A COMPERATIVE ANALYSIS OF THE LEGAL FRAMEWORK ON CYBERCRIME PREVENTION IN NIGERIA WITH UNITED STATES OF AMERICA, CANADA AND EGYPT*

Abstract

The introduction to computers and other digital contrivance to the modern world has simplified many hitherto, laborious activities. Over the years, Nigeria and Nigerians have been constantly fingered as the main actors in cybercrime activities worldwide. Unfortunately, the situation escalated unabated for a long time partly due to Nigeria's inherent demons: corruption, poverty, lack of effective regulatory framework, etc. The Cybercrimes (Prohibition, Prevention, etc) Act of 2015 was enacted and infused with copious provisions all aimed at combating the alarming incidence of cybercrime in Nigeria. In February 2024, the National assembly enacted the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024 to improve and enhance the provision of the Cybercrimes (Prohibition, Prevention, etc) Act of 2015. Notwithstanding the amendment however, the Act is still deficient in certain material respect, which could hamper its effective implementation. Therefore, this study is an appraisal of the legal frameworks for cybercrime prevention. This research work adopted doctrinal research method in its quest to appraise the provisions of the Cybercrime Act in order to determine its efficacy in tackling cybercrime in Nigeria. It was found, among other things, that as laudable as the provisions of the Cybercrime Act are, the Act is, however, still silent on some key issues, which are paramount to its enforcement. These challenges include the absence of the definition of cybercrime, conflict with other substantive laws, and lack of vibrant coordinating body for the enforcement of the Cybercrime Act etc. It was therefore, recommended that the Act just like in the USA and Canada be brought in harmony with the provisions of the conflicting statutes, and that Nigeria should accede to international treaties on the prevention of cybercrime thereby, encouraging entrepreneurship practice among Nigerian youths.

Keywords: Cybercrime, Cyberspace, Information Communications Technology, E-transactions, E-Business.

1. Introduction:

Information technology has enhanced several aspects of human life and has made virtually everything easier. It provides wider knowledge and can help in gaining and accessing information.[1]ICT has become an integral part of everyday life for many people.

* **Charity Chinedu-Uhuo**, Lecturer, Alex Ekwueme Federal University, Ndufu-Alike, Ebonyi State, Nigeria. P.O. Box 1397, Abakaliki, Ebonyi State, Nigeria.Email:charityuhuo2@gmail.com; +2437033543039; ****Paschal Oguguo Olebara**, Lecturer, Faculty of Law, Alex Ekwueme Federal University, Ndufu-Alike, Ebonyi State, Nigeria. P.O. Box 1397, Abakaliki, Ebonyi State, Nigeria; Email: olebarapaschal@gmail.com;Phone: +2348108243088.

However, the cyber world has no definite territorial boundaries. The world has become a global village and at just a simple click, one is already in another territorial jurisdiction with little or no restraint whatsoever.[2] We are all connected by an invisible thread. The digital age has transformed the way people communicate, network, seek help, access information and learn. Be it the service industry, banks, universities, airlines, medical industry and other business establishments and certainly our own homes, the remarkable influence of information technology (IT) is evident.[3] But it comes with a price, which is the use of the internet for perpetuation of various forms of cybercrimes.

Cybercrime encompasses criminal acts that involve computers and networks. Thus, cybercrime is a broad term that describes everything from electronic hacking to denial-of-service attacks that cause E-business websites to lose money. Cybercrimes are essentially criminal activities where computers, network or electronic information technology devices are the source, tool, target or place of crime. They are carried out by way of illegal access into another's data base, illegal interception, data interference, system interference, misuse of devices, forgery and electronic scams.[4]

The rapid growth of computer technology carries with it the evolution of various crimes on the internet. In recent years, there has been considerable focus within the criminal justice system on computer-related crime, as cybercrime has garnered increased attention because computers have become so central to several areas of social activity connected to everyday life. Internet users innovate freely on various platforms, reaching out to more people, aiding ubiquity of internet features and with attendant high utility and pecuniary returns. Thus, the internet has been a double-edged sword providing opportunities for individuals and organizations and, alongside, engendering an increased information security risk. This has prompted the Court of Appeal, in *Ekiti State Independent Electoral Commission & Ors. v. PDP & Anor.*,[5] to warn that 'with modern information communication technology, anything is possible. Documents and signatures are easily manipulated to the extent that genuineness of documents can no longer be ascertained by

---

[1] D.R. Johnson and D. Post, 'Law and Borders: The Rise of Law in Cyberspace' [1996] *Stanford Law Review* (48) 1367-1368.

[2] *Ibid*.

[3] O. Oke, 'An Appraisal of the Nigerian Cybercrime (Prohibition, Prevention, Etc.) Act, 2015' available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2655593>, accessed on January 15, 2020 at 3:34pm.

[4] J. Baiden, *Exchange Traded Funds: Sovereign Wealth Funds, Transfer Pricing, and Cyber Crimes* (Bloomington: Xlibris Corp, 2012)117.

[5] (2013) LPELR-46413 (SC), p. 37.

mere observation with the eyes.' In *United States v. Hunter*,[6] the court has observed that computer records are extremely susceptible to tampering, hiding or destruction, whether deliberate or inadvertent. Images can be hidden in all manner of files, even word processing documents and spreadsheets.'

It is apparent that the rise of internet technology has changed the daily activities of people for the better, ranging from education to health care, business to national security, touching nearly every sector. As the internet expands, its vulnerabilities have become glaring. Government agencies, financial institutions, private corporations, critical national infrastructure and the general public have all been victims of cyber attacks. As such, securing and maintaining cyberspace, secure, open and reliable internet is crucial to Nigeria's economy, critical national infrastructure and national security.

2. **Cybercrime and the Nigeria Society.**

Nigeria and Nigerians are no strangers to international controversy, especially with regards to its global notoriety for being involved in drug-trafficking, fraud, cyber-crime and other crime-related activities. Cybercrime offences know no limits to physical geographic boundaries and have continued to create unprecedented issues regarding the feasibility and legitimacy of applying traditional legislation based on geographic boundaries. These offences also come with procedural issues of enforcement of the existing legislation and continue to subject nations with problems unprecedented to its sovereignty and jurisdictions.

In 2015, the Cybercrimes (Prohibition, Prevention, etc) Act was enacted to effectively deal with the issue of cybercrime in Nigeria. However, this Act is still besieged with many loopholes. For instance, the Act does not make provision for the mode of enforcement of its provisions. This creates a huge *lacuna* for the law enforcement agencies that are in charge of the enforcement of its provisions. The Act also fails to take into cognizance some important Act of the National Assembly to ensure conformity with the other Acts which have legislated on some areas covered by the Act. One of such laws is the Evidence Act, 2011. Some of the provisions of the Cybercrime Act are not consistent with the provisions of the Evidence Act such as concerning burden of proof in criminal cases, admissibility of foreign judgements and the use of electronic signature for certain documents. The Act also attempted to regulate the activities of some financial institutions whose activities are already being regulated by the Banks and Other Financial Institutions Act (BOFIA). These shortcomings of the Cybercrimes Act, 2015, which are

[6] (1998) 13 F. Supp. 2d 574.

still not addressed by the Amended Cybercrimes Act, 2024 pose a great challenge in the proper enforcement of the law and the prosecution of cyber offenders. The amendment is a positive step-forward in the Nigerian cyberspace as it incorporates provisions which now ensures the freedom of expression in the country and combating evolving forms of cybercrimes like electronic fraud, data interception and unauthorized system interference.

3. **Critical Analysis of the Provisions of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015**

The Cybercrimes (Prohibition, Prevention, etc) Act, 2015 (hereinafter referred to as 'the Act') is the first legislation enacted in Nigeria which squarely focuses on regulating the conduct of persons in the cyberspace in Nigeria. The Act, which contains 59 sections, 8 parts and two schedules, was passed into law on the 5th of May, 2015.

Section 1 outlines the objectives of the Act as follows:

a. To provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
b. To ensure the protection of critical national information infrastructure; and
c. To promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The Act is applicable throughout Nigeria.[7] This means that no state legislature can validly make any law regulating cybercrime.[8] The Act vests in the President of Nigeria, for the purpose of preserving national security and public interest and based on the recommendation of his National Security Adviser, the power to order the protection of designated computer systems as constituting critical national information infrastructure.[9] This entails prescribing the minimum standards, guidelines, rules and procedures in order to render them tamper-proof to cybercrime. 'Critical infrastructure' has been defined to mean systems and assets, which are so vital to the country that the destruction of such

[7]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Section 2.

[8] This provision reinstates the doctrine of covering the field provided for in section 4(5) of the 1999 Constitution of the Federal Republic of Nigeria (as amended), which provides that where a law enacted by the House of Assembly of a State is inconsistent with any law validly made by the National Assembly, the law made by the National Assembly shall prevail.

[9]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, sections 3 and 4.

systems and assets would immensely impact the national economic security, public health and safety.[10]

3.1 **Offences and Penalties**

Section 5 provides that any person who commits an offence contrary to the provisions regarding critical national information would be liable to a maximum prison sentence of 10 years; and if the act causes bodily harm to any person, the offender shall face a maximum of 15 years imprisonment without the option of fine. Where the act occasions the death of another, then the offender shall be liable to life imprisonment.[11] Section 6 of the Act criminalizes unlawful access to a computer. Hence, any person who, without authorization, intentionally accesses, either wholly or partly, a computer system or network for fraudulent purposes and obtains data therefrom, which are vital to national security commits an offence and is liable to a maximum of 5 years imprisonment or to a maximum fine of ₦5,000,000.00 (Five Million Naira) or both. Where the offender in this case intends to obtain computer data, secure access to a program, commercial or industrial secrets, the punishment is a maximum of 7 years imprisonment or a maximum fine of ₦7,000,000.00 (Seven Million Naira) or both. Section 6(4) protects privately owned computers, whether located within Nigeria or outside, and slams the hacker with a maximum prison sentence of 3 years or a fine of ₦7,000,000.00 (Seven Million Naira).

Section 8 criminalizes the intentional or fraudulent use of a computer system by any person which results in the severe impairment of the normal functioning of the system; the offender shall be liable to a maximum imprisonment for 2 years or to a fine not exceeding ₦5,000,000.00 (Five Million Naira) or both. Similarly, the punishment for unlawfully destroying or aborting any electronic mail or process through which money or vital information is being transmitted is 7 years imprisonment in the first instance and 14 years in the second instance.[12]

With respect to the above section 9, what is the standard of determining what valuable information is? The Act does not define valuable information in its interpretation section. Thus, the task of setting the standard of determining what valuable information entails should be on the part of the sender of the information, thereby making the standard subjective. More so, the reason for the circumscription of this section to only electronic mails where money or valuable information is conveyed is not yet manifest. Where the

[10]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 42.

[11]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 5.

[12]*Ibid*., section 9.

data being tampered with is a critical infrastructure and the offender is a government or private employee assigned to work on same, then the offender is liable to imprisonment for 3 years or a fine of ₦2,000,000.00 (Two Million Naira).[13] This section 10 regulates employment relationships between an employer and employee. However, this regulation is only limited to employees working with any critical information. The rationale behind criminalizing an act of performing a role outside the scope of an employee's contract of service is still unclear. It is submitted that the section should have been modified to provide that the employee must have had an intention to tamper with the critical information.

Where a person unlawfully intercepts and misdirects electronic messages with the intent to fraudulently obtain financial gain therefrom, he is liable to 3 years imprisonment or a fine of ₦1,000,000.00 (One Million Naira) or both.[14] Where the data intercepted also includes electromagnetic or emission signals from a computer, then the penalty is ₦5,000,000.00 (Five Million Naira) or a maximum of 2 years imprisonment or both.[15]Section 12(2) criminalizes the act of any person who by false pretence induces any Local, State or Federal government worker to deliver any electronic message to him which is not specifically meant for him. Section 12(3) criminalizes the act of any Government worker who hides or detains any electronic mail and delivers same to wrongful person. A government or private employee who willfully hoards any message or payment credit card which was delivered to him in error shall be imprisoned for 1 year or fine of ₦250,000.00 (Two Hundred and Fifty Thousand Naira).[16]

Section 13 criminalizes any act of computer-related forgery, which includes willfully accessing any computer or network with the intent to compromise the authenticity of the data contained therein. Section 14 of the Act provides for computer related fraud. Hence, any person employed by or under the authority of any bank or other financial institutions who, with intent to defraud, directly or indirectly, diverts electronic mails commits an offence and shall be liable on conviction to imprisonment.[17] Section 14(4)(b) further provides that any person who commits an offence subject to subsection (4)(a), which results in material and/or financial loss to the bank or financial institution or customer shall in addition to the term of imprisonment refund the stolen money or forfeit any

[13]*Ibid*., section 10.
[14]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 11.
[15]*Ibid*., section 12(1).

[16]*Ibid*., section 12(3).

[17]*Ibid*., section 14(4)(a).

property to which it has been converted to the bank, financial institution or the customer. This provision of remedial compensation for the victims of the crime is a novel introduction under the Nigerian criminal law. Remedial compensation for victims seeks to monetarily compensate the victim for the crime committed against him as if he instituted the suit in a civil action where he is normally entitled to damages or compensation.[18]

3.2 **Electronic Signature**

The Act provides for electronic signature and slams any person convicted of fraudulently forging another person's signature electronically with 7 years imprisonment or the fine of Ten Million Naira or both.[19] All electronic signatures relating to the purchase of goods and other transactions shall be presumed to be binding until the otherwise is proved.[20]The burden of proof in this case shall be on the person disputing the authenticity of the signature.[21] However, the Act failed to state the form which electronic signatures should take i.e. whether as a sign or name or other form of impressions, etc.

The Act, however, stipulates certain transactions which cannot be validated by an electronic signature. These include: birth and death certificates, family law matters (such as marriage, divorce, adoption, etc.), court orders and official documents, any cancellation or termination of utility services, etc.[22] It has been argued that the most plausible reason for the exclusion of these transactions is because they do not involve the purchase of goods, nor do they require the making of profit or monetary gains therefrom; they are basically administrative matters.[23]

The provisions of the above section 17(4) of the Cybercrimes Act is clearly at variance with the provisions of section 93(2) of the Evidence Act, 2011, which states that 'where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.' More so, section 84 of the Evidence Act reinforces this provision by prescribing the procedures for tendering of electronic evidence.

---

[18] U.A. Yusuf and S.S. Yahaya, 'Crime Victims and Criminal Justice Administration in Nigeria' [2014] *Global Journal of Interdisciplinary Social Sciences* (3) (5) 48.

[19]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 17(3).

[20]*Ibid*., section 17(1).

[21]*Ibid*., section 17 (2).

[22]*Ibid*., section 17(4).

[23] C.M. Ogwezzy, 'Cybercrime Perspectives to Electronic Commerce and Signature: Is the Nigerian Cybercrimes Act 2015 Apposite?' in F.E. Eboibi (ed.), *Handbook on Nigerian Cybercrime Law* (Benin City: Justice Jeco Publishers, 2018) 307.

3.3 **Cyber Terrorism**

The Cybercrimes Act made provisions for the offence of terrorism under its section 18. In order to ascertain the meaning of terrorism, the Act adopted the definition as provided in the Terrorism (Prevention) Act, 2011 (as amended) which defines an 'act of terrorism' as any act, which is deliberately done with malice and may seriously harm or damage a country or an international organization. The Amendment to the Act[24]expanded the definition of terrorism to include the act of financing any terrorist group. By virtue of the provisions of the Cybercrimes Act, cyber terrorism is a crime in Nigeria. To that effect, anybody who accesses, either personally or at his instance, any computer or computer system for the intention of carrying out terrorist activities shall, upon conviction, be sentenced to life imprisonment.[25]

3.4 **Child Pornography**

Section 23(1) of the Act forbids child pornography and other perverted acts. Hence, it is a crime for a person to be involved in the production, marketing, distribution, procurement (for oneself or for another), possession in a computer system or storage medium, of child pornography.[26] The sending of unsolicited pornographic images to another computer is also an offence under the Act.[27]Section 23(3) criminalizes the act of using any computer system[28] or network[29] to communicate and eventually meeting a child and engaging in sexual relations with the child. The definition of computer system in the definition section is wide enough to cover portable handset and other communication devices. Section 23(5) defines a child as a person below the age of 18 years.

3.5 **Cyberstalking**

Section 24 of the Act covers cyberstalking. It is a crime for a person to intentionally send a grossly offensive, obscene, menacing or false message with the intent to annoy, bully, threaten, harass, endanger, inconvenience, insult, intimidate, or cause unjustifiable anxiety to, another person.[30] Section 24(3) of the Act empowers the court to make any order necessary for the prevention of any act of further harassment on the targeted victim, such as a restraining order. The order may last for a stipulated period and the defendant may apply to the court to vary or discharge the order.[31] The court can also make an

[24] Amended by the 'Terrorism (Prevention) (Amendment) Act, 2013'.
[25]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 18(1).
[26]*Ibid*., section 23(1).
[27]*Ibid*., section 23(2).
[28] Computer system includes cellphones, laptops, tablets, etc.
[29] This includes social networks such Facebook, Twitter, Instagram, Whatsapp, Tinder, etc.
[30]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 24 (1) & (2).
[31]*Ibid*., section 24 (5).

interim order for the protection of victims from further exposure to the alleged offences.[32] This is a commendable provision of the Act, because it provides not only for the punishment of the offender but also the protection of the victim of the offence from further acts of cyberstalking from the offender.

3.6 **Cybersquatting.**

Cybersquatting refers to the acquisition of a trademarked domain name over the internet in bad faith in order to mislead, profit, destroy reputation, and deprive others from registering the same, and subsequently offering it for sale to the trademarked owners with the intent of making profit.[33]Section 25(1) provides that any person who intentionally takes or makes use of any name, business name registered and owned by any individual or government without authority or right commits an offence. In awarding a penalty against the offender, the court is to consider the refusal by the offender, upon formal request by the rightful owners, to relinquish the domain name and an attempt by the offender to obtain compensation in any form for the release to the rightful owners for use of the name.[34] The court may order that the offender relinquish such registered name, mark, trademark, domain name or other word or phrase to the rightful owner. The essence of this provision is to extend the protection of intellectual property from the physical to the virtual sphere and it is a commendable one.[35]

3.7 **Hate Speech**

Section 26 criminalizes the use of any computer system or network medium to promote and incite racism and xenophobia. Thus, it is a crime to publicly insult or threaten, through a computer system or network, another person or persons for the reason of their belonging to a different race, colour, religion, nationality, ethnicity, descent, etc. This also includes the distribution of materials containing such sentiments or which justifies acts constituting genocide or crimes against humanity. The punishment for this offence is a maximum punishment of 5 years or a maximum fine of Ten Million Naira or both. In the case of *Okedara v. Attorney-General of the Federation*,[36] the applicant sought a declaration nullifying the provisions of section 24 of the Cybercrimes Act because it violated the freedom of expression guaranteed under the Constitution. The Federal High Court dismissed the suit on the ground that the said provision did not conflict with the

[32]*Ibid*., section 24 (6).
[33]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 58.
[34]*Ibid*., section 25 (2).
[35]*Ibid*., section 25 (3).
[36] (Unreported) Suit No. FHC/L/CS/937/17.

Constitution as the latter provides, under its section 45, for instances where the right to freedom of expression may be derogated from.

By virtue of section 27, any person who attempts to commit an offence under the Act or aids and abets another in committing an offence shall be liable for the same punishment as the principal offender. Additionally, any employee of a financial institution who is found to have connived with another person to perpetuate fraud shall be liable to seven years imprisonment and to return the stolen money to the financial institution or the customer, as the case may be. Section 28 of the Act criminalizes the unlawful production, supply, adaptation, manipulation, procurement, importation, exportation, sale or distribution of e-tools. E-tools include any device, including computer program or component, access code or similar data which is designed or adapted for the purpose of committing an offence under the Act.

3.8 **Manipulation of ATM/POS Terminals**

Section 30 of the Act criminalizes the act of a person manipulating an ATM machine or point of sale (POS) terminals. Section 31 orders every employee to relinquish to his employer all codes or access rights upon the cessation of his employment. The refusal of the former employee to do so shall be construed to be that he intends to hold such employer to ransom and such employee would, therefore, be liable for an offence. This provision is, however, without prejudice to any contractual agreement between the employer and the employee.

Section 32 provides for the offence of phishing, spamming and also malicious spread of computer virus. Phishing is defined in section 58 as the criminal and fraudulent process of attempting to acquire sensitive information such as usernames and password, etc. by disguising as a legitimate entity in an electronic communication such as via e-mails or text messages. Spamming, on the hand, means an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations.

3.9 **Administration and Enforcement**

Section 41(1) of the Act proclaims the Office of the National Security Adviser as the coordinating body for all security and enforcement agencies under the Act. It imposes several duties on the body, among which is to provide all relevant security and intelligence for combating cybercrimes in Nigeria. It also mandates the office to establish and maintain a National Computer Emergency Response Team (CERT) and the National Computer Forensic Laboratory. It also mandates the Office of the National Security Adviser to coordinate Nigeria's involvement in international cyber security cooperation

to ensure the integration of Nigeria into the global framework on cyber security. Section 41(2) of the Act imposes a duty on the Attorney-General of the Federation to enhance Nigeria's cybercrime and cyber security law in order to conform to international standards and to maintain international cooperation in combating cybercrime.

Another remarkable provision of the Cybercrimes Act is the requirement for all law enforcement agencies to organize training programme for officers in charge of the prohibition, prevention, detection, investigation and prosecution of cybercrimes.[37] This makes it more effective for the law enforcement agencies under the Act to detect, prohibit and prevent cybercrimes in Nigeria.

Section 42 of the Act also establishes the Cybercrime Advisory Council which shall meet four times annually and shall be presided over by the National Security Adviser. Section 43 of the Act lists the duties of the Council, one of which is to create an enabling environment for members to share knowledge and promote the study of cybercrime detection. Section 44 of Act establishes the National Cyber Security Fund, and the monies that will be deposited in the Funds include levies, fines, gifts, contributions, grants, etc.

3.10 **Jurisdiction and International Co-Operation**

Section 50 of the Act vests the jurisdiction over offences committed under the Act on the Federal High Court regardless of where the offence is committed in Nigeria, in a ship or aircraft registered in Nigeria, by a citizen or resident in Nigeria if it would constitute an offence under a Law of the Country where the offence was committed, or outside Nigeria where the victim of the offence is a citizen or the alleged offender is in Nigeria and not extradited.

Section 51 provides that offences created under the Act shall be extraditable under the Extradition Act. Section 1 of the Extradition Act[38] provides that where a treaty or other agreement has been made by Nigeria with any other country for the surrender by each country to the other, of any persons wanted for prosecution or punishment, the National Council of Ministers may, by an order published in the Federal Gazette, apply this Act to that country. Nigeria has entered into extradition treaties with countries such as the United States of America[39] and the United Kingdom.[40] This enhances international co-operation in fighting cybercrimes.

[37]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 41(3).

[38] Cap. E25, LFN, 2010.

[39] Published in the Official Gazette (No. 23, Vol. 54 of the 13th day of April, 1967).

Section 52 of the Act mandates the Attorney-General of the Federation to co-operate with any foreign state to investigate or prosecute offences under the Act. Section 53 of the Act provides that evidence obtained in a foreign country can be used in court proceedings in Nigeria if such evidence is authenticated by a judge, magistrate or justice of the peace, or by the seal of a ministry or department of the government of a foreign state. This section is aimed at bolstering the mutual international assistance between Nigeria and other countries.

Section 54 of the Act stipulates the modes through which a foreign country can request for evidence in Nigeria. Section 55 provides for expedited preservation of computer data. Section 56 mandates the National Security Adviser, for the purpose of international cooperation, to provide a round-the-clock contact point which shall connect the contact points of other countries in accordance with agreements, treaties or conventions.

3.11 **Key Amendments to the Act**

President Bola Ahmed Tinubu signed the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024(hereinafter referred to as the Amendment Act) into law in February 2024. This Act amends 11 sections of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and consists of thirteen (13) sections. The purpose of the Cybercrimes (Amendment) Act, as stated in the Explanatory Memorandum, is to insert consequential words that were inadvertently omitted in the Cybercrimes Act. However, upon closer examination, it is evident that the Cybercrimes (Amendment) Act introduces new provisions that are significant to Nigeria's cyber security ecosystem.

(i) The Act [41]amended section 17(2) of the Cybercrimes Act 2015 to provide an exception to transactions that would be excluded from the categories of contractual transactions or declarations that are valid by virtue of electronic signature.[42] This exception allows for transactions to be legally verified in Certified True Copies. Additionally, the Act also amends section 17(1) (b) of the Cybercrimes Act by substituting the word 'geniuses' with the word 'genuineness'.[43] With this amendment, section 17(1)(b) of the Principal Act now places the burden of proof on the contender in cases where the genuineness of electronic signatures is in question.

(ii) The Act amended section 21(1) to read thus:

---

[40] Sahara Reporters, 'Court Orders Extradition to UK of Ex-MINT Boss, Emmanuel Okoyomon', available at<http://saharareporters.com/2015/05/04/court-orders-extradition-uk-ex-mint-boss-emmanuel-okoyomon>, accessed on 4th February, 2019.

[41]The Cybercrimes (Amendment) Act, 2024

[42]*Ibid.*, section 2 (1)(b).

[43]Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, section 2 (1) (a)

Any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team (CERT) Coordination Center through their respective sectoral CERTs or sectoral Security Operations Centres (SOC) of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues.[44] This amendment aims to improve the efficiency of managing reports of cyber threats by the Centre. The amendment to 21(3) changes the timeline that a person or institution is required to report an incident on a computer system or network from '7 days of its occurrence' to '72 hours of its detection'.[45] Section 22 of the Principal Act is expanded to include persons who are engaged in the services of public and private organisations as those who may be liable for the offence of identity theft and impersonation.[46] In the principal Act, only persons engaged in the services of financial institutions could be held liable for this offence.

Section 24(1)(a) and (b) which define the offence of cyberstalking has been a subject of many debate as many believed that it limits the freedom of expression provided for in the constitution.[47] The Amendment Act amended section 24 (1)(a) and (b) to read thus:
Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that is pornographic, and he or she knows to be false, for the purpose of causing a breakdown of law and order, posing a threat to life, or causing such message to be sent, shall be guilty of a crime.[48]

This provision in the principal Act defined cyberstalking to include materials that were grossly offensive, indecent, obscene, of menacing character or sent to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, hatred, ill will and needless anxiety.

The amendment has narrowed down the definition of the offence of cyberstalking. This means that some acts that previously constituted cyberstalking will not be considered as such moving forward. Before the amendment, it was argued that the Act did not define the word 'grossly offensive' as used in the section therefore making it vague. Member of

[44]Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, section 3.
[45]*Ibid*., section 3.
[46]*Ibid*., section 4.
[47]*Okedara v. Attorney General of the Federation* (2019) LCN/ 12768;See also section 39 of the Constitution of the Federal Republic of Nigeria 2009 (As Amended).
[48]Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, section 5.

the public did not know acts or expression that constitute 'gross offense'[49]Hence, section 24 has often been used by security agents as the basis to arrest journalists and other persons who speak or make publications criticising public officials. Under section 27(2), the scope of persons who may be liable for the offence of perpetrating fraud using computer systems or network has been expanded by the amendment from an employee of 'a financial institution' to an employee of 'any private or public organisation.[50]

In section 30(1) and (2), the offence of manipulating an ATM machine or Point of Sales terminal and the offence of connivance by the employee of a financial institution to perpetrate fraud using an ATM or Point of Sales device has been expanded by this amendment to include 'any other payment technology means'.[51]The amendment to section 37(1)(a) requires financial institutions to verify the identity of their customers by asking them to present a 'National Identification Number issued by the National Identity Management Commission and other valid' documents bearing their personal details, before issuing them ATM cards, credit/debit cards and other related electronic devices.[52]

The amendment to section 38(1) which provides for retention of traffic data and subscriber information records by communication service providers for a period of two years, now stipulates that such records are to be retained in accordance with the provisions of 'the Nigeria Data Protection Act.' It also streamlines the records to be retained to 'specific' traffic data and subscriber information.[53] The section acknowledges the recently enacted Nigeria Data Protection Act as the primary legislation on data protection in the country. Section 41(1), which provides for the responsibilities of the Office of the NSA as the coordinating body for all security and enforcement agencies under this Act, is amended to include two more responsibilities as follows:
(a) ensure the establishment of sectoral Computer Emergency Response Teams (CERT) and sectoral Security Operation Centres (SOC) that shall feed into the national CERT;[54]and
(b) ensure that all public and private organisations integrate and route their internet and data traffic to the sectoral SOCs thereby protecting the national cyberspace.[55]

[49]*Incorporated Trustees of Laws and Right Awareness Initiative v. The Federal Republic of Nigeria,* (Unreported) Suit no. ECW/ CCJ/ APP/53/2018.
[50]Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, section 6.
[51]*Ibid*., section 7.
[52]*Ibid*., section 8.
[53]*Ibid*., section 9.
[54]Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, section 10 (1) (d).
[55]*Ibid*., section 10 (1) (j).

The amendment to section 44 (2)(a) was the addition of the word 'value' to the word 'transactions' and also by the addition of '0.5% (0.005) equivalent to half percent' to emphasise the proportion of the levy, and an inclusion of new subsections (6) and (8), which reads thus:
(6) The Office of the National Security Adviser shall administer, keep proper records of the accounts and shall ensure compliance monitoring mechanism.
(8) A business specified in the Second Schedule to this Act that fails to remit the levy under section 44(2)(a) of this Act commits an offence and is liable on conviction to a fine of not less than 2% of the annual turnover of the defaulting business and failure to comply shall lead to closure or withdrawal of the business operational licence.[56]

By this amendment, the powers of the Office of the NSA in subsection (6) is expanded by adding administration and ensuring compliance monitoring mechanism of the National Cybersecurity Fund to the responsibilities of the NSA. Previously, the only responsibility of the Office of the NSA under the former subsection (6) was keeping the records of the accounts of the Fund. The new subsection (8) criminalises failure to remit the levy by specified businesses.

The amendment deletes section 48(4) which provided one of the punitive measures for offences under the Act. It provided for the cancellation of the international passport of a person convicted of an offence under the Act and for the withholding of a foreigner's passport until he has served his sentence or paid any fines imposed on him.[57]While most of the amendments introduce new words that enhance or modify the meaning of the affected provisions of the Act, the amendment of section 44 enables the implementation of the cybercrime levy and even stipulates a punishment if the specified businesses fail to comply.

4. **Comparative Analysis of Cybercrime Act Regimes in the United State of America, Canada and Egypt**

4.1 **United States of America (USA)**

In the USA, the main enforcement agency for combating cybercrime is the Federal Bureau of Investigation (FBI) and this agency is very instrumental in the investigation and apprehension of cybercriminals. It has set up special technical units and developed 'Carnivore', a computer surveillance system which can intercept all packets that are sent to and from the Internet Service Provider (ISP) where it is installed to assist in the

[56]*Ibid*., section 11.
[57]*Ibid*., section 12.

investigation of cybercrime.[58] The main legislation on cybercrime in the United States of America is the Computer Fraud and Abuse Act (CFAA) of 1986 (as amended).[59]

In order to keep up with the fast metamorphosis of the scope of cybercrime, numerous laws have been enacted in succession to curtail the nefarious activities of cybercriminals.[60] Under the CFAA, any person who suffers damage or loss by reason of unauthorized access and malicious use of a computer by another may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Such action must be brought within two years from the date of the act complained of or the date of the discovery of the damage.[61] Furthermore, in the case of *United States v. Janosko*,[62]the court held that restitution is mandatory when related to a violation of any paragraph of the CFAA, which proscribes fraud or property damage.

This position is in slight contrast with the provisions of the Nigerian Cybercrimes Act which does not recognize the right of victims of cybercrime to institute civil actions against the accused person for damages and other equitable reliefs. Rather, the court, which found the accused guilty of false pretence or fraud under the Act shall order him to make restitution to the victim. The restitution may be in form of return of the money or property, which was fraudulently obtained, and where it is no longer to return the property, the monetary value of the property shall be refunded the victim. This compensation is, however, enforceable as a civil action.[63]

4.2 **Canada**

Canada is a signatory to the Budapest Convention on Cybercrime, 2003,which requires state parties to prosecute cybercrimes committed within their respective territories.[64] In other words, a state party could claim territorial jurisdiction in a case where the computer system attacked is located in its territory, even if the perpetrator of the attack is not. The Criminal Code of Canada, (as amended in 2005) makes provisions for crimes relating to the use of computer and computer networks. A crime is a computer-based if it falls under

[58] K. OmoteMrabure, 'Lack of Centralized Database as an Impediment in Curtailing Cybercrimes in Nigeria' in Efoibi (ed.), *op. cit.*, 511-512.

[59] 18 U.S.C. 1030.

[60] These laws include Electronic Communications Privacy Act of 1986, the National Infrastructure Protection Act of 1996, the Digital Millennium Copyright Act of 1998, the Cyberspace Electronic Security Act of 1999, the Patriot Act of 2001, the Cyber Security Enhancement Act of 2002, the Anti-Phishing Act of 2005, and the Cyber security Act of 2010: Omote Mrabure, *op. cit.*, (n 58) 512.

[61]18 U.S.C. 2707 (c) & (f).

[62] 642 F.3d 40, 41 (1st Cir. 2011).

[63]The Cybercrimes (Prohibition, Prevention, etc) Act, 2015, section 49.

[64]Budapest Convention on Cybercrime, 2003, article 22.

section 430 or section 342(1) of the Canadian Criminal Code, that is, where a computer or data is object of the crime. Thus, under section 430 (1.1), an offence occurs when viruses are used to cause mischief to data. Under the Code, there is no law expressly prohibiting the creation or dissemination of computer viruses although section 430(5.1) of the Code provides that the distribution of virus might constitute an offence even if the virus is yet to be activated. The Criminal Code equally provides for computer-related fraud and other economic crimes, such as misuse of credit or bank cards, breach of trust or abuse of confidence, forgery and related offences.[65] Under the Canadian law, anything that can be considered property can be the object of theft or fraud. In the case of *Regina v. Stewart,*[66] the Ontario Court of Appeal held that copying a confidential list of hotel union employees from a computer printout constituted theft of property.

Combating cybercrime in Canada comes under the purview of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), a division of Public Safety Canada.[67] Under the OCIPEP umbrella is the Cyber Security division responsible for the Canadian Cyber Incident Response Centre (CCIRC), Canadian Cyber Incident Response Centre Partners, Cyber Security Technical Advice and Guidance, and Cyber Security in the Canadian Federal Government. OCIPEP facilitates communication and networking amongst Canadian organizations and businesses, provides updates and advisory tools, provides training and workshops, and acts in conjunction with similar departments of foreign government.

With regards to hate speech, advocating genocide against an 'identifiable group' is an indictable offence under the Canadian Criminal Code, and carries a maximum sentence of five years imprisonment.[68] Publicly inciting hatred against any identifiable group is also an offence which can be prosecuted either as an indictable offence with a maximum sentence of two years imprisonment or as a summary conviction offence with a maximum sentence of six months imprisonment.[69] However, unlike Nigeria, the Canadian Criminal Code provides for available defences to this offence. According to section 319(3) of the

[65]The Criminal Code of Canada, (as amended in 2005), section 430.
[66]42 Ontario. 2d 225 (1983); *Turner v. The Queen,* 13 Criminal Code of Canada 3d 430 (1984).
[67] D. Lyons-Hutton, 'Cybercrime in Canada: Strategies, Reforms, and Amendments in the Canadian Judicial and Law Enforcement Systems' available at <http://s3.amazonaws.com/academia.edu.documents/33973508/cybercrime_in_canada_strategies_reforms_and_amendments_in_the_canadia_judicial_and_law_enforcement_systems.pdf?>, accessed on 31st may, 2024 at 3:21pm.
[68]Criminal Code of Canada, RSC, 1985, section 318.
[69]*Ibid.*, section 319(2).

Code, no person shall be convicted of the offence of inciting hatred against an identifiable group in the following circumstances:

a. If he establishes that the statements communicated were true;
b. if, in good faith, the person expressed or attempted to establish by an argument an opinion on a religious subject or an opinion based on a belief in a religious text;
c. If the statements were relevant to any subject of public interest, the discussion of which was for the public benefit, and if on reasonable grounds he believed them to be true; or
d. If, in good faith, he intended to point out, for the purpose of removal, matters producing or tending to produce feelings of hatred toward an identifiable group in Canada.[70]

It is submitted that the above exceptions are very necessary under the Nigerian law in order to prevent or curtail the rate of harassment of citizens and abuse of rights to freedom of expression by the government under the guise of apprehending 'hate speech' propagandists. The above statutory provision was also confirmed in the landmark Canadian case of *R. v. Keegstra*[71]where the Supreme Court of Canada unanimously held that hate propaganda formed part of protected freedom of expression pursuant to section 2(b) of the Canadian Charter of Rights and Freedoms, 1982[72] because hate propaganda is a form of expression. The Court further held that section 319(2) of the Criminal Code violated section 2(b) of the Charter because it prohibited hate propaganda. Nevertheless, the Court, divided 4 to 3, concluded that section 319(2) of the Criminal Code violated the individual right to freedom of expression.

4.3 **Egypt**

The Anti-Cybercrime Law on Combating Information Technology Crimes[73] of Egypt came into force on 15th August, 2018. This Law deals with a wide range of issues, from combating cybercrime to fighting extremist and terrorist organizations that use the internet to promote their ideas among youth and to censoring websites with sensitive content.[74] It was designed to arrest the rising incidences of cybercrime sweeping through

[70] This provision is similar to the provisions on sedition under section 50 of the Nigerian Criminal Code.
[71] (1990) 3 SCR, 697.
[72] This Charter is part of Canada's Constitution.
[73]Law No. 175/2018.
[74] G. Sadek, 'Egypt: President Ratifies Anti-Cybercrime Law' available at<https://www.loc.gov/law/foreign-news/article/egypt-president-ratifies-anti-cybercrime-law/>, accessed on 1st June 2024.

Egypt and the Middle East in general.[75] Article 7 grants the investigating authority the power to block Egyptian-based or foreign websites featuring content that threatens national security or the national economy, as well as any content criminalized under the Anti-Cybercrime Law. Furthermore, by virtue of article 9, the public prosecutor is entitled to impose a travel ban on individuals suspected of committing a crime under the Anti-Cybercrime Law. The authorities may also access, seize, attach, or trace information, data, or information systems for a period of not more than 60 days and in any medium in order to establish facts related to the commission of a crime punishable under the law. Article 3 empowers the Egyptian authorities to claim criminal jurisdiction over non-Egyptian citizens for crimes punishable under the Anti-Cybercrime Law when committed outside Egypt, provided such actions are also punishable in the country in which they were perpetrated. As a result, action can be taken against websites and the people who operate them, even if they are hosted or located outside Egypt.

It appears that the Egyptian jurisprudence took advantage of the boundless nature of cyberspace to claim jurisdiction over acts of nationals of other countries who are not even residing in Egypt. On the contrary, the Nigerian Cybercrimes Act limits its jurisdiction to where the offence was committed within Nigeria, in a ship or aircraft registered in Nigeria, by a Nigerian citizen or resident if the person's conduct also constitutes an offence in the country where the offence was committed, or where the offender is in Nigeria and is not extradited to any other country for trial.[76]

Just as is obtainable under the Nigerian law, network service providers in Egypt are mandated to disclose any information related to users' activities as required by the authorities.[77] However, the Egyptian Anti-Cybercrime Law holds web administrators criminally accountable for the safety of the information systems, websites, and accounts under their control and management than its Nigerian counterpart. Under article 29, if a web administrator exposes a website, an email account, a private account, or an information system to a crime punishable under the Anti-Cybercrime Law, the penalty is imprisonment for a maximum period of one year and/or a fine ranging between 20,000 to 200,000 Egyptian Pounds. Where the crime was caused by the negligence of web administrator, the penalty is reduced to a maximum imprisonment of six months and/or a fine of between 20,000 and 200,000 Egyptian Pounds. Negligence is assumed when the

[75] E.A. Tahoun, 'Cybercrime in the Middle East' available at<https://www.researchgate.net/publication/317648264>, accessed on 1st June 2024.

[76] Nigerian Cybercrimes Act (As amended) 2015, section 50(1).

[77] Anti-Cybercrime Law on Combating Information Technology Crimes of Egypt, (Law No. 175/2018) article 6.

safety measures and precautions stipulated in the Executive Regulations are not satisfied. If an entity's website or email accounts become the victim of a crime punishable under the Anti-Cybercrime Law, the entity's manager is obligated to report the matter to the competent authorities. Hence, article 35 provides for imprisonment of not more than three months and/or a fine of between 30,000 and 100,000 Egyptian pounds for managers who fail to report such incidents. Furthermore, pursuant to article 36, the manager of a legal person who is aware of a crime committed in the name or through the account of the legal person or facilitates the same shall be punished with the penalty designated for the perpetrator.

5. **Loopholes and Inadequacies in the Enforcement of the Provisions of the Cybercrimes Act**

5.1 **Lack of a Specific Enforcement Agency**

Despite the dire nature of the crime which the Act was enacted to check, the Cybercrimes Act failed to specify the particular law enforcement agencies that will be in charge of enforcing its provisions; it only made mention of 'relevant enforcement agencies.'[78] The interpretation section scantily defines 'law enforcement agencies' to include such agencies that will be in charge of enforcement of the provisions of the Act.[79] Also, the First Schedule to the Act only listed the numerous agencies and parastatals which constitute the members of the Cybercrime Advisory Council, but did not include as one of their functions under section 43(1) the enforcement of the Act. Nevertheless, the Act empowers the Attorney-General of the Federation to make rules and procedure for the enforcement of the provisions of the Act. The Act also imposes a duty on the office of the National Security Adviser to be the coordinating body for all security and enforcement agencies under the Act.[80]

It is submitted that a specific and adequately equipped enforcement body be put in place in order to give effect to the provisions of the Cybercrimes Act. Considering the spate of wanton and violent abuse of powers by members of the various forces and paramilitary organizations in Nigeria, making a sweeping generalization with regards to the enforcement of this Act will certainly create too many chiefs but not enough Indians. There will be multiplicity of investigations and prosecutions over a single case and this would lead to unnecessary wasting of resources. It is also feared that there would not be

[78]Nigerian Cybercrimes Act (As amended) 2015, section 47.

[79]Nigerian Cybercrimes Act (As amended) 2015, section 58.

[80]*Ibid*., section 41(1).

accountability on the part of the enforcement bodies. In the end, the Act will only be a paper tiger and devoid of any enforcement and accountability.

5.2 **Lack of Provisional Consonance with Related Laws**

The Act also failed to take into cognizance the provisions of relevant Acts of the National Assembly to ensure that the provisions of the Cybercrimes Act are in alignment with the provisions of those other Acts. One of such Acts is the Evidence Act, 2011. While the Evidence Act gave powers to a wide range of officials to certify foreign judgments,[81] the Cybercrimes Act restricted the number of persons who can certify a foreign judgment in Nigeria,[82]etc. This apparent conflict could be resolved in favour of the Cybercrimes Act because, by the authority of *FRN v. Osahon*,[83] the specific law overrides the general law between two equivalent pieces of legislation on the same subject matter.

Another enforcement challenge to be encountered under the Act is the international outlook of cybercrime, which makes it imperative for Nigeria to cooperate with various nations of the world to tackle cybercrime. Nigeria have achieved a milestone in cyber security by accession to the Convention on Cybercrime[84] in 2022, and this will enhance international corporations in the fight against cybercrime.

Furthermore, section 41(3) of the Nigerian Cybercrimes Act (as amended) which provides that employees of law enforcement, security and intelligence agencies should undergo training programmes on cybercrime prevention. It is submitted that judges equally need to undergo comprehensive training in order to be abreast with the current nature and trend of cybercrime. This will enable them hand down judgments that are not out of touch with reality. Certainly, the non-inclusion of judges as among the people required to undergo training programmes would affect the effective implementation of the Act. For instance, section 45(3)(d) of the Act states that a court may not issue a warrant under subsection 2 of the section unless the court is satisfied that there are reasonable grounds for believing that the person named in the warrant is preparing to commit an offence under this Act. Thus, if the judge in question is not well versed in the basics of computer crimes and cyber security, he would not know exactly what amounts to 'reasonable grounds' in order to believe that a person named in the warrant is about to commit an offence under the Act. Therefore, without adequate training and acquisition of

[81] Evidence Act, 2011, section 106(i),

[82]Nigerian Cybercrimes Act (As amended) 2015, section 52.

[83]*Supra.*

[84] Budapest Convention on Cybercrime 2003.

knowledge by the judges on the subject of computer crimes and cyber security, the Act would not be effectively implemented.

5.3 **Absence of the Definition of Cybercrime**

The Nigerian Cybercrimes Act omitted the definition of 'cybercrime' in its interpretation section. Whether this omission is deliberate or not is unknown. But since the Act is geared towards, among other things, prohibiting, preventing, detecting, investigating and prosecuting cybercriminals, an all-inclusive meaning to the concept of cybercrime would not have been out of place for better clarification of the provisions of the Act.

5.4 Statutory Requirement of Direct Oral Evidence

Sections 126 and 127 of the Evidence Act, 2011 require that all facts be proved by oral evidence which must be direct, apart from the contents of a document. In this case, 'direct' refers to anything or state of things capable of being perceived by the senses or any mental condition of which a person is conscious.[85] What this connotes is that for any oral evidence of a fact to be admissible in court, it must be given through a witness who came in contact with such fact through any of his five senses: sight, smell, hearing, touch and taste. This provision poses a major hitch to the prosecution of cybercrime in the Nigerian courts because since cybercrime is usually a transboundary offence, victims and witnesses are most likely to be situated in a different country from that of the accused. Due to some reasons such as distance, feeling of insecurity, cost of transportation, etc., the witnesses would be unable to physically appear before the court. The alternative is the use of virtual video conferencing, and live video streaming via a voice over internet protocol (VoIP) such as Skype, which unfortunately, are not recognized under the Nigerian law of evidence.[86]

6. **Conclusion and Recommendations**

This present era of globalization and information technology has introduced myriad of concerns and developments in the growth of modern and sophisticated technologies. Almost all facets of the society have been significantly influenced by this new wave in technological advancement and pervasive machines.[87]The Cybercrime (Prohibition, Prevention, etc.) Act, 2015 of Nigeria was enacted to provide a unified legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation, and prosecution of cybercrimes in Nigeria. The Act is a legislative response to the increasing

[85] Evidence Act, 2011, section 258.

[86] F.E. Efoibi, 'Introduction to Law and Cybercrime' in F.E. Efoibi (ed.), *Handbook on Nigerian Cybercrime Law* (Benin City: Justice Jeco Pub. Co., 2018) 240-241.

[87] I.J. Lloyd, *Information Technology Law* (4th edn., Oxford: Oxford University Press, 2004) 3.

rate of fraudulent activities in the cyberspace for which there had hitherto, never been any specific statutory or regulatory regime in Nigeria. The Act also portrays a positive legislative effort to ensure the protection of information which is vital to national security as well as the privacy of the citizens.

Admittedly, the Act is a well-articulated effort to deter people from certain unwholesome and illegal behaviours on the internet by proscribing them through the instrument of legislation. For instance, conducts such as cyberstalking, cybersquatting, computer-related fraud and forgery, cyber terrorism, etc. are prohibited and a wide range of sanctions attached to their violations under the Act. However, due to some of the shortcomings found in some of the provisions, there is still room for improvement of the Act in some respects, especially considering the fact that the scope and form of cybercrime progressively expand with each passing day. Accordingly, this article recommends that there should be public awareness on the existence and provisions of the Cybercrimes Act, and that the Act should be harmonized with other related laws. In addition to training the judges, the article also calls for the amendment of the Evidence Act, 2011 to provide for cyberrelated evidence procedures.