Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.32, 2014

Cybercrime in Nigeria: An Overview of Cybercrime Act 2013

Mu'azu Abdullahi Saulawa[1*] M. K. Abubakar [2]
1. Faculty of Law, Umaru Musa Yar'adua University, P.M.B. 2218 Katsina State, Nigeria
2. Federal Inland Revenue Services, P. M. B 33, Garki, Abuja, Nigeria
* Email- muazu.abdullahis@gmail.com

Abstract
The paper focuses on cybercrimes in Nigeria, the examples of cybercrimes and also an overview of Cybercrimes Act 2013. Cybercrime are associated with Nigerian for examples email scams, phishing and credit card fraud; the Nigerian banks are susceptible to these attacks. It is evident that many Nigerians, organizations and government are investing significant amount of money in protection their Information communication and technology (ICTs) systems and networks. The increase rises of cybercrimes in the Nigerian cyberspace prove that some organizations are fighting cybercrimes through cyber security experts but only when security is breached or compromise. The recent Cybercrimes Act established by the Nigerian legislation intends to fight cybercrimes in all angles. The Overview of Cybercrimes Act 2013 gives us an inside of the relevancy of the Act to the current issue at hand where the Act dedicated a Part discussing the offences and their penalties in relation to cybercrime. With this Act in operation a roadmap in curbing the menace of cybercrime in Nigeria is captured. The paper will proffer recommendations and conclusions for effective measures for proper implementation and enforcement.
Keywords: Cybercrime, examples of cybercrimes, overview of Cybercrime Act 2013

1. Introduction

The paper focuses on cybercrimes in Nigeria, the types of cybercrimes as well as the overview of Cybercrime Act 2013. Cybercrimes are factor that has been a great threat to information communication and technology, the operation of cyberspace transactions; other cyberspace related functions are the most wonderful means of communications and transactions in the field of internet. "The Department of Justice ("DOJ") defines computer crimes as 'any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution''. [1]

2. Cybercrime in Nigeria

Cybercrime has been an eluding factor in the cyberspace transactions in Nigeria, where cybercrimes and computer related crimes are endemic. The integration of computer technology as a global issue, the economy of most nations in the world is accessible through the use of Information communication and technology and at stake.

With the opportunity opened to the general public in use for viable objectives, certain high-level of crimes are committed and some of the perpetrators of these menace crimes are refereed as 'Yahoo boys' syndrome. They took advantage of cyberspace transactions available on the internet to defraud the unsuspected victims who are mostly foreign transactions in thousands and million dollars. [2]

Fraudulently, they represent themselves as having particular goods to sell or that they involved in shipping or in a loan scheme. Most of the perpetrators-criminals/yahoo boys take advantage of some people looking for spouse through the internet. These criminally minded individuals will have a discussion with the victims through the internet and they will pretend to be interested and loving. Before the victim realised, the criminals would have succeeded in luring them to send dollars to enable them facilitate travelling documents. They falsify documents and tell all sorts of lies to get money or that they are beneficiary to a thousand of dollars in a trust account but they need a little money to secure the services of a Counsel to claim the trust fund.[3] Cybercrime in Nigeria is difficult to prove, thus requires the knowledge of expertise/specialist in computer technology and internet protocols

Nigeria battles against cybercrimes, efforts have been put in place by directing the sources and channel through which cybercrimes are perpetrated in Nigeria generally are targeted at individuals and not directly to computer systems, hence they require less technical expertise on the part of the criminals.

---

[1] Sheri A. Dillon et a l., Note , *Computer Crimes*, 35 Am. Crim. L. Rev. 503, 505 (1998) (defining "computer crime") (*quoting* National Institute of Justice, U.S. Dep't of Justice, Computer Crime: Criminal Justice Resource Manual 2 (19 89)).
[2] Ehimen O. R and Bola A, 'Cybercrimes in Nigeria', Business Intelligence Journal-January, 2010 Vol. 3, No.1. page 95.
[3] Ibid.

Recently, a report indicated that Nigeria is losing about $ 80 million dollars yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, is a market research based in South Africa. Also the American national Fraud Information Centre reported Nigerian money offers as the fastest online scam, up to 90 % in 2001. The centre also ranked Nigeria cybercrime impact per capita as being exceptionally high. [1]

Email scams and spam are the most repulsive phenomena among the cybercrime, these are ways used to present false financial investment. Nigeria's image is in question and has been tarnished as a result of her citizens' involvement in the cybercrime. The criminals send email that the victim is the named beneficiary to a will of estranged relative and stands to benefit the estate or the trust fund. Sometimes they used online charity; the criminals send email to the victims soliciting for funds and assistance to charitable organizations that do not exist.[2]

This discussion is not meant to portray Nigeria as the only people that engaged in these types of crimes. Although electronic scam or spam emails are generally believed to be linked to Nigeria, the scam is now prevalent in many other African countries and the targets are usually innocents individuals who could be anywhere in the world. The shift in the act has now extended to text messages, with the increase of use of cell phones, text messages are sent to mobile users to lure the victim into captivity. In the mist of their act, a mobile user will receive a text message congratulating the user for winning certain amount of money in promo by directing the user to call a particular number to claim the prizes or a package sent from US to deliver but someone has to pay doorstep delivery or clearing agent fees. The criminals have developed different strategies aimed at luring its victims.

In an attempt to fight the menace of cybercrimes in Nigeria, in a discussion where Mr. Tim suggested that for a Nigeria to fight the prevalent challenges of a growing menace of cybercrimes and cyber terrorisms there is need of cyber security experts nothing lee than one million in the next two years. And he further stressed that Nigeria has to prepare for cyber warfare to protect its economy in the 21st century, that in 2012, an estimated $ 1 trillion was lost to cyber-related frauds globally 'although only $390 billion was reported for obvious reasons.[3]

In a country of capacity development like India is targeting five million cyber security experts from now to the next three years. Currently, North Korea already sponsored 15, 000 cyber security experts well trained to defend the cyberspace of their country while china have over 25 million cyber commandos. [4]

Recently, the Nigerian government awarded a contract to Elbit Systems, an Israeli firm at the tune of $ 40 million, a cyber-intelligence expert for the purpose of spying and monitoring phones conversations text and reading private email messages. Although the Nigerian government is silent on the awards of contract as to true picture of 'internet surveillance for the purpose of gathering intelligence and national security'. The opinion of the Nigerian citizens across was not the nature of the contract that worried neither the citizens nor the company profile but the company is reputed as being 'a world leader in the fields of intelligence analyst and cyber defence, with proven solutions highly suitable for countries armies and critical infrastructure sites'. [5]

Naturally the contract should not have been a source of worry to any right thinking individual since its purpose is to "track down terrorist activities online." The worry comes with the fact that history is replete with governments of different countries abuse of such enormous power that gives them the legitimate access to their citizen's private lives. So even though it was rumoured that the federal government awarded the contract for the purpose of tracking and fighting the online activities of the Boko Haram members, Nigerians in general were quick to be critical and maybe to justify their fear, the federal government have been silent on the matter.[6]

The general Manager of Elbit, Yehuda Vered, announced that 'Elbit systems will supply its Wise Intelligence Technology (WiS) system to an unnamed country in Africa under new $ 40 million contract… for Intelligence

[1] The Economic Times: September 11, 2004. 1.

[2] 'Types/Incidences of Cybercrime in Nigeria', Martins Library, available at http://martinslibrary/blogspot.com/2013/08/type-incidence-of-cybercrime-in-nigeria.html.

[3] Mr. Tim Akano is a CEO of New Horizons and Vice-Chairman of Wini Group, in a discussion related to cybercrimes and Cybercrimes: 'Nigeria needs one million cyber security experts', National Mirror Newspaper, May 22, 2013, available at http://nationalmirroronline.net/new/cybercrimes-nigeria-needs-one-million-cyber-security-experts/. Accessed on 7/10/2014.

[4] Ibid.

[5] 'Cyber warfare and Nigeria's National Security', Thisday Newspaper, 30 May, 2013, available at http://www.thisdaylive.com/articles/cyber-warfare-and-nigeria-s-national-security/148887/. Accessed on 7/10/2014.

[6] Ibid.

Analysis and Cyber Defence'. [1]

A cyber intelligence expert and ethical hacker view that 'this project will be more offensive than ordinary intelligence gathering or record keeping system, I will classify it as a 'Black Operation Programme'. And further opined that monitoring systems with or without the Elbit Systems contract, the facts finding of experts that our online and offline extension activities are already being monitored. 'The internet as a whole has no privacy; the biggest technology being used in the world today is the biggest spy project ever created in the world.[2]

Another cyber security expert viewed that 'this is one of the most far-reaching policies ever designed in Nigeria's history to invade the privacy of citizens by secretly awarding Elbit Systems, a spy contract on Nigerian citizens. As usual the justification is that only by having access to our confidential communication can the enforcement agencies and security services keep us safe from criminals and terrorists. He further stressed that 'maintaining privacy on the internet is nearly impossible, if you forget to enable your protection, click on the wrong link or type the wrong thing, by implication you permanently attached your name to a possible anonymous service you are using. If the director of Central Intelligence Agency (CIA) cannot monitor his privacy on the internet then we don't have hope'.[3]

The National Security Adviser (NSA), Sambo Dasuki expresses his concern that every 9 seconds, Nigerian commits crime on the internet with a sharp rise from 0.9% in the 90s to 9.8% in 2014. [4]

The rapid used and communication of cyberspace activities today. The medium of tracking citizens are enormous for example google tracks us both in its pages and other pages it has access to as well as its range of android devices. Same with Facebook while others with socials media. For example Facebook correlates your online behaviour and even your cell phone has a location data. This is a clear case of all round surveillance. We are all being monitored and watched at all times and that data has been stored forever. These available data can be utilized and analysed effectively in tracking cyberspace criminal's activities.

3. Types of Cybercrime

The most prevalent cybercrime in Nigeria are:

3.1 **Yahoo boys:** these are called 419 they used e-mail addresses obtained from the Internet access points using e-mail address access applications.[5]

3.2 **Hacking:** the Nigerian hackers are engaged in cracking of a security codes for e-commerce, funds point cards and e-marketing product sites of computer system in order to steal or destroy data.[6]

3.3 **Software Piracy:** This act involves the unlawful reproduction and sharing of applications software for example games, movies/videos and audios. [7]

3.4 **Pornography:** generally consist of films and videotapes with varying degrees of sexual contents. The pornography is a free market-site in the Internet and that makes it easy for criminals to commits offences.

3.5 **Credit Card or ATM Fraud:** these can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction or when withdrawing money using ATM card.

---

[1] 'Elbit Systems officials arrive, begin installation of $ 40 million internet spy facility for Nigeria', Premium times, Newspaper, Nov 26, 2013, available at https://www.premiumtimesng.com/news/150333-exclusive-elbit-systems-officials-arrive-begin-installation-40-million-internet-spy-facility-nigeria.html. Accessed n 7/10/2014.

[2] Nsikak Joseph with Centrex Ethical Lab and 'Cyber warfare and Nigeria's National Security', op. cit.

[3] Adewale Obadare, CEO of Digital Encode, a Lagos based Cyber Security outfit and 'Cyber warfare and Nigeria's National Security', op. cit.

[4] The NSA was represented by Special Services Officer, Alhaji Ibrahim Bamiye at a forum title 'National Cybersecurity Forum' in Lagos where he said that cyber threat is real as it poses a national threat and indeed obvious at the national level; also the Director of communication, Amb. Wondo H further explained that the Office of National security Adviser (ONSA), has taken significant steps in engaging public-private partnership, incorporation of international law practices, establishment of computer unit in intelligent gathering to building functional system, drafting and electing prominent members to fill up security council seats in the office of Presidency among others are some of the measures taken to curb crime in Nigeria and 'Rate of Cybercrimes in Nigeria is alarming-NSA', Vanguard, June 21, 2014, available at http://www.vanguardngr.com/2014/06/rate-cybercrimes-nigeria-alarming-nsa/#sthash.j96Hm0Uh.dpuf. Accessed on 7/10/2014.

[5] Maitanmi Olusola et tal, 'Impact of Cyber Crimes on Nigerian Economy', the International Journal of Engineering and Sciences (IJES) Volume 2, Issue 4, p. 47. ISSN 2319-1813. Available at . http://www.theijes.com/papers/v2-i4/part.%20%284%29/H0244045051.pdf. Accessed on 3/2/2014.

[6] Ibid.

[7] Ibid.

The hackers can abuse this card by impersonating the credit card holder. Sometimes are called identity theft.

3.6 **Denial of Service Attack:** This is an act by the fraudster who floods the bandwidth of the victim‟s system or fillshis e-mail inbox with junk mails depriving him of the services he is entitled to accessor supply.

3.7 **Virus Dissemination:** A virus is a computer program that infects files, frequently executable programs, by inserting a duplication of itself into the file. There are different types of virus and each type requires human participation (usually unaware) of its spread. [1]

3.8 **Phishing:** it refers to cloning product and e-commerce web pages in order to dupe unsuspecting users. This is a technologically advanced scam that often uses spontaneous mails to trick people into disclosing their financial and/or personal data. [2]

3.9 **Cyber Plagiarism:** This is the act of stealing people's ideas through the Internet public domains. This is very common in academic institutions as students and lecturers alike use it to steal other people's ideas and publish them as their own original work.[3]

3.10 **Cyber Stalking:** The fraudster follows the victim by distributing mails and entering the chat rooms frequently.[4]

3.11 **Cyber Defamation:** The fraudster sends e-mails containing defamatory content to people related to the victim or posts it on a website.[5]

3.12 **Cyber Terrorism:** According to the U.S. Federal Bureau of Investigation, cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents (searchsecurity.techtarget.com. [6]

Nigeria is taking a great concern in combating the menace of cybercrimes, as legislation are enacted to look in to the acts of the perpetrators and to be punished when found guilty. Now the next segment of the paper will discuss the overview of Cybercrimes Act 2013.

4. An Overview of Cybercrime Act 2013

An overview of the Cybercrime Act will be divided into three parts, Part I will discuss the objective and application of the Act, while Part II will examine the protection of critical national information infrastructure and lastly Part III will analyse the offences and penalties of the Act.

This Part I discusses the following objectives[7] and application[8].

The objectives of this Act are to –

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

(b) ensure the protection of critical national information infrastructure; and

(c) promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

The Application of the provisions of this Act shall apply throughout the Federal Republic of Nigeria. The Act looks into the position of the nation with reference to information and communication where it provides for the designation of certain computer systems or networks as critical national information infrastructure. [9] And it further provides that:

The President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well being of its citizens, as constituting Critical National Information Infrastructure. [10]

The Presidential Order made under subsection (1) of this section may prescribe minimum standards,

[1] Ibid. p. 48.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Cyber terrorism http://searchsecurity.techtarget.com/definition/cyberterrorism.
[7] Section 1, Cybercrime Act 2013.
[8] Section 2, Ibid.
[9] Section 3, Ibid.
[10] Section 3 (1) Ibid.

guidelines, rules or procedure in respect of- [1]

(a) The protection or preservation of critical information infrastructure;
(b) the general management of critical information infrastructure;
(c) access to, transfer and control of data in any critical information infrastructure;
(d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national information infrastructure;
(e) the storage or archiving of data or information regarded critical national information infrastructure;
(f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and
(g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure

The Act explore the audit aspect, where it provides that The Presidential Order made under section 3 of this Act may require the audit and inspection of any Critical National Information Infrastructure, from time to time, to evaluate compliance with the provisions of this Act. [2]

The next part of the paper is Part III where it discusses the offences and penalties in relation to cybercrimes.

The Act provides for Offences against critical national information infrastructure.[3]

Any person who commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to section 3 of this Act, is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine. [4]

Where the offence committed under subsection (1) of this section results in grievous bodily injury, the offender shall be liable on conviction to imprisonment for a minimum term of 15 years without option of fine. [5]

Where the offence committed under subsection (1) of this section results in death, the offender shall be liable on conviction to death sentence without out option of fine. [6]

The Act further provides that Unlawful access to a computer[7] as an offence which attracts punishment.

Any person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000 or to both fine and imprisonment. [8]

Where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, the punishment shall be imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment.[9]

Any person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification with the act or omission, commits an offence and liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7, 000,000.00 or to both fine and imprisonment.[10]

The Act discuss unlawful interception of communications, where it further provides that Any person, who intentionally and without authorization or in excess of authority, intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment. [11]

The Act provides for unauthorized modification of computer data[12] and further discusses the following

[1] Section 3 (2) Ibid.
[2] Section 4, Ibid.
[3] Section 5, Ibid.
[4] Section 5 (1) Ibid.
[5] Section 5 (2) Ibid.
[6] Section 5 (3) Ibid.
[7] Section 6, Ibid.
[8] Section 6 (1), Ibid.
[9] Section 6 (2), Ibid.
[10] Section 6 (3), Ibid.
[11] Section 7, Ibid.
[12] Section 8, Ibid.

Any person who directly or indirectly does an act without authority and with intent to cause an unauthorized modification of any data held in any computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment. [1]

Any person who engages in damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority or in excess of authority, commits an offence and liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment. [2]

For the purpose of this section, a modification of any data held in any computer system or network takes place where, by the operation of any function of the computer, computer system or network concerned any-[3]

(i) program or data held in it is altered or erased;
(ii) program or data is added to or removed from any program or data held in it; or
(iii) act occurs which impairs the normal operation of any computer, computer system or network concerned.

The Act discusses the content of system interference and its punishment where it provides that Any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference in the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment. [4]

The Act further discusses the misuse of devices[5] where it subsections provides:

Any person who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available- [6]

(a) any devices, including a computer program or a component designed or adapted for the purpose of committing an offence under this Act;
(b) a computer password, access code or similar data by which the whole or any part of a computer, computer system or network is capable of being accessed for the purpose of committing an offence under this Act, or
(c) any device designed primarily to overcome security measures in any computer, computer system or network with the intent that the devices be utilized for the purpose of violating any provision of this Act,

The punishment further states that a person commits an offence and is liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both imprisonment and fine.

Any person who with intent to commit an offence under this Act, has in his possession any devise or program referred to in subsection (1) of this section, commits an offence and shall be liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment. [7]

Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer or network for any unlawful purpose or gain, commits an offence and shall be liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment. [8]

Where the offence under subsection (1) of this section results in substantial loss or damage, the offender shall be liable to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment. [9]

Any person who with intent to commit any offence under this Act uses any automated means or device

[1] Section 8 (1), Ibid.
[2] Section 8 (2), Ibid.
[3] Section 8 (3), Ibid.
[4] Section 9, Ibid.
[5] Section 10, Ibid.
[6] Section 10 (1), Ibid.
[7] Section 10 (2) Ibid.
[8] Section 10 (3), Ibid.
[9] Section 10 (4), Ibid.

or any computer program or software to retrieve, collect and store password, access code or any means of gaining access to any program, data or database held in any computer, commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10, 000,000.00 or to both fine and imprisonment. [1]

The Act provides for computer related forgery and the punishment that Any person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment.[2]

It further provides for Computer related fraud[3] where the Bill provides as follows:

Any person who knowingly and 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 for himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment. [4]

Any person who with intent to defraud sends electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment. [5]

The Act provides for the Identity theft and impersonation[6] and further provides that any person who in the course of using a computer, computer system or network-

(a) knowingly obtains or possesses another person's or entity's identity information with the intent to deceive or defraud, or

(b) fraudulently impersonates another entity or person, living or dead, with intent to -

(i) gain advantage for himself or another person;

(ii) obtain any property or an interest in any property;

(iii) cause disadvantage to the entity or person being impersonated or another person; or

(iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice,

The person commits an offence and liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment.

The Act also provides for Child pornography and related offences[7] and further provides that any person who intentionally uses any computer or network system in or for- [8]

(a) producing child pornography for the purpose of its distribution;

(b) offering or making available child pornography;

(c) distributing or transmitting child pornography;

(d) procuring child pornography for oneself or for another person;

(e) possessing child pornography in a computer system or on a computer-data storage medium;

commits an offence under this Act and is liable on conviction –

(i) in the case of paragraphs (a), (b) and (c) to imprisonment for a term of ten years or a fine of not less than N20,000,000.00 or to both fine and imprisonment, and

(ii) in the case of paragraphs (d) and (e) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than N10,000,000.00 or to both fine and imprisonment.

And further provides that any person who, intentionally proposes, grooms or solicits, through information and communication technologies, to meet a child, followed by material acts leading to such a meeting for the purpose of:[9]

(a) engaging in sexual activities with a child;

(b) engaging in sexual activities with a child where -

[1] Section 10 (5), Ibid.
[2] Section 11, Ibid.
[3] Section 12, Ibid.
[4] Section 12 (1), Ibid.
[5] Section 12 (2), Ibid.
[6] Section 13, Ibid.
[7] Section 14, Ibid.
[8] Section 14 (1), Ibid.
[9] Section 14 (2), Ibid.

(i) use is made of coercion, inducement, force or threats;
(ii) abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or
(iii) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence;

(b) recruiting, inducing, coercing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes; commits an offence under this Act and is liable on conviction-

i) in the case of paragraphs (a) and (b) to imprisonment for a term of not less than 10 years or a fine of not less than N15,000,000 or to both fine and imprisonment; and
ii) (ii) in the case of paragraph (c) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than N10,000,000 or to both fine and imprisonment.

Also provides that for the purpose of subsection (1) above, the term "child pornography" shall include pornographic material that visually depicts-[1]

(a) a minor engaged in sexually explicit conduct;
(b) a person appearing to be a minor engaged in sexually explicit conduct; and
(c) realistic images representing a minor engaged in sexually explicit conduct.

However, the Act provides for the purpose of this section, the term "child" or "minor" shall include a person below 18 years of age. [2]

The Act provides for Cyberstalking[3] and further provides for any person who, by means of a public electronic communications network persistently sends a message or other matter that - [4]

(a) is grossly offensive or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or
(b) he knows to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to another or causes such a message to be sent; commits an offence under this Act and shall be liable on conviction to a fine of not less than N2,000,000.00 or imprisonment for a term of not less than one year or to both fine and imprisonment.

Also provides for any person who, through information and communication technologies, by means of a public electronic communications network, transmits or causes the transmission of any communication – [5]

(a) with intent to bully, threaten or harass another person, where such communication places another person in fear of death, violence or personal bodily injury or to another person;
(b) containing any threat to kidnap any person or any threat to injure the person of another, any demand or request for a ransom for the release of any kidnapped person, with intent to extort from any person, firm, association or corporation, any money or other thing of value; or
(c) containing any threat to injure 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, with intent to extort from any person, firm, association, or corporation, any money or other thing of value; commits an offence under this Act and is liable on conviction-

(i) in the case of paragraphs (a) and (b) of this subsection to imprisonment for a term of not less than ten years or a fine of not less than N25,000,000 or to both fine and imprisonment; and
(ii) in the case of paragraph (c) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than N15,000,000.00 or to both fine and imprisonment.

The Act also provides that a court sentencing or otherwise dealing with a person convicted of an offence under subsections (1) and (2) may (as well as sentencing him or dealing with him in any other way) 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- [6]

(a) amounts to harassment, or
(b) will cause a fear of violence, death or bodily injury; prohibit the defendant from doing

[1] Section 14 (3), Ibid.
[2] Section 14 (4), Ibid.
[3] Section 15, Ibid.
[4] Section 15 (1), Ibid.
[5] Section 15 (2), Ibid.
[6] Section 15 (3), Ibid.

anything described/specified in the order.

The Act provides that a defendant who does anything which he is prohibited from doing by an order under this section, commits an offence under this section and shall be liable on conviction to a fine of not less than N10,000,000.00 or imprisonment for a term of not less than three years or to both fine and imprisonment. [1]

Also, the Act provides that the order made under subsection (3) of this section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court which made the order for it to be varied or discharged by a further order. [2]

The Act provides for Cybersquatting[3] and further provides that any person who, intentionally takes or makes 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 Governments in Nigeria, on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and is liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment. [4] In awarding any penalty against an offender under this section, a court shall have regard to the following - [5]

(a) a refusal by the offender to relinquish, upon formal request by the rightful owner of the 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 Governments in Nigeria; or

(b) an attempt by the offender to obtain compensation in any form for the release to the rightful owner for use in the Internet of the 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 of Nigeria.

In addition to the penalty specified under this section, the court may make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner. [6]

The Act provides for Cyberterrorism[7] and further discuss that any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and liable on conviction to life imprisonment. [8] Lastly, provides for the purposes of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended. [9]

The Act provides against Racist and xenophobic offences [10] and that any person who[11] -

(a) distributes or otherwise makes available, any racist and xenophobic material to the public through a computer system or network,

(b) threatens, through a computer system or network, with the commission of a criminal offence -
  (i) persons for the reason that they belong to a group, distinguished by race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors, or
  (ii) a group of persons which is distinguished by any of these characteristics;

(c) insults publicly, through a computer system or network -
  (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or
  (ii) a group of persons which is distinguished by any of these characteristics; or

(d) distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998; commits an offence

[1] Section 15 (4), Ibid.
[2] Section 15 (5), Ibid.
[3] Section 16, Ibid.
[4] Section 16 (1), Ibid.
[5] Section 16 (2), Ibid.
[6] Section 16 (3), Ibid.
[7] Section 17, Ibid.
[8] Section 17 (1), Ibid.
[9] Section 17 (2), Ibid.
[10] Section 18, Ibid.
[11] Section 18 (1), Ibid.

and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than N10,000,000.00 or to both fine and imprisonment.

In addition, the Act provides for the purpose of subsection (1) of this section, the term **"**racist and xenophobic material" means any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors. [1]

Amongst the offences, the Bill provides for Attempt, conspiracy, aiding and abetting and further provides that any person who -[2]

(a) attempts to commit any offence under this Act; or

(b) does any act preparatory to or in furtherance of the commission of an offence under this Act; or

(c) abets, aids or conspires to commit any offence under this Act,

commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

Finally, in the offences against cybercrimes Bill, the bill provides for corporate liability [3] and further provides that a body corporate that commits an offence under this Act shall be liable on conviction to a fine of not less than N10,000,000.00 and any person who at the time of the commission of the offence was a chief executive officer, director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment; [4] and lastly, provides that nothing contained in this section shall render any person liable to any punishment where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.[5]

Fighting cybercrimes requires not only IT but also requires IT security experts as discussed above in this paper and that includes the roles of security agencies. The most important aspect is how to deal with threats associated with the cybercrimes not just to keep talking about the crimes, the talk is meaningless if we can closed the gaps. The security agencies need to be equipped with the skills, the insight and outsights necessary means to fight cybercrimes.

While the necessary resources to fight the menace of cybercrimes so does the imperative measure to be used with a focused direction to be utilized against misdirect approach on the problem. The priorities be identified and proffer a strategies that would be adopted in tackling the menace. The knowledge should be fully circulated to the general public, so as to have a practical approach and appreciate the use of technology not to talk of the crimes as the negative aspect of it.

In addressing the cybercrimes, it requires a holistic approach, both the cyber cafes and other relevant stakeholders to comes in to a platform by creating education-awareness programme on how to foresee the problem, risk and solutions and a potential victim in the use of ISP, cybercafés, government and security agencies and internet users.

With Cybercrime Act 2013 coming into operation, it addresses the most important aspects of cybercrimes and even extended beyond. The highlight of the offences and penalties is one aspect that gives the Act a credit what matter the most now is the crucial aspects that is the implementation and enforcement. Mishandling the enforcement can backfire and enforcement can only be achieved if it avoids harassment, abuse of privacy, abuse of office, extortion etc. we cannot allowed where the genuine users of the internet, cyber security experts to be frustrated from doing their job and unable to benefit from the internet and let other used it for another purpose. The only measure to be adopted in curing the menace of cybercrimes is accountability, sincerity, rigor and corruption free in the implementation and administration of the Act for its effective use.

5. Conclusion

Cybercrime is the global practice today, particularly in Nigeria where it has become a predominant practice whereby the regulations to these crimes are newly established for the purpose of tackling cybercrime threats. That the paper recommends that a full compliance in the implementation and enforcement of Cybercrimes Act 2013, also further to this the government shall in conjunction with other stakeholders create a Unit of cyber-

[1] Section 18 (2), Ibid.
[2] Section 19, Ibid.
[3] Section 20 Ibid.
[4] Section 20 (1), Ibid.
[5] Section 20 (2), Ibid.

security experts. The formalization of the countries of its legal instruments and the implication arising from the ICTs are essential in fighting this menace. The criminals took the advantage of innocent citizens, ICT Corporation and the infrastructures of the government in carrying their acts and that is why there is need for a provision of software tracker of internet service provider ISPs to monitor cybercrimes and make used of Patrol Units so as to strategize the trace and track of the criminals and ensure that an awareness to the general public on the cyber security information has been ensures.

References

Cybercrime Act (2013).

Ehimen O. R and Bola A, (2010), 'Cybercrimes in Nigeria', Business Intelligence Journal-January, Vol. 3, No.1, 95.

Maitanmi Olusola, Ogunlere Samson, AyindeSemiu, AdekunleYinka, (2013) 'Impact of Cyber Crimes on Nigerian Economy', the International Journal of Engineering and Sciences (IJES) Volume 2, Issue 4, 47.

Sheri A. Dillon, Douglas E. Groene and Todd Hayward,. (1998), Note , Computer Crimes, 35 Am. Crim. L. Rev. 503, 505.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar