"The Internet is a paradise for those who prey upon the gullible, the greedy or the vulnerable. …[I]t provides unprecedented access to victims."
Jonathan Clough, Principles of Cybercrime, 2015, 2nd Ed. Cambridge University Press, p. 210

CYBER OFFENCES IN THE DIGITAL STRATOSPHERE: CIVIL AND CRIMINAL IMPLICATIONS AND TACKLING THE MENACE

Introduction

My Lord, the Chief Judge of Lagos State, My Lord, the co-Guest Speaker, Hon justice Williams Dawodu, JCA, My Lords of the Lagos State High Court and various other jurisdictions here present, learned Senior Advocates of Nigeria, learned colleagues of the utter Bar, distinguished ladies and gentlemen, and gentlemen of the fourth estate of the realm present.

It is a privilege to address you on a topic of paramount importance in our modern society: *Cyber Offences in the Digital Stratosphere: Civil Implications and Tackling the Menace*. In an era where technology drives our economy, communications and social interactions, it is essential that we address the dark side of this digital revolution—the rise of cybercrime. Of course, this is based on the assumption that technology and its applications have vast benefits in the system, just as much as it has corresponding liability, in other words, the more the use of computers, the more profound the opportunities for criminals. This is further exacerbated by the proliferation of tablets, mobile phones and other portable devices now accessible to all. This is coupled

with the increased governmental activities online, even mere recruitment of staff.

As technology increases daily, so also is the zeal to acquire the latest technology. Keeping pace with technological development is even becoming a challenge for most people. Before we finish digesting one technology , another is already out there. The resultant effect of this is incremental steps in the crimes committed through the devices and technology. So, as you update your devices and technology periodically, so also is your risk profile increasing. Essentially, what we want to interrogate in this attempt is the misuse of computer technology and cyber space. The devices, according to CLOUGH now "allows offenders to reach millions of potential victims at virtually no cost". All that seems to be required in contemporary period in the perpetration of cybercrimes is internet connectivity. The highest danger these days is the use of technology to recruit terrorists and attack websites, particularly of government and large corporations.

Cybercrime is a global challenge, but it has a particularly unique flavor here in Nigeria. It is a transborder crime in some instances. Our nation, while being a leader in technological adoption across Africa, has also been associated with certain notorious cyber activities, the most infamous being what is dubbed after the relevant section of the Criminal Code called "419" scams. Today, the prevalence of internet fraud known as "*Yahoo, Yahoo*" in the country is a source of worry to all and sundry. The sad commentary on this is that substantial number of our youth are now into the 'trade". While the Economic and Financial Crimes Commission (EFCC) should be fully engaged with tackling economic governance crimes and its associated acts, the Commission is now spending valuable time and resources pursuing the perpetrators of internet frauds. The situation is so bad in the country today that there are even informal schools established for the training of these youths in the criminal trade. Not too long ago, it was reported that there was

even in existence an association of the mothers of the fraudsters involved in these activities. I remember handling a case recently in which the mother of the perpetrator of the crime served as the conduit pipe for the receipt and processing of the illicit fund. What a shame!

As we battle this, so also, we are battling the plague of cyber bullying, stalking and other defamatory practices via the digital platforms. However, as we delve deeper into this issue today, we will see that cybercrime is evolving and expanding beyond this narrow confine, impacting our economy, reputation and personal lives in unprecedented ways. Why is the world in this turmoil? The fact is that the same set of gurus that innovates, are the same class that unethically commits, promotes and sponsors the attacks on the system. It is simply a case of abuse of knowledge. There is no more any safe haven again as far as internet frauds are concerned.

As our daily lives are now substantially governed by technology, so also are we daily vulnerable to internet frauds. In our Financials, we now rely substantially on online transactions. At the hospitals, our records are kept in electronic format, just as even our identity is now in data form. Feeding itself is becoming so much digitalized that we hardly have to interface with any trader again to get our desires as goods are ordered online only to be delivered at our doorsteps. Education generally is now virtually based on online materials, including virtual learning in non-physical classrooms. In our profession, Artificial intelligence is creeping in already. Coupled with remote hearing, fillings are now done electronically, so also are judgments delivered online and electronically archived. Families, even within the same home, now converse through technology. A worse one is that physical social interaction is now at the lowest ebb. Gone were the days that event of this nature was held physically, providing opportunity for interaction and networking. Virtually all our lives now revolve round technology. The good old days, in my view, are vanishing fast. Adieu!

As we embrace new technologies, however, we must realise that the more crimes we are likely to be experiencing and harvesting. Traditionally, cybercrimes used to be confined to money laundering through online systems, child sex offences like pornography, cyber-terrorism and cyber-espionage, identity theft, stalking, harassment and bullying through online messages electronic funds Transfer, Click frauds, and phishing. Phishing involves sending emails claiming to be from a person's online banking, informing the user that something is 'wrong' with their accounts and they should rectify it. These emails often contain links to fake websites that steal personal details.' This has, however, extended to the broadcast of subversive elements; destructive ideas; indoctrination for groups; invasion of websites etc. Remember the Estonia digital infrastructure attack of 2007, attacks on master and visa cards websites virtually disrupting the financial system. It is said that we are in the information technology age.

The essence of this discourse is to enlighten ourselves through interactions as to why we must prepare for the eventualities and forestall being victims of cyber-crimes. How do we protect our lives, personal and official dealings from the internet invasion? What do we expect from the stakeholders such as the providers of services, regulators and by extension, the government etc. in the event of being victims of cyber-crimes? Cybercrimes now pose significant challenges to every user of the internet service, lawyers, judges, business men, companies, governments etc. As indicated earlier, the more we depend on internet and technology, the more cybercrimes fester. For example, cloning of face and voice now. The range of offences are limitless and in order to protect citizens and businesses, governments all over the world have enacted legislation to regulate cyber uses and define offences relating to cybercrimes with punishments attached. In Nigeria, the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (as Amended in 2024) is the Act regulating cybercrimes. It is this Act that shall be

our statutory guide in this discourse. However, prior to venturing into full discourse of this paper, permit me, for the purpose of proper grasp of the subject of discussion, to interrogate conceptually, the meaning of the key words.

CONCEPTUAL CLARIFICATIONS.

Commencing with the word "cyber offences" otherwise known as cyber-crimes, internet crimes, computer crimes, high-tech crimes, information technology crimes, electronic crimes etc., there appears to be no precise definition of cybercrime. The first place to first seek an understanding of what amounts cybercrimes ought to be the relevant statute, as what amounts to an offence is what is statutorily so prescribed with the relevant punishment attached.[1] Unfortunately, the Act regulating cybercrimes in Nigeria, the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (as Amended in 2024) provides for no definition of the word 'cybercrime' hence the need to have recourse to definition by writers.

According to *Yousef Nawafleh, Abdulla Nawafleh* and *Sahem Nawafleh* in their publication, "Cybercrimes: Concept, Forms and Their Civil Liabilities" described cybercrimes thus:

> "Cybercrimes are crimes which occur through the internet, information, networks and illegal access to private networks such as companies, Banks and others, individuals, and the misuse of digital data which contain information such as counterfeiting or data corruption and omission, possession of tools or secret words to facilitate crimes that cause damage to the data and information itself , as well as network software and hardware that they contain."[2]

[1] See Section 36(12) of the Constitution of the Federal Republic of Nigeria, 1999 (as amended).
[2] *Yousef Nawafleh, Abdulla Nawafleh* and *Sahem Nawafleh*, "Cybercrimes: Concept, Forms and Their Civil Liabilities" International Journal of Arts & Sciences, CD-ROM. ISSN: 1944-6934 :: 09(01):211–234 (2016), 213-214. Also avaiilable on

Similarly, Dr Hesham Fareed Rostom, in his publication in "Penal Code and the Dangers of Information Technology", (Modern Machines Library, Asyout, 1992, P. 29), describes cybercrimes as "All forms of illegal and wrongful conduct carried out through using computers."

Inferable from the above attempts at defining cybercrime is the difficulty inherent in precisely capturing the nature and essence of cybercrime. The description of cybercrime is therefore infinite just as the concept is nebulous. However, what amounts to crime can only be as defined by statute, and it may be said that not all wrongful use of the computer or internet will amount to cybercrime except such acts as are prescribed to be offences. This is understandable against the background that as technology develops, the more the criminals innovate. As reflected in the UK legislation on Cyber crimes, any attempt to define cybercrime will either lead to under-inclusion or over-inclusion, both of which come with attendant consequences. This may be the reason that the Nigerian Act also shied away from providing a general definition of what amounts to cybercrime. By way of working description, however, we can say that cybercrime refers to *illegal activities that involve the use of digital technology and networks*. At times, I am tempted to describe it as borderless crimes, the import of which is that such conduct or misconduct must have some form of criminal or civil implications. Please note that eavesdropping without lawful backing could also amount to a cybercrime.

The challenge in precisely capturing the scope of cybercrime is also traceable also to the difficulty of defining what a computer is. This is also not free from controversy and that explains why in the Australian jurisdiction, the court's position is that the meaning of what a computer is, is best left to the courts depending on the circumstances

<https://www.researchgate.net/publication/323394145_CYBERCRIMES_CONCEPT_FORMS_AND_THEIR_CIVIL_LIABILITIES> last visited on 16 September 2024.

of each case. This is why the view expressed in the case of WILSON v. COMMISSIONER OF STAMP DUTIES (1988) 13 NSWLR 77@78 PER KIRBY, P is apt in the following language:

> "These are times of particularly rapid technological change. The legislature, with the many pressures upon it, may have insufficient time quickly to elaborate statutory provisions specifically to refer to new technological developments. Accordingly, it may be an appropriate modern canon of statutory construction to adopt language of generality, although originally designed to apply to an earlier technology, to apply to the supervening technology as well."

We can, therefore, conclude that to know what cybercrime is, we need to know those acts that have been proscribed and identified as offences for which punishments have been prescribed.

We must observe that some of the offences identified above as cybercrimes had existed in manual form before the advent of the computer. For instance, advance fee fraud otherwise known in Nigeria as "419" which refers to the section of the Nigerian Criminal Code dealing with fraud, and it has become synonymous with advance fee fraud schemes. These scams typically involve a promise of large financial rewards in exchange for small upfront payments, but the promised rewards never materialize. It can thus be concluded that a cybercrime is an offence prescribed in the Cybercrimes Act and for which a punishment is prescribed.

In the past, these scams were mostly perpetrated through letters and faxes. However, with the advent of the internet, they have evolved and become more sophisticated. Scammers now use email, social media platforms, and even dating websites to target victims. In recent years, we have seen the rise of Business Email Compromise (BEC) schemes,

where fraudsters impersonate company executives to trick employees into transferring large sums of money.

Unfortunately, these scams have tarnished Nigeria's international reputation, leading to the stereotype of the "Nigerian Prince" scam. However, it is important to note that not a great number of Nigerians are involved in these activities, and many Nigerians are working tirelessly to combat this negative image.

In the modern era, 419 scams have also adapted to new technologies. Cryptocurrency, for instance, has become a new frontier for fraud, with scammers convincing victims to invest in fake digital currencies or fraudulent initial coin offerings (ICOs). This evolution of 419 shows that cybercriminals are constantly adapting, and our strategies to combat them must also evolve.

Terrorists also abuse technology now to recruit followers. In the light of the above, therefore, the definition of cybercrime will appear intractable, as it is constantly evolving. Not all crimes associated with the cyberspace are often recorded, particularly where there is no loss. The magnitude is best envisioned than asserted.

Crime

The term ‘crime’ can be described as an act or omission forbidden by law with penal consequences attached to its happening. It is in the light of the above that we shall not bother to discuss further what actually amounts to a crime having indicated earlier that a crime is what has been statutorily prescribed to be an offence and for which a punishment is prescribed. The above becomes most imperative in view of Section 36(12) of the Constitution which forbids a person from being convicted of an offence not defined and the penalty prescribed in a written law. The same subsection of the Constitution goes ahead to define a written law as “an Act of the National Assembly or a Law of a State, and

subsidiary legislation or instrument under the provisions of a law." See *Okafor v. Lagos State Govt & Anor* (2016) LPELR-41066(CA) (Pp. 34-35 paras. E); Jadny Trust Ltd v. State of Lagos & Ors (2018) LPELR-47646(CA) (Pp. 31-33 paras. D)

Civil

Another critical term in our paper of today is the word "civil" as the topic requires us to look at the civil implications of cybercrimes. One may wonder whether an act said to be criminal in nature could have civil implications. It sounds contradictory but it can be understood from the perspective of a cybercrime victim being entitled to some civil compensation or some aspects of criminal regulations of cybercrimes that can be applicable in civil proceedings.

The term 'civil' in this regard should be understood from the perspective of what is not criminal. For instance, the word 'civil' may be seen from the perspective of civil law which is that "part of a country's set of laws that is concerned with the private affairs of citizens, for example marriage and property ownership, rather than with crime." (See https://www.collinsdictionary.com/dictionary/english/civil-law accessed on 14/09/2024 at about 7.34 pm.). Thus, in this regard, we shall be considering what civil rights can arise in an action relating to cybercrimes. In addition to this are certain provisions of the Cybercrimes Act which regulate some civil transactions, and while such provisions create offences and penalties, they cannot be precluded from regulating the civil transactions they relate to. All these shall be considered *anon*.

Digital Stratosphere

The expression, 'digital stratosphere', can be understood from the decomposition of the two words "digital" and "stratosphere". The word "digital" can be defined as

“1. (of signals or data) expressed as series of the digits 0 and 1, typically represented by values of a physical quantity such as voltage or magnetic polarization; 2. (of a clock or watch) showing the time by means of displayed digits rather than hands or a pointer.” (See “digital”, online publication accessed on 14/09/2024 at about 7.42 pm.). Miriam Webster Dictionary defines the word “digital” as follows: “of, relating to, or utilizing devices constructed or working by the methods or principles of electronics”. The implication is that something is digital if it utilizes devices constructed or working by the methods of principles of electronic.

On the other hand, is the word “stratosphere”. This is a technical word relating to “the layer of the earth's atmosphere above the troposphere, extending to about 50 km above the earth's surface (the lower boundary of the mesosphere).” That definition is according to the Oxford Languages. Miriam Webster Dictionary defines it as “**1.** the part of the earth's atmosphere which extends from the top of the troposphere to about 30 miles (50 kilometers) above the surface and in which temperature increases gradually to about 32°F (0°C) and clouds rarely form.; **2:** a very high or the highest region on or as if on a graded scale.”

The basic connotation of the expression “digital stratosphere” is a region that is far and above the surface of the earth where the regular rules of law can be said not to be directly applicable as they are difficult to be subjected to a particular jurisdiction. It is not an actual location but a non-physical jurisdiction where activities capable of aiding or complicating normal daily transactions are carried out by virtue of use digital equipment. For an event that takes place in an international flight, for instance, it may be difficult to say which particular law of a country shall govern the activity or transaction thereof which is applicable in private international law or what is otherwise known as ‘conflict of laws. That is the civil aspect, but here,

we are confronted with offences or acts carried out digitally with the effect of the transactions being felt in other or many other jurisdictions.

While a major exception to the application of conflict of laws principles is criminal jurisdiction which is basically territorial and constitutes an expression of sovereignty of every country, it is clear that cybercrimes have thrown up the issue of which country shall exercise jurisdiction where the offence in issue is transborder in nature? This has led many writers to the fantasies of statelessness where they contend that the internet is above our regular jurisdictions. An example is activist like John Perry Barlow of the Electronic Frontier Foundation who issued the Declaration of Independence of Cyberspace. (See Fukuyama, F., The Origins of Political Order, Profile Books, Ltd., 2011, p. 12.) This will lead us to consider the relevance and application of legislations attempting to regulate cybercrimes in view of the tendency of such crimes to be transborder or transnational. I believe this is what informed the topic of this discourse as framed.

CATEGORIES OF CYBERCRIMES

In Nigeria, by the scheme of the Cyber Crimes Act, cybercrimes are often categorized into two broad types:

1. **Crimes Against Individuals:

These include cyberstalking, online harassment, identity theft, and financial fraud. Individuals are targeted for their personal information, which can be used for illicit financial gain or even to ruin reputations.

2. **Crimes Against Organizations and the State:

This category includes hacking into government systems, corporate espionage, data breaches, and even attacks on critical infrastructure like banking systems and telecommunications networks. Just recently, we learnt of the attack on the website of Guaranty Trust Bank and the

hacking of the Sterling Bank's system by which cyber criminals attempted to scoop more than 2 billion Naira from the treasury of the bank but which was nipped in the bud. Remember that attack against Betnaija, an online lottery business company and several other corporate bodies. I equally recall the several attempts made on the portal of INEC during the last general elections in 2023.

A notable aspect of cybercrime in Nigeria just as elsewhere, as opined above, is that it transcends geographical boundaries. Perpetrators may be located in Nigeria but their victims could be anywhere in the world, making it a global issue with local implications and global complications. They are often regarded as transnational crimes. At times, challenge to jurisdiction often rears its ugly head in the process of prosecution, thus inviting the application of the principles of conflict of laws. If time and space permits, we will venture but if not, it will suffice to note that cybercrimes create conflict of law problem.

Although the assigned topic requires me to speak to the criminal and civil implications of cybercrimes, I must confess that I am at a loss as to the import of this. By the very nature of the designation of the acts and conducts that constitute cybercrimes, such ordinarily cannot have civil implication *stricto sensu*. However, if the context of the usage is in terms of civil remedies or impacts on the society, then it is explorable. To therefore agitate that aspect of this discourse, I believe that it is pertinent first and foremost that we consider the criminal import of cybercrimes.

Criminal Implications of Cyber Offences

Cybercrimes are generally regulated by law. This is due to the nature of the crime described above. This also stems from the fact that the crime is dynamic and developing daily. Thus, the more the technology

advances, the more the increment in cybercrimes, and the more the legislative work.

Let me commence by stating that prior to the Cybercrimes Act, some of the conducts presently regulated by the Act have been constituted under various other criminal and civil laws. For example, obtaining under false pretense or deception have always been under our criminal laws while the tarnishing of person's reputation or brand was initially also provided for under the old criminal laws; such as it is provided for under the law of tort, defamation to be precise. However, with the enactment of the Cybercrimes Act, most of those hitherto covered areas are now subsumed under the Act. That Act now regulates those conducts that border on the abuse of the use of computer and technology. The criminal implications of cyber offences in Nigeria are severe. The Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 (amended in 2024) was a landmark piece of legislation that sought to define and penalize various forms of cybercrime. Some key points of the Act include:

1. Offences against critical national information infrastructure: One of the key features of the Act is creation of an offence prohibiting attacks against critical national information infrastructure attacks (for instance an assault on a nation's power grid), which inevitably affects the wellbeing of the nation, individually and collectively. This is as seen in Section 5 of the Cybercrime Act which prescribes different penalties ranging from 10 years without option of fine, and where such attack results in grievous bodily harm, 15 years without the option of fine and to life imprisonment where the offence committed results in death of a person.

2. Penalties for Hacking and Unlawful Access: Section 6 of the Act criminalises unauthorized access to a computer system or network for

the purpose of obtaining data that are vital to national security,[3] or with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information,[4] with the intent to commit an offence under the section, uses any device to avoid detection or otherwise prevent identification or attribution with the act or omission,[5] or knowingly and intentionally traffics in any password or similar information through which a computer may be accessed without lawful authorization and such trafficking affects public, private or individual interest within or outside Nigeria.[6] These offences are punishable with several years imprisonment or fines. The activities of the yahoo, yahoo boys are captured under here.

3. **Fraudulent Emails and Financial Crimes (including 419): the Act specifically targets the infamous "419" scams—advance fee frauds that promise large sums of money in return for small upfront payments. The penalties for this type of fraud are severe, including up to 7 years in prison. As a computer itself may be a victim of cybercrime, Section 8 criminalises unlawful interference with a computer to make it non-functional. It is an offence under Section 9 to intercept electronic message, emails and electronic money transfers, and this offence is punishable with 7 years at first instance and 14 years imprisonment upon second conviction. By section 10 of the Act, tampering unlawfully with critical infrastructure or electronic mail by any person employed under a Local Government, private organisation or financial institution attracts 3 years imprisonment or a fine of ₦2,000,000.00. Critical infrastructure is defined in Section 58 of the Act to mean "systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country."

---

3 See Section 6 (1) of the Cybercrimes Act, 2015.

4 See Section 6(2) of the Cybercrimes Act, 2015.

5 See Section 6(3) of the Cybercrimes Act, 2015.

6 See Section 6(4) of the Cybercrimes Act, 2015.

4. Computer-related forgery**: This is an offence under Section 13 with maximum of 3 years imprisonment or ₦7,000,000.00 fine.

5. Computer-related fraud**: Section 14 of the Act provides for the offence of computer-related fraud. It states in summary that a person who knowingly without authority or in excess of authority causes any loss of property to another, by altering, erasing, inputting, or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits on himself or another person commits an offence and on conviction liable to either a fine of not less than ₦7,000,000.00 (Seven Million Naira) or not less than a 3 year prison term or both.

Under Section 14(2), anyone who with an intent to defraud sends an electronic message upon which reliance is made, thereby causing the recipient or another person to suffer any damage or loss commits an offence and is liable upon conviction to either a fine of ₦10,000,000.00 or not less than a 5-year term or both. The above provision is highly welcome and it is hoped that its enforcement will drastically reduce the incidence of Online Advanced Fee Fraud also known in Nigeria as 419 or *'yahoo yahoo'*.

As fraud committed on bank accounts are often done in connivance with bank officials and employees, Section 14 seeks to deter this and hence in subsection (4) makes it an offence for anyone employed in the Public or Private sector who, with intent to defraud, manipulates a computer or other electronic payment devices with the intent to short pay or overpay or actually short pays or overpays any employee of the public or private sector, and is liable to imprisonment for a term of not more than 7 years and forfeiture of the proprietary interest in the stolen money or property to the bank, financial institution or the customer. Where an offence above results in material or financial loss to the bank,

financial institution or customer, in addition to 7 years imprisonment, the offender shall be liable to refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer by virtue of subsection (6) of Section 14. Furthermore, Section 14(7) provides that an employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using computer systems or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

6. ***Theft of electronic devices**:*** Other offences created by the Act include theft of electronic devices like Automated Teller Machines[7] and by this provision a person who steals a financial institution or Public Infrastructure Terminal is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 or both. Stealing an Automated Teller Machine (ATM) attracts imprisonment for a term of not more than 7 years or a fine of not more than =N10,000,000,00 or both and all proceeds of such theft shall be forfeited to the lawful owners of the ATM. In the same vein, mere attempt to steal an ATM constitutes an offence attracting a term of not more than 1 year or a fine of not more than ₦1,000,000.00 or both.

7. Unauthorised modifications of computer systems**: Section 16 of the Act prohibits unauthorized modifications of computer systems, networks data and system interference with punishment of of not more than 3 years or a fine of not more than ₦ 7,000,000.00 or both.

8. Cyber terrorism: Accessing a computer for the purpose of cyber-terrorism which is also an offence under Terrorism (Prevention) Act,

[7] Section 15

2011[8]. Thus, a person who accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.

9. Identity theft and impersonation**: This is an offence quite common these days. We receive regular calls from some persons who have hacked the whatsapp accounts of others and thereby making calls with the number of such a person ostensibly as a member of a common group notifying of a whatsapp group meeting fixed for a time of the day. Such a caller would require his intended victim to call out a code sent to him so as to be able to participate in the meeting. Where the intended victim believes that he has received a call for a reputable member of the group and calls out the code, his identity has been stolen and from that moment, the fraudster will start using the victim's number to solicit financial assistance from unsuspecting members of the public.

To this end, Section 22 of the Act makes it an offence for a person who is engaged in the services of any public or private organisation and, as a result of his special knowledge, commits identity theft of its employer, staff, service providers and consultants with the intent to defraud . The punishment is imprisonment for a term of 7 years or a fine of ₦5,000,000.00 or both.

Equally, under the same Section 22, fraudulently or dishonestly using the electronic signature, password or any other unique identification feature of any other person or to fraudulently impersonate another entity or person, living or dead, with intent to gain advantage for himself or another person, or obtain any property or an interest in any property, or cause disadvantage to the entity or person being impersonated or another person, or avoid arrest or prosecution or to

[8] Section 18

obstruct, pervert or defeat the course of justice, constitutes an offence with imprisonment of a term of 5 years or a fine of not more than ₦7,000,000.00 or both.

***10. Child pornography and related offences**:* producing, distributing, making avalaible, procuring child pornography through the use of computer system constitutes an offence under Section 23 and the penalties range from 1 to 15 years imprisonment or fine ranging from ₦250,000.00 to ₦25,000,000. Also in this category is intentionally proposing, grooming or soliciting to meet a child through the use of a computer system for sexual activities.

11. **Cyberstalking and Cyberbullying: These offenses may involve harassment or intimidation through electronic means either by posting pornographic materials of a person, or disseminating information about him which one knows to be false for the purpose of causing breakdown of law and order, knowingly or intentionally transmitting or causing the transmission of any communication through a computer system or network to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm to another person. The offence may also be made of such communication containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value, or where such communication contains any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association, or corporation, any money or other thing of value. By Section 12, all these acts are punishable under the Act with punishments ranging from 3 years or 5 years to 10 years imprisonment or ₦10,000,000 to ₦15,000,000 to ₦25,000,000., The above demonstrates the

government's commitment to protecting individuals from digital abuse as we have seen many cases of cyber criminals threatening to expose someone's sex records for financial extortion. A ready example is that of Tiwa Savage that occurred a few years ago and the best way to respond to such a threat is to report to the police and refuse to bargain with the criminals.

12. Cybersquatting which involves intentionally taking or making use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Government in Nigeria, on the internet or any other computer network, without authority or right, and for the purpose of interfering with their use by the owner, registrant or legitimate prior user. This offence attracts imprisonment for a term of not more than 2 years or a fine of not more than ₦5,000,000.00 or both.

13. Phishing, spamming and spreading of computer viruses constitute an offence under Section 32 of the Act the punishments for which are 3 years imprisonment or ₦1,000,000.00 or both.

Electronic cards related fraud**: Section 33 of the Act criminalises using, with intent to defraud, any access device including credit, debit, charge, loyalty and other types of financial cards, to obtain cash, credit, goods or service. The punishment is imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 or to both fine and imprisonment and is further liable to pay, in monetary terms, the value of loss sustained by the owner of the credit card.

14. **Data Privacy Violations:** Unauthorized access to personal data, including selling or sharing such data without consent, is a criminal offense. As more Nigerians engage in e-commerce and online

transactions, protecting personal data has become increasingly critical. There is also the Data Protection Act that addresses certain breaches as it relates to protection of private data.

However, while the legislation is robust, enforcement remains a challenge. Cybercriminals are often elusive, operating across multiple jurisdictions, making it difficult for law enforcement officers to track and prosecute them. This is an area where international cooperation and capacity building within our law enforcement agencies are critical, as we shall adumbrate later. It is not, as of recent, that some measure of cybercrimes prevention capacity is being built. Up till some few years back, the capacity was largely lacking to solve some of the reported crimes. The plague currently is, however, that of tools, that is instruments to carry out the job. Only few tracking equipment still exist in the country while other germane ones are lacking. It is through international cooperation that we have so far succeeded in taming some of the cybercrimes. As at date, the Interpol, cybercrimes unit of the police, the EFCC, and a unit in the NSA office deal with cybercrimes.

Above are just a few provisions of the Act which really show that there are criminal implications for digital stratosphere activities. The long arm of the law can reach into and beyond the clouds, and criminals may not be said to have a safe haven as the myth or fantasies of statelessness exulted in by some individuals at the dawn internet disruption of human activities have been burst.

Civil Implications of Cyber Offences

Beyond criminal penalties attached to some of the misconducts, cyber offences also have significant civil implications. Victims of cybercrimes can seek redress through civil litigation, where they can claim damages for losses suffered due to cyber attacks. Broadly, the civil liabilities fall into two categories. The contractual liability stemming from the breach of the contractual relationship between the service

provider/vendor such as the banks and clients and the victim of the offense; and the tort liability that is a familiar area, which involves injuring another person or entity through negligence, default, non-compliance with the regulations, guidelines or provision in a law. At times, it is committed by the offender through the disparaging of a persons' reputation, particularly where there is invasion of the person's privacy. It may also include assault on a property. The civil implications include the followings:

*1. **Financial losses and restitution:***

Ordinarily, victims of cybercrimes can sue for recovery of stolen funds or compensation for financial losses incurred as a result of fraud or identity theft. This is usually the case in the matters involving financial institutions and money kept therein. The question of protective clause or exemption used to be a major challenge in this regard as most financial institutions might have inserted clauses in account-opening forms protecting or limiting their liabilities. However, in this regard, it can be argued that the law has changed and the digital stratosphere have provided better opportunities as the Act has provided some liability to assist in recovering or refunding certain funds lost as a result of the operations of fraudsters using the financial institutions services.

By Section 19 of the Act, financial institutions shall, as a duty to their customers, put in place effective counter-fraud measures to safeguard their sensitive information although where a security breach occurs, the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity. Where, however, it can be shown that the financial institution or its employee failed to observe necessary precautions, the employee may be made liable to make good the losses of the customer. It is doubtful if the financial institution cannot be

vicariously liable where the employee is unable to refund the amount involved.

An example of this is under Section 27 of the Act dealing with attempts, conspiracy, aiding and abetting of a cybercrime. Thus, an employee of any public or private organisation found to have connived with another person or group of persons to perpetrate fraud using a computer system or network, aside from the criminal liability is under obligation to ***in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer***.

Victims of electronic cards related frauds are specially protected by the Cybercrimes Act. Section 33 of the Act provides for many instances where a victim of electronic card fraud is entitled to payment in monetary terms, the value of loss sustained by him. The same civil remedy is applicable under Sections 34 and 35 with respect to dealing in, sale or purchase of the card of another person. The victim is entitled to monetary compensation up to the value of the loss or the assets or goods acquired with the funds.

A civil remedy provided under Section 36 of the Act is where a person fraudulently re-directs funds transfer instructions during transmissions over any authorised communications path or device and re-directs funds transferred electronically with an authorized account. Aside from the criminal implication of 3 years imprisonment or a fine of N1,000,000.00, the cardholder victim is entitled to receive in monetary terms, the value of loss sustained or forfeiture of the assets or goods acquired with the funds from the account of the cardholder.

It is no longer business as usual for financial institutions to make fraudulent debits on customers' accounts. By section 37(3) of the Act, a financial institution that makes an unauthorised debit on a customer's

account shall, upon written notification by the customer, provide clear legal authorisation for such debit to the customer or reverse such debit within 72 hours, and any financial institution that fails to reverse such debit within 72 hours, commits an offence and is liable on conviction to restitution of the debit and a fine of ₦5,000,000.00.

However, a critical provision in this regard is Section 40 of the Act which provides for obligations on service providers to, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards (a) the identification, apprehension and prosecution of offenders; (b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or (c) the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence. Where proceeds are retrieved, such may be turned over to the victim. This is a civil compensation not otherwise available before the promulgation of the Cybercrimes Act, 2015 and the Administration of Criminal Justice Act, 2015. I must also add that contrary to popular belief that a court order is required before the service provider can provide the assistance to the law enforcement agency, section 40 of the Act does not state obtaining a court order as a precondition for the assistance. Another point noteworthy is that even in the absence of a request from the law enforcement agency, the service provider can, on its own volition, provide the assistance. Did I hear privacy concern?

By subsections (3) and (4) of Section 40 of the Act, a service provider who contravenes the provisions of subsections (1) and (2) of this section commits an offence and is liable on conviction to a fine of not more than ₦10,000,000.00 while each director, manager or officer of the

service provider is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both.

Another and very important provision guaranteeing civil remedy for victims of cyber fraud is Section 49 of the Act which provides the general powers of the court to order restitution or compensation for a victim of fraud. It provides that in addition to any other penalty prescribed under this Act, the Court shall order a person convicted of an offence under this Act to make restitution to the victim of the false pretense or fraud by directing the person, where the property involved is money, to pay to the victim an amount equivalent to the loss sustained by the victim and in any other case to (a) a return the property to the victim or to a person designated by him; or (b) pay an amount equal to the value of the property, where the return of the property is impossible or impracticable. It also provides that an order of restitution may be enforced by the victim or by the prosecutor on behalf of the victim in the same manner as a judgment in a civil action. It is definitely agreeable that cybercrimes may have civil implications in our digital stratosphere.

2. **Contractual Disputes:

In the digital age, many transactions are conducted online, and disputes arising from breaches of contract, such as failure to deliver goods or services purchased online, can lead to civil suits. Generally speaking, service providers hardly have liability in the case of breach of protocols. Where hacked, their liability will be at best to the co-contractor and not the user. Insurance comes in here by the companies to mitigate loss.

The modern transactions of online activities may require a proof or authorship of a document originating or evidencing a transaction. Electronic signatures then come in to avoid the delay in passing

documents from distant jurisdictions to another for the purpose of execution and disputes may arise with respect to whether such electronic signatures are binding. Section 17(1) and (2) of the Cybercrimes Act provides for bindingness of such signatures although with the exception of some particular transactions as contained in Section 17(4) of the Act. Thus, according to the Act, “Electronic signature in respect of purchases of goods, and any other transactions shall be binding” and “Whenever the genuineness or otherwise of such signature is in question, the burden of proof, that the signature does not belong to the purported originator of such electronic signature shall be on the contender.”

In Section 17(4) as stated above, contractual transactions or declarations that are excluded from electronic signature except where they are legally verified in "Certified True Copies" include a creation and execution of wills, codicils and other testamentary documents; death certificate; birth certificate; matters of family law such as marriage, divorce, adoption and other related issues; issuance of court orders, notices, official court documents such as affidavits, pleadings, motions and other related judicial documents and instruments; a cancellation or termination of utility services; an instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; and any document ordering withdrawal of drugs, chemicals and any other material either on the ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.

3. Intellectual property, defamation and privacy infringements

In cases of cyberstalking or online harassment, traditionally under the law of Torts, victims can seek damages for defamation or breaches of privacy. The Act has not made monetary compensation intervention in this regard probably because such damage can be remedied through an

action in court. However, the Act has made some civil implications with respect to activities that take place in the digital stratosphere.

The only remedies provided by the Act in relation to cyberstalking is contained in Section 24(3) of the Act which provides that a court sentencing offender under subsections (1) and (2) thereof may also make an order, which may, for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which- (a) amounts to harassment; or (b) will cause fear of violence, death or bodily harm, prohibit the defendant from doing anything described specified in the order. By sub-section (6), the court may also make an interim order, for the protection of victims from further exposure to the alleged offences.

With respect to the use of another person's name, business name, trademark, domain name or other word or phrase registered, owned or in use which is captured under the term *cybersquatting* under Section 25, a civil remedy provided is for the court to make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner. The Act does not provide for damages. This is understandable as the traditional intellectual property statutes like the Copyrights Act, Trademarks Act have made sufficient provisions with respect to that.

In defamation cases, however, unlike in conventional publications where ordinarily the newspapers are presumed to have seen the contents, and culpable, same cannot be said of online defamatory publications and proof in this regard may throw up some challenges to actually make the platforms where publications are made to be primarily liable. This is so because, the digital platforms are not in control of the content that passes through their systems except where it can be established that they enabled it. E.g. Whatsapp reporting, Trump example, Buhari example. Report mode is provided in most

instances. In most cases, encrypted messages are what pass through their systems, in which effect, the service providers lack the requisite capacity, legally and technically to know the content.

However, the civil route also has its challenges. Litigation can be expensive and time-consuming, and often the perpetrators are anonymous or located in foreign jurisdictions, making it difficult to enforce civil judgments.

JURISDICTION

It is trite to say that jurisdiction is the live wire of adjudication as a court cannot intervene in a matter in which it has no jurisdiction. Anything done in the absence of jurisdiction is a nullity.[9] Thus. In criminal prosecution, a court without jurisdiction has only laboured in vain.

As observed by Femi Daniel,[10]

> "Jurisdiction in cyberspace is as interesting as it is intriguing. The first challenge prosecutors face is the issue of location. Unlike traditional crimes, a cybercrime could be conceptualized in one country, committed in another and the victim is reeling in pains in yet another country, all within minutes. Containing the menace is even becoming more challenging as different anonymiser devices are being deployed by technological savvy operators to further cloak identity in cyberspace."

The key questions in cybercrimes are what is the relevant "event" and where does it occur? What is it that constitutes the essence of these

[9] Ukwu v. Bunge [1997] 8 NWLR (Pt. 578) Pg. 527, Jeric Nig. Ltd v. Union Bank of Nig. Plc. (2000) 12 SC (Pt. 2) 133; AG Lagos State v. Dosunmu [1998] 3 NWLR (Pt. 111) Pg. 552, Nonye v. Anyichie [2005] 2 NWLR (Pt. 910) Pg. 623.

[10] Introduction to Computer Law in Nigeria, 2015, page 194.

crimes? Is it what is done? Or the effects of what is done? And where is the crime committed? Is it the location where the conduct was initiated? The nationality of the offender, or the location where the effect was felt? Is it committed in two or all of those places?"[11]

These are major issues that determine the jurisdiction of a country and that of the court to assume jurisdiction in a cybercrime case. Further questions that rear their heads are, which country's law are you applying? How is testimony to be taken? Inspection of instruments method to be adopted, where are they located? Issues of access to them? Which one is admissible - original or photocopy version of electronic evidence? etc. Unlike in the conventional crimes where the scene of crime can easily be determined, it is amorphous in the space or stratosphere. Which rules of evidence applies? For example, in Nigeria, we are all conversant with Section 84 of the Evidence Act that has displaced the ordinary rules of admissibility of evidence.

A country's jurisdiction is often constrained by physical boundaries. Its concern is to detect and prosecute crimes that occur within the area of sovereignty. As it is known, the rules of jurisdiction differ from one country to another. There is no universal rule of jurisdiction. As stated above, perpetration of cybercrimes is often across several countries, hence the question of which country has jurisdiction? In some instances, the affected country lacks jurisdiction as the act may not constitute an offence while that which possesses jurisdiction is unwilling to assume it for one reason or the other, probably because it is her citizen. This is where the issue of territoriality is equally challenged.

Due to the challenges associated with jurisdiction, judicial and enforcement officers are constantly at a quagmire over ways and means of enforcing the law. In some cases, point of origin and destination of

[11] See Kim Soukieh, Cybercrimes - The Shifting Doctrine of Jurisdiction 2011) 10 CAN. L.R. 221 @ 226.

crimes differ, and numerous territories are often passed. In DPP V SUTCLIFFE,[12] the Victoria Supreme Court in Australia held the applicable provision to have extra-territorial effect in so far as the substantial part took place within the area. In GUTNICK V. DOW JONES & CO (2002) HCA F6, the High Court of Australia held that the defamatory material was published on the internet, but the relevant tort was committed where the material was downloaded from the server and read, and not where it was uploaded. See also the case of Daily Times Nig Plc v. Arum.[13]

In USA V ANDREW AVERNHEIMER, UNITED STATES COURT OF APPEAL FOR THE THIRD CIRCUIT, APRIL 11, 2014, upheld the 'doctrine of essential element', which means that jurisdiction is vested in a country where the material ingredients took place. Example is where the issue occurred in Australia or the perpetrator is an Australia citizen. Even where there has to be transfer, several challenges that we shall shortly discuss arise, for instance, the issue of dual criminality.

In the context of cybercrimes, the typology of jurisdiction are three. According to Susan Brenner & Bart-Jamp Koors, there are 3 types of jurisdiction which are:

a. prescriptive jurisdiction, jurisdiction to prescribe: a state's authority to make its own law applicable to activities, relations, or persons by enacting legislation, administration rule, executive order or the determination of a court;
b. jurisdiction to adjudicate: a state's authority "to subject persons or the entities to the process of its courts or administrative tribunals for the purposes of determining whether prescriptive law has been violated;

[12] (2001) VSC 243.
[13] [2023] 17 NWLR (Part 1914), P. 559

c. jurisdiction to enforce: a state's authority to compel compliance or to penalize non-compliance with its laws or regulations".[14]

Countries have to lower the threshold of sovereignty for jurisdiction over cybercrimes. In the light of the above, territorial jurisdiction which enables the state to only punish within her territory where the object occurred becomes a challenge. Challenges to exercise of countries' jurisdiction on crimes not committed within their territories came up in the 1927 *Lotus Case*. In that case, A collision occurred on the high seas between a French vessel – Lotus – and a Turkish vessel – Boz-Kourt. The Boz-Kourt sank and killed eight Turkish nationals on board the Turkish vessel. The 10 survivors of the Boz-Kourt (including its captain) were taken to Turkey on board the Lotus. In Turkey, the officer on watch of the Lotus (Demons), and the captain of the Turkish ship were charged with manslaughter. Demons, a French national, was sentenced to 80 days of imprisonment and a fine. The French government protested, demanding the release of Demons or the transfer of his case to the French Courts. Turkey and France agreed to refer this dispute on the jurisdiction to the Permanent Court of International Justice (PCIJ).

The questions posed to the Court was whether Turkey violated international law when Turkish courts exercised jurisdiction over a crime committed by a French national, outside Turkey? If yes, should Turkey pay compensation to France? The Court answered this in the negative to the effect that Turkey, by instituting criminal proceedings against Demons, did not violate international law.

Another case is *USA v. Fawaz Uniz*[15] where Yunis (Defendant) argued that the Government (Plaintiff) could not prosecute him for a hijacking that he perpetrated when its only connection to the United States was

[14] "Approaches Cybercrime Jurisdiction (2003) 4 (1) Journal of High Technology Law, p. 3.
[15] 681 F. Supp. 896 (D.D.C. 1988) February 12, 1988

that several Americans were on board the plane. The US Court held that the federal government may prosecute an airline hijacker even if the hijacking's only connection with the United States was the presence of Americans on board the plane.

However, the further challenges of jurisdiction vis-a-vis cybercrimes, according to Souikeh[16], include the issue of dual criminality wherein the tension between one country's desire to enforce its laws and another country's determination to preserve its legal sovereignty. Where a particular country does not have a legislation on such crime that the other country wants to seek extradition on, it becomes impossible as one of the principles of extradition is that the act over which extradition request is made must constitute an extraditable offence for extradition to be granted. This is a frustrating element on its own.

However, it is pleasant to observe that under the Nigerian jurisdiction, all the offences created in the Act are extraditable offences by virtue of Section 51 of the Act. This is a strong provision guaranteeing and extending cooperation to other countries of the world. It is expected that this provision shall be contained in the laws of other countries so as to guarantee mutual cooperation and assistance.

Also, as I remarked earlier, by tradition where extradition of the offender is to be done, primarily there must be a treaty. In the absence of a treaty or legal framework between the countries, extradition is impaired. There are no international instrument governing cybercrimes globally except some regional conventions such as the Budapest Convention otherwise known as the European Convention of 2001 which came into force in 2004 with non-member states such as America, Japan, Australia, Dominican Republic etc. signing it. Most of the countries that are signatories have subsequently harmonized their

[16] Supra

domestic or municipal laws along the Convention, though some uncomfortable with some provisions like retention of data for two years. The European Convention covers illegal access and interception; data and system interference; misuse of devices; computer-related forgery and fraud, offences related to child pornography; copyright infringement and attempting, aiding and abetting.

By articles 23-35 of the European Convention, enforcement procedure is to be by way of extradition, mutual assistance, spontaneous information, mutual assistance without international agreement, confidentiality, storage, disclosure, transborder access for computer and internet traffic data, mutual assistance for real time collection and interception of internet traffic data, and the provision of a 24/7 network.

There is also the African Union Convention on Cyber Security and Personal Data Protection adopted by African countries in June 2014, which entered into force on 8 June 2023, originally signed by 19 countries, ratified by 15. Treaty of mutual assistance is another tool that has been deployed. Finally, universality of jurisdiction is the ultimate goal. This enables any country where the offender is present to exercise jurisdiction over him. To resolve further the issue of jurisdiction, the tension between jurisdiction and sovereignty needs to be minimized or rethought so as to enable actualization of remedies.

Along this line, Nigeria has taken proactive steps which are quite commendable. By Section 52 of the Cybercrimes Act, the Attorney-General of the Federation is empowered to request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under the Act. He may as well authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under the Act. Such joint investigation or

cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreement exists between Nigeria and the requested or requesting country. The Attorney-General of the Federation may, as well, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under this Act.

Nigerian Court's Jurisdiction on Cybercrimes

Section 50 provides for jurisdiction and international co-operation, stating that the Federal High Court located in any part of Nigeria regardless of the location where the offence is committed shall have jurisdiction to try offences under this Act if the offence is committed in Nigeria[17], by a resident or citizen of Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed[18], in a ship or aircraft registered in Nigeria[19], or if the offence is committed outside Nigeria where the victim of the offence is a citizen or resident of Nigeria[20] and if the alleged offender is in Nigeria and has not been extradited to another country for prosecution. In addition the Court shall give all matters brought before it by the Council accelerated hearing. Furthermore subject to the Constitution of the Federal Republic of Nigeria, an application for stay of proceedings in respect of all criminal matters brought under this Act shall not be entertained until judgment is delivered. Section 50 gives the Federal High Court jurisdiction when the crime is committed in Nigeria but also where it is not committed in the country, in instances where the victim is a Nigerian citizen/resident or the offender is in Nigeria and is not extradited to any country.

---

17 Section 50(1) (a)

18 Section 50(1)(c)

19 Section 50(1)(b)

20 Section 50(1) (d)

Tackling the Menace of Cybercrime

So, how do we tackle the menace of cybercrime in Nigeria? The solution requires a multi-faceted approach involving government, the private sector, the civil society, and individuals. Through the international collaboration of countries and service providers, some motion or traction can be achieved. To engender confidence in the adoption of technology, there is a need for setting up national/international fund by all the stakeholders that are economically benefitting from the use, so that in instances where offenders could not be tracked, victims can be compensated from the fund. Although, by Section 44 of the Nigerian Act, as amended by Section 11 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2024, a National Cyber Security Fund has been created in Nigeria and domiciled in the Central Bank of Nigeria into which shall be credited a levy of 0.5% (0.005) equivalent to a half percent of all electronic transactions value by the business specified in the Second Schedule to the Act, the purpose of the Fund is not stated to include compensating of victims of cybercrimes where the offender could not be tracked, and the implementation has however been suspended.

Keeping pace with technology ahead of the criminals is another effort that can be made. Users of internet services cannot afford to be behind the advancement in technology in terms of stalling the nefarious activities of the criminals.

Strengthening Legislation and Enforcement: While the Cybercrimes Act of 2015, as amended, is a good start, we need to continually update our laws to keep pace with evolving cyber threats. Some amendments effected in 2024 have given a better bite. More importantly, we need

to build the capacity of our law enforcement agencies to investigate and prosecute cybercrimes effectively. This includes investing in cyber forensics, training, and international collaboration. The importance of international collaboration cannot be over-emphasized too.

Public Awareness and Education: One of the most effective ways to combat cybercrime is through public education. People need to be aware of the risks of sharing personal information online, recognize phishing attempts, and understand the dangers of downloading unknown software. Schools, universities, and workplaces should incorporate cyber hygiene education into their curricula.

Private Sector Involvement: The private sector, particularly tech companies and financial institutions, has a crucial role to play. They can invest in stronger cybersecurity measures, share intelligence on emerging threats, and collaborate with the government on initiatives to combat cybercrime. The banking sector, for example, has made significant strides in reducing fraud through the use of biometric verification and other security measures. Cloning however has emerged, and there must be effort at curtailing this also.

International Cooperation: Cybercrime is a global issue, and tackling it requires international cooperation. Nigeria should continue to work with organizations like INTERPOL, the United Nations, and foreign governments to track and apprehend cybercriminals operating across borders. Extradition agreements and joint task forces can be instrumental in bringing perpetrators to justice.

Supporting Victims: Finally, we must not forget the victims of cybercrime. Whether they are individuals who have lost their life savings or businesses that have been crippled by cyber attacks, victims need support. This includes legal assistance, psychological counseling, and mechanisms for recovering stolen funds.

CONCLUSION.

In conclusion, cyber offences present a significant threat to Nigeria's economy, security, and international reputation. However, by understanding the nature of these crimes, their criminal and civil implications, and by implementing a comprehensive strategy to combat them, we can protect our nation and its citizens from the dangers of the digital age.

The fight against cybercrime is not one that can be won overnight. It requires vigilance, cooperation, and a commitment to justice. However, I believe that with the right approach, Nigeria can not only tackle the menace of cybercrime but also become a leader in cybersecurity in Africa. Essentially, therefore, judicial officers' capacity needs to be enhanced for effective interpretation of cyber laws; education of users generally; strengthening of the legislation; cooperation amongst states; financial institutions and other corporate entities must also enhance their capacities regularly in terms of cybersecurity; development of binding international agreement etc. must be embraced.

Thank you for your attention, and I look forward to your questions and contributions as we continue this important conversation. Together, we can build a safer, more secure digital future for Nigeria.
