AN APPRAISAL OF THE NATURE AND TYPES OF SANCTIONS UNDER THE CYBERCRIME ACT 2015

Dayo Godwin Ashonibare* and Joel Barde**

Abstract

Cybercrime has been described as the crimes committed over the internet or computer network using a computer device as a tool for the commission of the offence. This has become more worrisome owing to the advancement in technology orchestrated by the increasing rate of telecommunication infrastructure deployment in every nook and crannies of Nigeria thereby providing access to internet. Cybercriminals have now deployed new methods provided by emerging technologies to commit cybercrime thereby making the punitive and deterrent effect of the Cybercrime Act, 2015 seemingly ineffective. By adopting the doctrinal research methodology, this paper analysed the history, categories and types of cybercrime with relevant provisions of the Act which prohibits the offences. Despite the various offences and its sanctions, the crime has continued to grow exponentially thereby suggesting the ineffectiveness of the extant laws. The work concludes by providing recommending that sanctions would only be effective if fully implemented by all stake holders in the criminal justice system.

Keywords: Cybercrime, Legislation, Offences, Punishment

1.0 Introduction

Cybercrimes are crimes committed over the internet or computer network through the aid of a computer device[1]. Cybercrime dates

* Lecturer, Faculty of Law, Baze University, PhD Student Faculty of Law, University of Jos, Nigeria. Email:

** Professor of Law, Faculty of Law, University of Jos, Nigeria. Email:

1What is Cybercrime? Types, Examples, and Prevention https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention accessed 10/12/2024

decades back according to Arctic Wolf Networks [2] in its publication which stated thus:

> Over the past decade, cybercrime has become big business — a $1.5T industry with an entire ecosystem of organizations run like legitimate organizations. Some offer technical leadership and step-by-step instructions through robust customer service via ransomware-as-a-service. The most brazen threat actors have even taken out pop-up ads selling their products. Yet, while the cybercrime industry has exploded in the past ten years, the truth is that cybercrime is not a new kind of threat. In fact, it goes back not just decades but centuries."[3]

Technically, the first cyber-attack took place in France in 1834, long before the internet was created. Attackers gained access to the French telegraph network and stole data on the financial markets. Since then, cybercrime has increased dramatically and is characterized by an intriguing evolution of strategies, tactics, and procedures that are all used for harmful ends.[4]

Taking a look at the history of cybercrime, this paper would present the evolution of cybercrimes as it provides notable attackers whose "groundbreaking" activities attracted the attention of federal agents, they include the following:[5]

i. The Telegraph System - Two criminals obtained access to the financial markets in 1834 by hacking the French telegraph

[2]"The Leader in Security Operations." Arctic Wolf, 27 Jan. 2023, https://arcticwolf.com/. Accessed 06 Feb. 2023

[3]Arctic Wolf. "History of Cybercrime." Arctic Wolf, 1 Dec. 2022, https://arcticwolf.com/resources/blog/decade-of-cybercrime/#:~:text=1962,their%20database%20via%20punch%20card. Accessed 06 Feb. 2023

[4]Ibid

[5]"Cybercrime: History, Global Impact & Protective Measures", 2022. BlueVoyant, https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022. Accessed 06 Feb. 2023

system and stealing information. Many professionals view this incident as the first cybercrime.

ii. Telephone Hacking - Alexander Graham Bell obtained a patent for the telephone in 1876, allowing telegraphic speech transmission.[6] Teenage boys broke into Bell's telephone firm two years after this idea was commercialized and switched calls. Later on, from the 1960s to the 1980s, phone hacking, or 'phreaking', gained popularity.

iii. 'White Hat' Hacking - A French computer scientist named Rene Carmille broke into the Nazi data base in 1940. Carmille, a punch card computer specialist, reprogrammed Nazi punch card equipment to stop them from accurately registering data. His efforts prevented the Nazis from registering and locating Jews.

iv. The 1988 'Morris Worm' - The Morris Worm-Robert Morris releases what on the Internet will be considered the first worm. Robert Morris, a graduate student at Cornell, was responsible for the internet's first significant cyberattack. Prior to the launch of the World Wide Web, when academic scholars dominated the internet, the "Morris Worm" attacked. Among other universities, it infected the computers at Stanford, Princeton, Johns Hopkins, NASA, Lawrence Livermore Labs, and UC Berkeley.

v. Social Media Scams[7]- Cybercrime truly started to take off in the early 2000s as social media started to take off. The surge of people filling up profile databases with all the information they could resulted in a torrent of personal data and an increase in ID theft. The data was utilized in a number of ways by thieves to access bank accounts, create credit cards, and commit other types of financial theft. The creation of an annual worldwide criminal operation worth millions of dollars is the new wave. These criminals target anything and everyone with a digital

[6]Arctic Wolf. "History of Cybercrime." Arctic Wolf, 1 Dec. 2022, https://arcticwolf.com/resources/blog/decade-of-cybercrime/#:~:text=1962,their%20database%20via%20punch%20card. Accessed 06 Feb. 2023

[7]"Cybercrime: History, Global Impact & Protective Measures", 2022. BlueVoyant, https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022. Accessed 06 Feb. 2023

> presence, operate in groups, and employ tried-and-true strategies.[8]

This historical development of Cybercrime in Nigeria has many histories as opined by different authors. Though, before the emergence of internet services we already had financial fraudsters also known as 419-ners in operation in Nigeria[9]. However, the emergence of internet fraud could be traceable to 1970s as result through the use of postal messages, fax mails which are means used to request for the transfer of money from accounts which most times are frozen accounts to an account overseas[10]. In the year 1996 due to the emergence of cybercafés postal mail started fizzling out gradually raising new breeds referred to as yahoo-yahoo boys coined from the word yahoo mail services.[11]

As the world develops technologically, there are several benefits that come with it which are widely acknowledged. However, it also has several challenges that unfortunately go unacknowledged, especially in less developed parts of the world such as African countries. Cybercrime and money laundering are the two main challenges resulting from the spread of technology which could all be summed up into the broad ambit of 'Identity Fraud'. It involves the unauthorized access to and use of people's personal data.[12]It could be described as any behaviour that is tainted with a criminal intent to defraud another individual or organization by using unsolicited tactics to cheat or deceive.[13]

---

[8]Acharjee, Sauvik. "The History of Cybercrime: A Comprehensive Guide (2021)." Jigsaw Academy, 6 July 2022, https://www.jigsawacademy.com/blogs/cyber-security/history-of-cybercrime/. Accessed 06 February 2023

[9]Samson Ezea, "Prevalence of internet fraud among Nigerian youths".

[10]OyelakinOluwatomisin, "Boutade Of Internet Fraudsters In Nigeria" https://djetlawyer.com/boutade-of-internet-fraudsters-in-nigeria/ accessed 22 June, 2023

[11] Ibid

[12]Paradigm Initiative and Privacy International, *The Right to Privacy in the Federal Republic of Nigeria: Stakeholder Report, Universal Periodic Review* [2018] (31), p. 8-11.

[13] B. A. Omodunbi, '*Cybercrimes in Nigeria: Analysis, Detection and Prevention'* FUOYE Journal of Engineering and Technology, [2016] (1)(1), Issue 1, September 2016

Nigeria is a country that has been rapidly developing in terms of technology. It also has one of the largest populations which means that it also has one of the largest populations of internet users and in turn a high occurrence of internet fraud which can be observed throughout the Nigerian history of internet Fraud.

Nigeria, similar to many African countries got access to the internet wholistically in the mid '90s where e-commerce took off and started to make a shift to cashless transactions.[14] At first, the shift was well received and led to numerous advantages such as a reduction in crime particularly theft as people were no longer carrying cash around. However, this reduction in crime was short-lived as criminals now adapted to a new environment. One of the first ways that fraud was committed was through the use of 'Famous Names'. [15] This is when a fraudster uses credit cards belonging to well-known celebrities to make several purchases. Considering the fact that the internet was a new concept this scheme may have been quite successful.

As the internet developed the many through which fraud was conducted evolved. It graduated from the scheme of "Famous Names" to more sophisticated schemes such as dummy websites, phishing and pharming. In the modern day of the internet, internet fraud is at an all-time high leading to what some have referred to as a data epidemic, especially among Nigerian male youth. This could be due to a number of reasons such as unemployment, high inflation and many more economic reasons. [16]

2.0 Conceptual Clarification

In order to situate some terms in the context of their usage in this paper, it is apposite to offer some clarifications into some salient terms in the paper.

[14]D. Montague, *Fraud Library History of Online Credit Card Fraud,* 2014
[15]Ibid
[16] L. Joseph and A Muiwa, *Chasing the Nigerian Dream: The Proliferation of Cyber Fraud Among Nigerian Youths and Its Effect on Nigeria's Global Image* available athttps://www.researchgate.net/publication/349173609_Chasing_the_Nigerian_Dream_The_Proliferation_of_Cyber_Fraud_among_Nigerian_Youths_and_its_Effect_on_Nigeria's_Global_Image accessed 22nd June 2023

2.1 Cybercrime

Cybercrimes can be defined as the series of illegal activities that take place in the cyber space with the aid of computer. A Computer has been described as any device for storing and processing information.[17]While the cyber space is also known as the internet consists of criminal acts that are committed online by using electronic communications networks and information systems.[18]

According to Smith, Grabosky, Urbas[19] defining cybercrime raises conceptual complexities. Varied definitions of cybercrime do exist. In addition to the difficulty of definition, it is also called by variety of terms such as computer crime, computer-related crime, digital crime, information technology crime,[20] Internet crime,[21]virtual crime,[22] e-crime[23]and net crime.[24] Cybercrime could reasonably include a wide variety of criminal offenses and activities.

The introduction of hackers, organized criminals, commercial competitors and government intelligence into the cyber space for the execution of theft, disruption, espionage and sabotage is one of the definitions that encapsulate the broad concept of cyber-crime.

---

[17] S. 258 (1) Evidence Act, 2011Cap E 14 and Section 58 Cybercrime Act, 2015

[18] The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers)

[19] Smith, R.G., Grabosky, P., Urbas, G.,Cyber Criminals on Trial. Cambridge (UK): Cambridge UP. Statistics Canada (2002). Canadian Community Health Survey Cycle 1.2: Mental Health and Well-being. 2004.

[20]Maat S., '*Cybercrime: A Comparative Law Analysis*' (University of South Africa; PhD Thesis, 2004).p.239.

[21]Wall, D.S., '*Maintaining Order and Law on the Internet'*. In: Wall DS (Ed.), *Crime and the internet*. (London: Routledge, 2001). Pp.167-183.

[22]Lastowka, F.G., Hunter, D.,Virtual Crimes. New York Law School Law Rev. 49:, 2004 293-316.

[23]Olayemi, OJ., A Socio-technological Analysis of cybercrime and cyber security in Nigeria, *International Journal of Sociology and Anthropology* , Vol. 6(3), 2014,.. 116-125.

[24]Mann, D., Sutton, M., NETCRIME:More Change in the Organization of Thieving. *Br. J. Criminol*. 38(2): 1998, 201-229.

United Nations Office on Drugs and Crime describes cyber-crime in this manner:

> Cybercrime is a growing, global problem. Whether you are a small business, a fortune 500 company, buying your first smartphone or becoming a cybersecurity expert, you need to be aware of cybercrime. The Internet affords education and economic opportunities beyond anything the world has ever seen. This same tool, however, also allows for unprecedented opportunities to cause harm. By abusing technology, cybercriminals ruin businesses and even lives.[25]

In establishing that cybercrime has taken place, there are certain elements that must be present. These elements are:

i. The act was criminal;
ii. The criminal act was executed on the cyber space;
iii. The criminal act has victimized an individual, corporate body or the government.

Viswanathan's book[26] further demystified on the above stated aspect on cyber to mean the following:

i. Any illegal action in which a computer is the tool or object of the crime i.e., any crime, the means or purpose of which is to influence the function of a computer,
ii. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,
iii. Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.

[25] "Cybercrime – University Module Series Overview". United Nations Office on Drugs and Crime. https://www.unodc.org/e4j/en/tertiary/cybercrime.html. Accessed 03 Feb. 2023

[26] S.T. Viswanathan. "The Indian Cyber Laws with Cyber Glossary", 2001, p. 81.

3.0 Categories of Cybercrime

The use of internet is infinite and immeasurable; this reality is accompanied by the endless possibilities granted to criminals online. Although cybersecurity experts put a lot of effort into closing security gaps, attackers are constantly looking for novel ways to avoid IT detection, get around defenses, and take advantage of developing weaknesses.

Cybercrime can be categorized into the following:

i. Cyber-crimes against individuals – These are cybercrimes targeted towards individuals e.g. cyber bullying, phishing, cyber defamation, etc. Ordinary people are typically the most vulnerable targets for cybercriminals due to ignorance, lack of direction, and weakness in cybersecurity.
ii. Cyber-crimes against organizations – These are cybercrimes targeted towards an organization through the sending of virus, Denial of Service (DoS) attack, web jacking, salami attack aimed at disrupting or stealing trade secrets etc. Cybercriminals may only be able to collect a small amount of ransom through crimes that primarily target individuals. On the other hand, attacking huge businesses or organizations can assist them in obtaining highly secret information from both private and public institutions and bodies.
iii. Cyber-crimes against society at large – These are cybercrimes targeted towards at a certain group within society or at the entire nation. e.g., cyber pornography, cyber terrorism, cyber espionage. The most recent cyberattacks are reinventing 'existing' threats by utilizing work-from-home settings, remote access technologies, and new cloud services. Examples are: Phishing/social engineering, malware, ransomware, Distributed Denial-of-Service Attacks (DDoS), man-in-the-middle attacks, Advanced Persistent Threats (ATPs).

4.0 Types of Cybercrime

When it comes to the types of cybercrimes, due to the endless possibilities to be explored in the internet and cyber space, there are

countless crimes that are committed on the cyberspace. This is by no means an exhaustive list, but it will give you a good understanding of the security flaws in networks and other systems that attackers may exploit, as well as their potential motivations.[27]

I. Hacking/Unauthorised Access: The definition of Hacking is said to be synonymous with unlawful access and system interferences[28]. Hacking a device or system can be referred to as altering or improving it, without any suggestion of illicit access.[29] This is a type of crime that occurs in the cyber space which involves the unauthorized access of computer systems, breaking security features and gaining unauthorized access to the data stored in them.[30] This type of crime is characterized by unlawful interception inbound and outbound data by hackers. It has also been described as the unauthorized access to personal sensitive information.[31] Hackers take advantage of the use of the weaknesses and loop holes in operating systems to attack/destroy data and steal important information from a victim's computer. Hacking is generally not illegal; it is the process that differs hence hacking can both ethical and unethical[32]. There is a clear difference between methods of Hacking and Hackers. We have the White Hat Hackers referred to as the good guys, the black hat hackers who hack for fraudulent purposes and are

[27]The 12 Types of Cyber Crime There Are Literally a ... - Delhi University. http://www.dcac.du.ac.in/documents/E-Resource/2020/Metrial/408sunitayadav4.pdf. Accessed 06 Feb. 2023

[28]D Ashonibare, Challenges of the Prosecution & Enforcement and Prosecution of Offences under the Cyber Crime (Prevention & Prohibition) Act 2015. Baze University, Law Seminar Series, Vol 1 August, 2018.

[29]Halderand D, Jaishankar K, "Cybercrime and the Victimization of women Laws, Rights, and Regulations", Hershey, PA, USA: IGI Global. ISBN 970-60960-830-9(2011)

[30]Ashaolu and Oduwole. Understanding Information Technology Law through the cases (Freedom Press) September, 2010.

[31]Ibikunle F and Eweniyi O. Approach To Cyber Security Issues InNigeria: Challenges And Solutionn (IJCRSEE) International Journal of Cognitive Research in science, engineering and educationVol. 1, No.1, 2013. Accessed on 10/01/2023

[32]D Ashonibare, Challenges of the Prosecution & Enforcement and Prosecution of Offences under the Cyber Crime (Prevention & Prohibition) Act 2015. Baze University, Law Seminar Series, Vol 1 August, 2018

also referred to as the "bad guys". The Grey Hat hackers combine the functions of a White Hat Hacker and Black Hat Hackers. Hacktivist usually hack for political and economic emancipation examples, wiki leaks, anonymous etc. The method of Hacking can either be electronic, computer, Distributed Denial of Service, Injection attacks and Remote Code Execution Attacks to mention a few.

Further to the above, Section 8 of the Cybercrime Act[33]recognize and prohibit the offence of Hacking, to wit:

> Any person who without lawful authority, intentionally or for fraudulent purposes 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 with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment.

The above provision best describes and defines the meaning of Hacking and the act that constitute a breach under the act. The section provides that any unauthorized access/system interferences intentional done by either inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system will amount to hacking of the system and shall be punishable under the act.

The Provision of Section 6(1-4) of the Act[34]categorize what constitutes System Interferences punishable under the act to wit:

[33]Cyber Crime (Prevention & Prohibition) Act 2015
[34] Ibid.

> 6 (1) Any person, who without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national security, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 Years or to a fine of not more than N5, 000,000.00 Or to both fine and imprisonment.
> 6 (2) Where the offence provided in subsection of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information, the punishment shall be imprisonment for a term of not more than 7 years or a fine of not more than N7, 000,000.00 or to both such fine and imprisonment.[35]

The above section categorizes the infringement and breach and prohibits any unauthorised interference with data that are vital to national security, protection for commercial or industrial secrets from unlawful access gain by rival company or for fraudulent purposes, unlawfully access into a computer system with hidden Identity for the sole purpose of perpetrating the act and the unlawful sale of passwords and computer keys to unlawfully access the system. Regrettably we are yet to record any land mark case in respect of the provisions mentioned above.

II. Identity Theft/Impersonation

Identity theft is the fraudulent act of using another person's personal information in other to commit crime. While impersonation is the act of pretending to be another person. The 2015 Act prohibits the offence of identity theft which is one of the most prominent cybercrimes

[35] *6 (3) Any person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification or attribution with the act or omission, commits an offence and shall be liable on conviction to Unlawful access to a computer. Imprisonment for a term of not more than 7 years or to a fine of not smore than N7,000,000.00 or to both such fine and imprisonment.*
6 (4) Any person or organisation who knowingly and intentionally traffics in any password or similar information through which a computer may be accessed without lawful authority, if such trafficking affects public, private and or individual interest within or outside the federation of Nigeria, commits an offence and shall be liable on conviction to a fine of not more than N7, 000,000.00 or imprisonment for a term of not more than 3 years or both such fine and imprisonment.

perpetuated by internet fraudsters in Nigeria. The Act now prohibits offences that are related to Identity theft. Identity Theft as defined above, is used when a person purports to be some other person, with a view of doing a fraudulent act[36]. The Crime is synonymous to the offence of impersonation though committed on the cyber space. The most common source to steal identity information of others, are data breaches affecting corporate organizations and government parastatals.[37] Breaching of private information such as credit card, insurance cards, emails and other relevant information that can be stolen online[38].

Impersonation online is another way identity thieves use to carry out their operation online. This takes place in cases of using another person's personal information which are; names, identifying numbers, or credit card numbers, security fixtures personal to a person without the owner's permission[39] Some foreigners, have fallen victims of fake online marriages after being deceived online by a non-existing lover.[40]However, it is important to note that there is a significant difference between the identity in the physical space and identity in the cyber space[41]. In the physical space, persons prove their identity by personal documents. In the cyberspace, identity is synonymous and may be replaced by a name, IP address and password etc. This means the login name and password and all security measures, for example, digital

[36] D Ashonibare, Challenges of the Prosecution & Enforcement and Prosecution of Offences under the Cyber Crime (Prevention & Prohibition) Act 2015. *Baze University, Law Seminar Series,* Vol 1 August, 2018

[37]Hoofnagle C.J, "Identity Theft: Making the Known Unknowns Known." *Harvard Journal of Law and Technology, Vol. 21, Fall 2007*

[38]J Lynch, Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks Berkeley Technology Law Journal Vol. 20, No. 1, Annual Review of Law and Technology (2005), pp. 259-300 (42 pages).

[39]Hoofnagle, Chris Jay, Identity Theft: Making the Known Unknowns Known. Harvard Journal of Law and Technology, Vol. 21, Fall 2007

[40] Ibid.

[41]D Ashonibare, Challenges of the Prosecution & Enforcement and Prosecution of Offences under the Cyber Crime (Prevention & Prohibition) Act 2015. Baze University, Law Seminar Series, Vol 1 August, 2018

certificates, although this has its advantages and disadvantages etc.[42] Prior to the passing into law of the Cyber Crime Act such offences are punished under the Criminal Code, Penal Code and the Advance fee fraud amongst other laws.

> *Section 22(2) of the Act[43]Any person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person; or*
> *Subsections (2) basically address the issue forging of signature or using password without the owner's permission to carry fraudulent activities on the Internet. This provision clearly provides what constitutes identity theft as described above.*

Similarly, Section 22(3)[44] elucidates further that anybody who fraudulently impersonates another entity or person, living or dead, with intent to ---

> (a) Gain advantage for himself or another person;
> (b) Obtain any property or an interest in any property;
> (c) Cause disadvantage to the entity or person being impersonated or another person; or
> (d) Avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.[45]

The above proviso clearly lay to rest all concerns regarding the prosecution of the offence of Identity theft but despite this proviso, law enforcement agencies have failed to utilize the provisions of the Act.

---

[42] "The Concept of Identity theft" http://www.vartotojai.lt/en/ID-theft/identity-theft/concept accessed on the 20 December 2022

[43]Cybercrime (Prevention & Prohibition) Act 2015

[44] Ibid

[45] 22(4) Any person who makes or causes to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false and with intent that it be relied upon respecting his identity or that of any other person or his financial condition or that of any other person for the purpose of procuring the issuance of a card or other instrument to himself or another person commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than N7,000,000.00 or to both such fine and imprisonment.

III. Cyber Stalking/Bullying

The term bullying was not defined by the act, the law merely refers to "cyberstalking" as a course of conduct directed at a specific person that would cause a reasonable person to fear; 'The provisions and the punishment contained in this law has however been misconceived by security agencies. Stalking can only be done to an individual because one must show that the act was done for the purpose of causing annoyance etc*'.*[46]

Cyberbullying entails the utilization of coercion, force, threats, and/or teasing to intimidate abuse and/or dominate another individual, via computer networks, the internet or social media platforms.[47] It may include false accusations, defamation, slander and libel, solicitation for sex, or information gathering that may be used to threaten, embarrass or harass a person.[48]

With rapid growth of internet, where several persons are members of different social media network, constantly post their information and details on the internet. People go as far as posting their locations, achievements and what they are currently engaged in. This has made people prone and vulnerable to stalking on the internet.[49]

People easily become victims of stalking as result of this and the internet have made stalking and blackmail on the increase owing to the fast rate of the internet. Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. The online stalkers usually take it further by accompanying the act with off line stalking to the extent of extorting

[46] Ibid

[47]Ali, Mohd, M. et al. "Cyberbullying Detection: An Overview". In 2018 Cyber Resilience Conference (CRC) (pp. 1-3). IEEE.

[48]Baer, M. (2010). Cyberstalking and the Internet Landscape We Have Created. *Virginia Journal of Law & Technology* Vol.15, No.154. p.153-174.

[49]*Spitzberg, Brian H.; Hoobler, Gregory (February 2002). "Cyberstalking and the technologies of interpersonal terrorism" (PDF). New Media & Society. 1. 4: 71–92.*

or killing their victims[50]. Stalkers are sometimes motivated by a dare[51]desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target. Another innovation introduced in the cybercrime act 2015 is the provisions of a law that prohibits cyber stalking which has been a menace to numerous online users.

Furthermore, Section 24 of the Act [52]prohibits the offence of Cyber stalking:

Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that;

> (a) is grossly offensive, pornographic 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 danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will 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 more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

Despite this novel innovation by the act, the law enforcement agencies are yet to secure any conviction in respect of this provision rather it has

[50]Goodno, N. H. (2007). Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws, 72 Mo. L. Rev. 125

[51]*"California Cyberstalking Laws". Shouselaw.com. Retrieved 2013-11-29. California stalking laws prohibit harassing or threatening another person to the point where that individual fears for his/her safety or the safety of his/her family.[1] When those threats or harassment are communicated via the Internet, e-mail, text messages, the phone (either cellular or a landline), a fax machine, a video message, or any other electronic device the crime is commonly referred to as "cyberstalking". ... "Cyberstalking" was officially prohibited in 1998 when the California Legislature amended Penal Code 646.9 stalking. The amendment changed the definition of "credible threat (one of the elements of the crime of stalking in California)...to include "electronically communicated" threats.*

[52] Cyber Crime (Prevention & Prohibition), Act 2015

been used as a tool of intimidation. It will never the less mean that any act that is done for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will.[53] Once it can prove that such act puts the party in fear of death, violence or bodily harm such will amount to Cyber Stalking.

IV. Cyber Terrorism

Since the motivation behind cyber terrorism typically comes to fruition before it is discovered, it might be challenging to identify it.[54]A simple definition of cyber terrorism is the use, operationalization, or targeting of computers and networks for the purpose of spreading information or inspiring fear, anxiety, or violence.

The terror attacks on the United States on September 11th, 2001 further thrust the concept of cyber terror into public discourse as the threat of giant disruptions to economy, infrastructure and national security were often discussed in depth by the media[55].

Cyber terrorism is an act of terrorism done using cyberspace, that is why it is regarded as the convergence of terrorism and cyberspace. Cyber terrorism in most case scenario can either be; 'premeditated, political, motivated attack against information, computer systems, computer programs, and data which result in the loss of lives or bodily injury, explosions, plane crashes, severe economic and financial loss and damage of critical national infrastructure.[56].The Cybercrime Act provides for protection of Critical Infrastructure[57].

[53]Dunmade Onibokun, "Penalty for Cyber stalking" available at http://www.legalnaija.com/2016/08/penalty-for-cyberstalking-in-nigeria.html accessed 10 November 2024

[54]Marsili, M. "The War on Cyberterrorism. Democracy and Security", 2019. 15(2), 172-199

[55]Gabriel Weimann,"Cyberterrorism How Real Is the Threat? Special report, UNITED STATES INSTITUTE OF PEACE(USIP)". Available at https://www.usip.org/sites/default/files/sr119.pdf accessed 9 January 2023

[56] Ibid

[57] Section 3 of the Cybercrime (Prevention & Prohibition Act, 2015

In furtherance to the issue of Cyber Terrorism, Section 18 Cyber Crime (Prevention & Prohibition) Act 2015 provides thus:

(1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.

(2) For the purpose of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended.

More often than not the term cyber terrorism has been blindly argued to include hacktivism and internet vandalism which they believe do not directly threaten the lives and livelihoods of their victims. [58] However, this proviso like others listed above is yet to be tested before any court of law in Nigeria.

v. Spamming and Phishing

Spamming is the act of sending the same message indiscriminately to a large number of recipients on the cyber space also known as the internet. This is also known as electronic junk mail or junk news group postings. Spamming are unsolicited messages and while real spam is generally email advertising or some product sent to a mailing list or social media group. The most widely recognised form of spam is email spam; the term is applied to the similar abuse on media like blogs, wiki spam and internet forum spam.

Spam can also be used to spread computer viruses, Trojan horses or other malicious software. The objective may be identified theft. However, the most common type of spamming (email scam) is phishing. Phishing is the act of sending emails to users falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email direct users to visit a website where they are asked to update

[58]Curran P, "Cyber Terrorism – How Real is the Threat?" May 04, 2016 available http://www.usip.org/publications/cyberterrorism-how-real-the-threat accessed on 20 February 2023

personal information, such as password and credit card information, social security, and bank account number which the legitimate organization already has. It is estimated that as much as 80% of all the email sent to individuals are spam emails.[59]That depressing statistic shows you just how much wastage spam creates. If you have never responded to spam (the vast majority of people don't) then you may wonder why these people bother. The truth is that even if only a tiny percentage of that bulk email gets a response they are able to turn a profit because the cost of sending it is so low.[60]

The Cybercrime Act in Section 32 prohibits and punishes the offence of spamming and the intention spreading of viruses, to wit:

(1) Any person who knowingly or intentionally engages in computer phishing shall be, liable upon conviction to 3 years imprisonment or a fine of N1, 000,000.00 or both.
(2) Any person who engages in spamming with intent to disrupt the operations of a computer be it public or private or financial institutions shall be guilty of an offence and liable upon conviction to 3 years imprisonment or a fine of N1, 000,000.00 or both.
(3) Any person who engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers shall be guilty of an offence is liable upon conviction to 3 years imprisonment or a fine of N1, 000,000.00 or both.

In reaction to the issue of spam/phishing, the Nigerian Communication Commission recently introduced guidelines to regulate bulk and unsolicited messages[61]. However, it is important to state that the act of

[59]https://www.theguardian.com/environment/green-living-blog/2010/oct/21/carbon-footprint-emailaccessed 11/02/2023

[60] Spot the Difference - Spam and Phishing Scams written by: Simon Hill edited by: M.S. Smith updated: 2/12/2010 available at http://www.brighthub.com/internet/security privacy/articles/63828.aspx

[61]NCC enforces 2442 "Do Not Disturb" Short code Available at https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=art

spamming is not necessarily illegal, until the point where people take advantage of it with malicious intent to defraud scam, steal identities, spread computer viruses etc.

VI. Child Pornography

Child pornography is a type of cybercrime that involves disseminating digital recordings (films, photos, and audio files) of children and adolescents in inappropriately scanty clothing or with no clothing on at all, as well as in poses or with language that is sexually suggestive.[62] Child Pornography involves any visual depiction involving the use of minor, one appearing to be minor, engaging in sexual explicit conduct.[63] The Child under the Cyber Crime Prevention and Prohibition Act is any child below that age of 18 years and an image of such child is actually or by simulation engaged in sexual act involving the sex organs of the child on the internet.[64]

Technological growth of the internet has disrupted and orchestrated the growth in digital pornographic content on the cyberspace.[65]Cyberspace and the pornographic matter transmitted through it have created jurisdictional challenges as a result of the lack of jurisdictional boundaries and the sheer volume of traffic that the Internet can handle, as well as the potential for anonymity have resulted in a complete lack of control over what appears on the Web at the click of a mouse button. More often than not the service providers have always been blamed for this problem[66]. Recently the rampant posting of pornographic content by children is growing on a daily basis and for the business of child pornography has been a lucrative field of crime. The distribution of

icle&id=1363:ncc-enforces-2442-qdo-not-disturbq-shortcode&catid=25&Itemid=179 accessed 20 February 2023

[62]Sae-Bae et al. "Towards Automatic Detection of Child Pornography". In 2014 IEEE International Conference on Image Processing (ICIP) (pp. 5332-5336). IEEE2014

[63]J. Grocki, "Child Pornography" https://www.justice.gov/criminal-ceos/child-pornographyaccessed 07 March 2023

[64] See S. 23(5) of the Cybercrime (Prevention & Prohibition) Act 2015

[65]Cyber Pornography Law in India- The Grey Law Decoded" March 5, 2015 this article is by Advocate Puneet Bhasin, Cyber Law Expert, Cyberjure Legal Consulting,

[66] Ibid.

child pornographic material has increased dramatically through the widespread use of the Internet. The victims are not only traumatised through the acts of sexual abuse but also victimised by the global and irrevocable distribution of the images.[67]

The Act also specifically criminalize the producer, distributor or transmitting, procuring in Section 23.[68] There are numerous acts that are criminalized with regards to child pornography and a considerable lot of these cases assert that the defendant did at least one of the accompanying: Downloading child pornographic pictures, Transferring child pornographic pictures, Sharing child pornographic pictures on the web, Preparing child pornographic pictures on a cell phone or PC, Sending child pornographic pictures through email, instant messages, or internet informing, Requesting minors to take an interest in making child pornography regularly on the web, Masterminding gatherings with a minor on the web and making a trip to the arranged area.

Moreover, casualties of child pornography experience the ill effects of the sexual abuse perpetrated upon them to deliver child pornography, yet in addition from realizing that their pictures can be exchanged and are seen by others around the world. When a picture is on the Web, it is hopeless and can keep on coursing until the end of time. The lasting record of a child's sexual abuse can modify their life for eternity. Numerous survivors of child pornography experience the ill effects of sensations of defenselessness, dread, embarrassment, and absence of control given that their pictures are accessible for others to see in ceaselessness. Where an individual didn't know that a document contained or there was likelihood that the connection contained a revolting image of a child, they won't be expected to take responsibility for child pornography.
A person would be said to have committed the offence of child pornography if he intentionally uses any computer system or network

[67] Ibid.
[68] Cybercrimes Act 2015

for producing,[69] or making available,[70] or distributing or transmitting,[71] or procuring,[72] or possessing[73] child pornography in a computer system or on computer data storage medium either for himself or another person commits an offence which is punishable by imprisonment for a term of 10 years or a fine of not less than 20 million naira. In some cases, imprisonment for a term of 5 years or a fine of not less than 10 million naira.

The *Actus Reus* of Child Pornography is using computer system or network for producing, or making available, or distributing or transmitting, or procuring, or possessing child pornography in a computer system or on computer data storage medium. An interesting legislative diction used above is the non-usage of the clause 'computer system or on a computer-data storage medium'. The Act in exchange used 'information and communication technologies.[74] This therefore acknowledges the fact that it does not matter whether the offender used a computer devise or any devise capable of data storage to contact the victim.[75] It therefore does not restrict this provision only to the use of internet. It is however arguable that text messages may fall into this category, and an offender could be prosecuted within these provisions.[76] The *Mens Rea* is intention and willfulness. It goes further to include any person who intentionally proposes, grooms or solicits, through any computer system or network to meet a child for the purpose of engaging in sexual activities with the child.[77] The second aspect of this involves where the offender for intentionally proposes, grooms or solicits,

[69] Ibid. s 23 (1) (a)
[70] Ibid s 23 (1) (b)
[71] Ibid s 23 (1) (c)
[72]Ibid s 23 (1) (d)
[73] Ibid s 23 (1) (e)
[74] E Nwelih and KC Ukaoha; Cybercrime and the Nigerian Nation-Evolving Dimensions in Benin City (2012) *International Journal of Academic Research*, 4(2)
[75] Julia Davidson and Petter Gottschalk, 'Characteristics of the Internet for criminal child sexual abuse by online groomers' (2011) Criminal Justice Studies 24.1, 23-36
[76] Virginia M. Kendall, and T. Markus Funk, Child exploitation and trafficking: Examining the global challenges and US responses (Rowman & Littlefield publishers, 2012) 21; Igor Bernik, Cybercrime and cyber warfare (John Wiley publishers 2014)
[77] Section 23 (3)

through information and communication technologies[78] to meet a child, followed by material acts leading to such a meeting, for the purpose of engaging in sexual activities with a child where: Use is made of coercion, inducement, force or threats; Abuse is made of a recognized position of trust, authority or influence over the child, including within the family; or Abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence[79]

VII. Cybersquating

Cyber Squatting originated in the late 1990s when many companies did not necessarily use the Internet for marketing purposes and did not understand the value of registering their own trademark domain names. Others saw the potential profit and registered these valuable domain names in order to sell them back to the companies[80]. As of 2012, a total of 2,884 complaints have been filed involving "Cybersquatting. Cyber Squatting refers to illegal domain name registration or use. Cybersquatting can have a few different variations, but its primary purpose is to steal or misspell a domain name in order to profit from an increase in website visits, which otherwise would not be possible. Trademark or copyright holders may neglect to reregister their domain names, and by forgetting this important update, cyber squatters can easily steal domain names. Cyber Squatting also includes advertisers who mimic domain names that are similar to popular, highly trafficked websites. Cybersquatting is one of several types of cybercrimes.[81]

Section 25 of the Act[82] provides*:*

> *(1) Any person who, intentionally takes or makes use of a name, business name, trademark, domain or*

[78] Abdullahi Y. Shehu; Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession (2014) Online Journal of Social Sciences Research, 3(7), 169-180

[79] Section 23 (3) (b)

[80]creatly. (2015, November 20). "*What is Cybersquatting and What You Can do to Prevent It*." Retrieved from creately.com: http://creately.com/blog/marketing/what-is-cybersquatting-prevention-steps/accesssed 20/02/2023

[81]Meaning of Cybersquating, available at https://www.techopedia.com/definition/2393/cybersquatting accessed 20/02/2023

[82] Cybercrimes Act, 2015

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, and for the purpose Of interfering with their use by the owner, registrant or legitimate prior user, commits an Offence under this Act and shall be Liable on conviction to imprisonment for a term of not more than 2 years or a fine of not more than N5,000,000.00 or both.[83]

VIII. **ATM/POS Manipulation:** This involves the manipulation of Automated Teller Machines or Point of Sale Terminals by a person in order to defraud another. As noted by the Cybercrimes Act, it is not uncommon in some circumstances for staff of financial institutions such as banks, to connive with criminal elements to perpetrate such an offence.

---

[83] *(2) In awarding any penalty against an offender under this section, a court shall have regard to the following ---*
(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 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.
(3) 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.

Section30(1)(2) of the Act[84] defines the offence of ATM/POS Manipulation and provides for imprisonment of up to five years and a fine of N5,000,000 in an ordinary case and up to seven years' imprisonment for staff of financial institutions who connive with others to carry out this act.[85]

5.0 Conclusion and Recommendation

Understanding the various aspect of cybercrimes, concepts and term will aid not just the security agencies and authorities in fighting the menace which has become a cankerworm eating up every fabric of Nigerian digital world, it will also help the individuals and corporate organizations who are the targets of these attack taking caution towards not falling victim. Understanding the dynamics of these attacks will go a long way in winning the cyber security way. The methodologies used by perpetrators have definitely changed owing to the massive deployment of telecommunication infrastructure thereby taking advantage of the vulnerability of the financial institutions in Nigeria. Stakeholders in the criminal justice sector must implement the Cybercrime Act 2015 to the later, promote international collaboration and invest in Cybersecurity education and awareness.

[84] Ibid

[85] D.G Ashonibare (2021) Impacts and Challenges of Prosecuting Cyber crime in Nigeria Section on Legal Practice Law Journal (SLP LAW JOURNAL) Nigerian Bar Association Vol. 7 June, 2021