective. The policy challenges created by criminal and malicious activities of cybercriminals over the cyberspace at the regional, continental, and international arena requires not just a harmonized cyber-security framework but a flexible mechanism that ensures cooperation and sharing of information regarding cybercrimes by all stakeholders since cybercriminals operate globally using current and developing technologies.[73]

Within the context of cybercrime regulation therefore, International Economic Law broadly covers issues such as extradition, mutual legal assistance, and general measures to ensure cross-border cooperation on cyber-security issues. Such measures include the sharing of information and resources within a bilateral or multilateral framework with the aim of facilitating efficient responses to cyber threats.[74] The kernel of the matter is that law

---

67 GATT

68 WTO

69 IMF eLibrary, "The Multilateral Trading System and the Uruguay Round of Trade Negotiations: An Arab Perspective" [December, 1992], https://www.elibrary.imf.org Last accessed, 17th September, 2024.

70 Payne, C., & Finlay, L., 'International Law Cannot Keep Up with Cyber-Criminals', [2019], *https://www.weforum.org/agenda/2019* Accessed, 1st July, 2024

71 Oxford Bibliographies, "International Economic Law", https://www.scirp.org Last accessed, 17th September, 2024.

72 Irina Chernykh & Daniil Volodin, 'The Principle of International Cooperation and Sharing of Information Principle under International Space Law: Towards Synergy', *Space Policy*, Volume 67, 2024.

73 S Chen, "Exploring the global geography of cybercrime and its driving forces" , [2023], https://www.nature.com Last accessed, 17th September, 2024.

74 *Ibid*.

enforcement agencies still face the challenge of an obligation to respond effectively in all cross border investigations since with the increasing wave of trans-border crimes and the attendant consequences on the economy of nations, it is impossible to successfully conduct cybercrime investigation and prosecution of culprits without efficient regional and international cooperation with other countries.[75]

Given the circumstances, serious attention is increasingly being paid to how priority can be given to mutual legal assistance and cooperation at the international level, to ensure effective policing of cybercrimes. Cooperation in this sense is not just from the standpoint of operational linkages, but also in term of sharing of experiences and capacity building against cybercrime.[76]

Besides, jurisdictional challenges are heightened in the face of fragmented and localized laws that do not set a clear architecture for cooperation. These and other nutty challenges such as complex official and bureaucratic requirements make the entire investigation and prosecutorial process cumbersome. The likelihood of promptly negotiating a new and globally acceptable United Nations Treaty on cybercrime is equally very bleak given the slow movement of previous treaties from conception to ratification as experience has shown that implementing a new global treaty always takes several years.[77] The alternative is for more diplomatic effort to be channeled towards engaging more countries to consider embracing the Council of Europe Convention, 2001 by addressing the concerns earlier raised by non-members,[78] in view of the fact that the Convention already provides a global legal framework for cooperation and has proven to be relatively effective in creating more synergies among its present signatories.

Conclusion

There is no gainsaying the fact that there exists a clear nexus between unemployment and crime rate especially in the developing countries of the world such as Nigeria. The trend of development across the globe and the drift towards virtual electronic transactions both for commercial, business, and leisure purposes makes it inevitable for majority of the world's population to necessarily embrace online transactions. This naturally exposes everyone to the new wave of crimes available within the cyberspace, thus making all potential targets and impending victims. As more information about each person is progressively made available online, cybercriminals keep closing in on almost everyone by harvesting these personal data and information no matter how well they are stored. This trend is likely to continue except governments in developing countries such as Nigeria create legitimate employment for their teeming youth population.

Indisputably, given the trans-boundary nature of cybercrimes, domestic legislation and regulations are no longer effective since often the evidence, victim(s), proceeds of crime, and the actual cybercriminals are usually in different jurisdictions making it practically impossible for both the law enforcement authorities and the legal framework at the domestic

---

75 UNODC, "Strengthening International Cooperation to Combat Cybercrime", https://www.unodc.org , accessed, 22nd August, 2024.

76 The Council of Europe, "International Cooperation Against Cybercrime", https://www.coe.int , accessed, 22nd August, 2024.

77 Chatham House, "What is the UN Cybercrime Treaty And Why Does it Matter?", [2023], https://www.chathamhouse.org , accessed, 22nd August, 2024.

78 CCDCOE, "Battling Cybercrime Through the New Additional Protocol", [2021], https://ccdcoe.org , accessed, 23rd August, 2024.

level to be effective. This verity makes resort to mutual legal assistance and cooperation both desirable and inevitable thus making international economic law unavoidably the way to go.

Recommendations

Given the above scenario, the following recommendations are put forward to guide the Nigerian authorities:

First, it is recommended that strict liability be proposed on the part of banks and financial institutions in cybercrime offences involving the loss of money in the accounts of individuals or corporate organizations.

Second, it is recommended that cybercrime reporting should be structured to factor in the anonymity of victims as well in order to encourage most of them to volunteer information that will assist law enforcement officials to further understand the working system of these crimes.

Third, there is an urgent need for the Federal Government to create employment opportunities for the teeming youth population since it is the high level of unemployment in the country that is responsible for the recent foray of most Nigerian youth into various forms of cybercrime.

Fourth, law enforcement agencies and institutions should be better funded and equipped by the various levels of government, while an aggressive manpower training of their personnel is further advocated.

Fifth, there is need for improved cybercrime legislation both at the domestic and international levels to engender a more robust and effective cybercrime policing. This should prioritize mutual legal assistance and cooperation, extradition procedures, and free flow of data, information, and movement of personnel.

Sixth, more African countries need to pass domestic cybercrime legislation, align them with international best practices, and indeed ratify and domesticate the African Union Convention on Cyber-security and Personal Data Protection 2014, as well as other international laws regarding cybercrime to enhance applicability to suit local conditions.

Seventh, all countries across the globe should prioritize the ratification and domestication of international Conventions and Treaties regulating cybercrime while aligning their domestic legislations to these international legal instruments for greater effectiveness.

Finally, the federal government through the various law enforcement agencies, as well as the judiciary is urged to partner with the business community to prioritize the raising of awareness of these cybercrime policies and legislations.

REFERENCES

BOOKS

Mchuan, M., *The Gutenberg Galaxy: The Making of Typographic Man*, London: University of Toronto Press, (16th edn.), 2011.

Microsoft Encarta Dictionary, [2017], https://answers.microsoft.com , accessed, 23rd August, 2024.

Nwosu, U. W., *The Practice of Administrative Law in Nigeria*, (2nd edn), Owerri: Zubic Infinity Concepts Printers, 2018.

Nwosu, U. W., "Cybercrime and Nigeria's Receding Economy: The Role of the Legal System", *Institute of Public Policy & Administration [IPPA], Unical Book Series*, Lagos, Advanced Publishers Limited, 2018.

The Levin Institute, "How is International Law Enforced", The University of New York, *Institute of International Law Yearbook*, 2018.

CONFERENCE PROCEEDINGS

African Forum on Cybercrime, Conference Program on the theme: "Policies and Legislation, International Cooperation, and Capacity Building', held at Addis Ababa, Ethiopia from 16-18th October, 2018.

IC3 Report, 2010.

JOURNALS

Ajayi, E.F.G., 'Challenges to Enforcement of Cybercrime Laws and Policy', *Journal of Internet and Information Systems*, Vol.6, Issue 1, 2016, 1-12.

Du Pont, G. F., 'Criminalization of True Anonymity in Cyberspace', The Michigan Telecommunications And Technology Law Review, Vol. 7., Issue 1, 2001, 191. Global Cyber-security Index, 2018.

Ibikunle, F., 'Approach to Cyber-security Issues in Nigeria: Challenges and Solution', *International Journal of Cognitive Research in Science, Engineering, and Education*, Vol. 1, No.1, 2013.

Okorie, C.K., 'Cybercrime in Nigeria: Issues and Challenges', *Orient Law Journal*, Vol. 4, 2021, 19-34.

LEGISLATIONS

Austrian Extradition and Legal Assistance Act.

Basic Law for the Federal Republic of Germany.

Code of Criminal Procedure (Legislative Part).

Constitution of the Federal Republic of Nigeria, 1999.

Cybercrimes (Prohibition and Prevention) Act, 2015.

Evidence Act, 2011.

ONLINE RESOURCES

Agbakoba, O., "Cybercrimes and Cyber Laws in Nigeria: All you need to know", [July, 2021], https://oal.law Last accessed, 16th September, 2024.

Britannica, "Cybercrime – Identity Theft, Privacy Invasion", [2024], https://www.britannica.com , accessed, 22nd August, 2024.

Chen, S., "Exploring the global geography of cybercrime and its driving forces" , [2023], https://www.nature.com Last accessed, 17th September, 2024.

Chernykh, I., & Volodin, D., 'The Principle of International Cooperation and Sharing of Information Principle under International Space Law: Towards Synergy', *Space Policy*, Volume 67, 2024.

Channels Television, "National Security Adviser Sets Up Cybercrime Advisory Council", [2016], https://www.channelstv.com Last accessed, 17th September, 2024.

Chatham House, "What is the UN Cybercrime Treaty and why does it matter?", [August, [2023], www.chathamhouse.org Last accessed, 17th September, 2024.

Chernykh I., & Volodin, D., 'The Principle of International Cooperation and Sharing of Information Principle under International Space Law: Towards Synergy', *Space Policy*, Volume 67, 2024.

Council of Europe, "International Cooperation Against Cybercrime", https://www.coe.int , accessed, 22nd August, 2024.

Cybersource, "2023 Global Fraud Report", [2023], https://www.cybersource.com , accessed, 23rd August, 2024.

Data Protection Africa, "AU's Malabo Convention Set to Enter Into Force After Nine Years", [2023], https://dataprotection.africa , accessed, 22nd August, 2024.

ECOWAS, "ECOWAS And the Council of Europe Join Forces to help West African Countries in the Fight Against Cybercrime", [2017], https://old22.ecowas.int , accessed, 22nd August, 2024.

FOLEGAL, "A Review of the Cybercrime (Amendment) Act, 2024", [2024], https://blog.folegal.net , accessed, 23rd August, 2024.

IMF eLibrary, "The Multilateral Trading System and the Uruguay Round of Trade Negotiations: An Arab Perspective" [December, 1992], https://www.elibrary.imf.org Last accessed, 17th September, 2024.

Mbachu, G., & Nazeef, B., "Cybercrime: Nigeria's Losing Battle Against Unrelenting Enemies", https://leadership.ng Accessed, 25th October, 2023.

Mills, N., "Cyber-security: Why we are Stronger together", [August, 2022], www.cyberdefensemagazine.com Last accessed, 16th September, 2024.

Oxford Bibliographies, "International Economic Law", https://www.scirp.org Last accessed, 17th September, 2024.

Payne, C., & Finlay, L., 'International Law Cannot Keep Up with Cyber-Criminals', [2019], *https://www.weforum.org/agenda/2019* accessed, 1st July, 2024.

Punch Online, "How Nigerian Authorities use Cybercrime Act to silence free press", [June, 2024], www.punchng.com Last accessed, 16th September, 2024.

SADC, "Discussing Cyber-Security and Cybercrime in the SADC Region (Africa)" https://www.sadc.net/en/southern-african-news-features/sadc-response-to-cybercrime/ accessed, 11th October, 2021.

The Africa Report, "Nigeria: Cybercrime law still used to harass citizens despite amendment", [May, 2024], www.theafricareport.com Last accessed, 17th September, 2024.

Uba, J., "Nigeria: Cybercrimes And Cyber Laws in Nigeria: All You Need To Know", [2021] https://www.mondaq.com/nigeria/security/108 accessed, 13th September, 2021.

UNCTAD, "Least Developed Countries Still Lag Behind in Cyber Law Reforms", [2022], https://unctad.org , accessed, 25th August, 2024.

UNODC, "Comprehensive Study on Cybercrime", *http://www.unodc.org/documents/organized-crime/UNODC*, CCPCJ EG.4 2013/CYBERCRIME STUDY 210213.pdf accessed, 3rd August, 2024.

UNODC, "Strengthening International Cooperation to Combat Cybercrime", https://www.unodc.org , accessed, 22nd August, 2024.

Wikipedia, "Spanish Prisoner", https://en.wikipedia.org accessed, 22nd August, 2024.

World Economic Forum, "Why We Need Global Rules to Crack Down on Cybercrime", [2023], https://www.weforum.org accessed, 22nd August, 2024.

PERIODICALS

Legal Brief E-Law & Management Cyber-law & Technology Watch, Issue No. 1581, 2015.

UNPUBLISHED WORKS

Oho, S.O., "A Critical Analysis of the Cybercrime Law in Nigeria", Unpublished Undergraduate Long Essay submitted to the Faculty of Law, Baze University Abuja, 2017.