Cybercrime and Cyber Law in Nigeria: An Overview of Challenges and Way Forward

Yakubu Aliyu Ibrahim
Department of Computer Science, Bingham University Karu, Nigerian
yakubu.ibrahim@binghamuni.edu.ng
0000-0002-5529-5243

Silas Ageebee Faki
Department of Computer Science, Bingham University Karu, Nigeria
faki.silas@binghamuni.edu.ng
0000-0003-1531-0119

Musa Yusuf
Department of Computer Science, Bingham University Karu, Nigeria
yusufmusa@binghamuni.edu.ng
0000-0002-7893-9531

Adamu Sulaiman Usman
Department of Computer Science, Bingham University Karu, Nigeria
adodass@binghamuni.edu.ng
0000-0002-4917-1455

Adelaiye Oluwasegun Ishaya
Department of Computer Science, Bingham University Karu, Nigeria
oluwasegun.adelaiye@binghamuni.edu.ng
0000-0002-4193-5641

Ann Hassan Brijik
Department of Computer Science Bingham University Karu, Nigeria
annebjk@gmail.com
0000-0001-6718-1078

Joseph Oladele Aremu
Department of Computer Science Bingham University Karu, Nigeria
josepharemu8@gmail.com

Comfort Ayenopwa George
ICT Unit, Bingham University Karu, Nigeria
comfort@binghamuni.edu.ng

***Abstract* - The increasing use of computers, mobile devices, and the Internet in recent times has created new ways to commit cybercrime. In Nigeria today a number of internet-enabled crimes are committed daily in various forms such as identity theft, identity theft, hacking, phishing emails, spam, pornography, cyberbullying, scams, hacking, etc. Cybercrime is a threat to many organizations and individuals accessing the Internet through their computers or mobile devices. As a result, the study points to the effects of the Internet turning the world into a global village, which has become a major challenge for law enforcement and judicial officers in taking action against them. Cybercrime legislation is part of the federal government's response to Internet crime, but law enforcement has not been enough to accommodate the complexity of technological developments. One of the earliest acts against cybercrime in Nigeria was the Cybercrime Prevention and Prevention Act 2015, enacted by the Parliament of the Federal Republic of Nigeria. The law's specific objectives include providing an effective legal, regulatory, and institutional framework for the prohibition, detection, prevention, and prosecution of cybercrime in Nigeria however, existing Nigerian laws present ambiguities that can be exploited by cybercriminals. The law aims to ensure the protection of critical national information infrastructure, promote cybersecurity, and protect computers and networks, electronic communications, data and computer programs, intellectual property, and privacy rights. This document reviews the provisions of the law, identifies its challenges, and proposes a path to online law enforcement not only for Nigeria but for other African countries as well.**

Keywords- Cybercrime, Cybersecurity, Computer security, information security, Internet, Nigeria.

I. INTRODUCTION

Today, the Internet allows us to send and receive all kinds of information via email, but people are not sure how secure the information sent to others is without data leakage. In recent years, the use of computers and the internet for cybercrime has increased rapidly in Nigeria. However, Information Communication and Technology (ICT) and many new technologies are changing our lifestyles and behaviors. In the same vein, these new technologies do not prevent system hackers from gaining unauthorized access to our personal data. Therefore, cybercrime is increasing day by day. Today, the use of the Internet for social media chats and other online commerce is increasing day by day. Field computers, therefore, require a high degree of security to ensure authorized access to online transactions. In this context, cyber security has become an important issue [1,13].

The scope of cybersecurity includes various fields such as cyberspace as well as information security in the ICT industry [1]. Also, modern technologies such as cloud computing, mobile computing, e-commerce, and Internet banking require high levels of security. This is because these information technologies contain sensitive information about individuals, which makes security very important. Improving cybersecurity, preventing cybercrime, and enforcing cyber laws are essential to prevent unauthorized access to information infrastructure [1]. Making the Internet safer for users and protecting against cybercrime has become an integral part of national development and government policy. Combating cybercrime of all kinds requires a comprehensive and safer approach. Technological measures alone cannot prevent cybercrime, so it is important and necessary for law enforcement to be able to effectively investigate and prosecute cybercriminals [2]. Many countries and governments, especially the Federal Government of Nigeria, now have strict cybercrime laws to prevent loss of sensitive information [3]. The Cybercrimes (prohibition, prevention, etc.) Act 2015 3 section 419 Criminal Code Act 4 Section 2 Money Laundering (Prohibition) Act (MLA) 2011 Advance Fee Fraud Act5 , Nigeria Data Protection Regulation 2019 and Nigerian Communications Act (NCA) deals with cybercrime among others in Nigeria [3]. However, the focus of this article is the Act which is established primarily to curb cybercrimes in Nigeria. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (“the Act”)

The Act has the objective of providing an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria.

The Act also seeks to promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights [3]. The paper presents different types of cybercrime and the prospects for effective cyber-law enforcement not only in Nigeria but also in other African countries.

II. Literature Review

The rapid growth and widespread acceptance of Internet usage has increased Internet security threats. Several cyber-crimes take place in Nigeria every day in many forms, including identity theft, hacking, fraudulent emails, spam, pornography, cyber harassment, phishing, Automated Teller Machine (ATM) spoofing, piracy, and more [2]. Cybercrime threatens a wide variety of organizations and individuals who connect to the Internet through mobile devices and computer systems. The prevalence of cybercrime around the world, and especially in Nigeria, poses a major challenge to law enforcement and the judicial system, and it should not be overstated [2]. Nigerians spend a lot of time using mobile devices and computers online. As computer and internet usage increases, so does cybercrime in Nigeria. It has therefore become necessary to combat these seemingly uncontrollable phenomena that have led to Nigeria's cyber legislation.

Cyberlaw acts as the guardian of cyberspace and prevents cybercrime by cybercriminals. The federal government of Nigeria is working to enact new laws and enforce regulations to combat illegal online activity. The Cybercrime (Prohibition and Prevention) Act 2015 has had a significant impact on Nigeria's cyber law. This law creates a comprehensive legal, regulatory, and institutional framework in Nigeria to prohibit, prevent, detect, prosecute, and punish all cybercrime [3]. The law also promotes cybersecurity and protects computer systems and networks, electronic communications, computer data and programs, intellectual property rights, and privacy, and protects infrastructure. important national information. Nigerians are well known at home and abroad as experts in causing cybercrime. The number of Nigerians arrested for illegal internet activities broadcast by television stations is much higher than that of citizens of other countries [2]. However, the Internet's contribution to Nigeria's development has had a positive impact on various sectors of the country. However, sectors such as banking, e-commerce, education, and other organizations still struggle with the effects of cybercrime [2].

The Economic and Financial Crimes Commission (EFCC) Formal Executive Chairman Abdulrashed Bawa said the rise in cybercrime was alarming and the rate calls for concern, speaking at a cybercafe conference in Nigeria in September 2021. He said 80% of EFCC convictions to date have been related to cybercrime. The get-rich-quick syndrome is often attributed to cybercrime in Nigeria, but there are other factors such as unemployment, poverty, declining social morals and values, peer pressure, lack of cyber awareness, and lenient penalties for cybercrime. Other factors contribute to the increase in unwanted crime in cybercrime. In today's Nigeria, most parents don't care about their children's academic performance in higher education institutions. Instead, they should focus on graduating first in their class and wondering why they drive around in the latest cars with no clear source of income. Some parents even refer children involved in this crime to an herbalist to help prepare spells that enable the crime. The concept of cybercrime is rapidly changing its face and meaning in Nigeria and has just spawned a new phenomenon called Yahoo Plus [2]. Yahoo Plus in simpler terms is an advanced form of Yahoo Yahoo that uses traditional amulets, most commonly human body parts, to defraud victims. This Yahoo Plus is widely used by online scammers who are unable to withdraw money for illegal activities. Young women are the primary victims of unpleasant incidents on Yahoo Plus these days.

III. The Phenomenon of Cybercrime

Cybercrime is a word often for any illegal activity that uses a computer or the Internet as a primary vehicle for unauthorized system access or identity theft. The United State (U.S.) Department of Justice has expanded the definition of cybercrime to include any illegal activity that uses computers to store evidence. The growing list of cybercrime includes computer-assisted crimes such as network intrusions and spreading computer viruses while existing computer-assisted crimes such as identity theft, stalking, bullying, and terrorism Subspecies are also included, which is a big problem for people and society. nation [3]. Most organizations in Nigeria now use the Internet to conduct transactions, serving as a tool that can contribute to national and socio-economic development. Therefore, increasing the cybersecurity awareness of employees and users is a mandatory requirement. Adopting a cybersecurity policy is one of the standard practices that enable nations to build secure cyberspace. Above all, the Federal Government of Nigeria has developed cybersecurity policies and strategies to enhance business success in Nigeria through digitization [5].

IV. Types of Cybercrimes

A. Cyberterrorism

A cyberterrorist is someone who launches an attack against a government or organization to modify or access information stored on a computer or its network [6].

B. Malware

Malware is viruses, Trojan horses, worms, and other software that enter your computer without your knowledge [6].

C. Cyberstalking

Cyberstalking is essentially the use of the Internet to repeatedly harass another person [6].

D. Spam/Phishing

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately [6].

E. Fraud-Identity Theft

Fraud is the criminal act of someone impersonating another person to obtain important information about someone [6].

F. Logic Bomb

A typical logic bomb tells a computer to execute a set of instructions at a specific date and time or under specific conditions [6].

G. Email and SMS Spoofing

Spoofing is a technique that allows attackers to send emails and text her messages (SMS) to users, which can lead to bank account and identity theft [6].

H. Password Sniffing

A password sniffer can monitor all traffic within your network area [6, 12].

V. CAUSES OF CYBERCRIMES IN NIGERIA

A. Unemployment

One of the main causes of cybercrime in Nigeria is unemployment. Over 20 million graduates are known to be unemployed in the country. This automatically increased the frequency with which they engaged in criminal activity to ensure their survival [3].

B. The pursuit of get-rich-quick schemes

This is another source of cybercrime in Nigeria. Today's young people are very greedy and try to catch up with the rich instead of starting small [3].

C. Lack of strong cyber law

This also encourages perpetrators to commit more crimes, knowing that they may always go undetected. Our government needs to have tougher laws and be able to enforce those laws so that criminals go unpunished. Legal documents may sometimes have ambiguities or require interpretation, which can create uncertainty in the application and enforcement of the laws. Clear and specific definitions are essential to avoid misinterpretations and potential legal loopholes [3].

D. Poor Personal Computer (PC) Security

Some PCs lack proper or adequate security controls, making them vulnerable to criminal activity and theft of information on the PC [3].

VI. CYBER LAW IN NIGERIA

Cyber law is the law that deals with crime using the Internet. The study believes that while the EFCC deals with financial and white-collar crime, criminal law has all the powers to effectively combat cybercrime [6].

A. The Nigeria Criminal Code Act 1990:

The Criminal Law Act 1990 makes all forms of theft of money a crime and a crime punishable by law. Cybercrime is not mentioned in law, but it is a form of theft punishable by criminal law. The law's most prominent provisions deal with the acquisition of property through false pretenses and fraud. The specific provisions relating to cybercrime are Article 419, and Article 418 provides the definition of criminal offenses under this Act. Section 418 states that any representation of fact made by word, document, or deed, whether past or present, is in fact false, and the person making it knows It states that what you don't believe to be true is pretending to be false [6].

B. The Economic and Financial Crime Commission Act, 2004:

The Economic and Financial Crimes Commission Act 2004 is a law of the Commonwealth of Nigeria and provides the legal framework for the establishment of commissions. The main duties of the committee are [7]:

1) Investigate all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal fee transfers, futures market fraud, negotiable instrument transfer fraud, card fraud computer credit, and contract fraud, among other crimes;
2) Coordinate and enforce all economic and financial crime laws and enforcement functions delegated to another person or agency;
3) review and investigate all reported cases of economic and financial crime to identify the individuals, legal entities or groups involved;
4) undertakes research and similar work to determine the manifestation, extent, scale, and impact of economic and financial crime and advise governments on appropriate responses to combat it;
5) takeover, monitor, control, and coordinate all responsibilities, functions, and activities in connection with the ongoing investigation and prosecution of all offenses related to or in connection with economic and financial crimes, in consultation with the Federal Attorney General;
6) coordination of all existing Economic and Financial Crimes Investigation Units, in Nigeria.

C. Advance Fee Fraud and Related Offences Act 2006:

According to Section 23 of the Advance Fraud Act (Federal Law of Nigeria, 2006). Pretend to be false means a statement, intentionally or recklessly, made orally, in writing or in attitude, of an event or law, past or present, that is false on fact or law, and the person who knows the truth is false or does not believe it to be true. Section 383 sub-section 1 of the Nigerian Criminal Code states: A person who fraudulently takes something that could be stolen, or fraudulently converts it for his own use or for any other person's use of anything that could be stolen, is considered to be stolen.

Economic crime is defined by law as non-violent crimes and illegal activities carried out with the aim of making money illegally, individually, in groups or in an organized manner, thereby violating existing laws. government regulation of economic activities. all forms of fraud, drug trafficking, money laundering, embezzlement, corruption, robbery and all forms of corruption, illegal arms trade, smuggling, human trafficking and child labor, oil bunkers illegal mining and mining, tax evasion, exchange fraud including counterfeit money, theft of intellectual and political property, open market abuse, dumping of hazardous wastes and prohibited goods [6]. Currently, this is the only law in Nigeria dealing with cybercrime issues. It is only intended for internet service providers and cyber cafe regulations and does not address widespread computer misuse or cybercrime [6].

D. Cybercrime Act 2015 of Nigeria

Offenses mentioned in the law include: Misleading electronic messages, cybersquatting, operating unregistered cybercafes, breach of confidentiality and data/end-user privacy policies, interception of electronic funds transfers, interception of emails, data tampering and hacking, electronic fraud, ATMs/payment terminal (point of sale/POS) tampering and hacking, online breaches of national data infrastructure, piracy, online/privacy violations [3].

VII. Enforcement of Cyber Laws as parts of the Solution to Cybercrimes

Extending the rule of law to cyberspace is an important step in creating a trusted environment for citizens and businesses. As this extension is still a work in progress, today's organizations must first and foremost protect their own systems and information from attack, whether external or internal. They can only depend on the deterrent that effective law enforcement can provide. To ensure this self-protection, organizations should focus on implementing cybersecurity plans that address people, process, and technology issues. Companies should educate their employees about security practices, develop rigorous plans for handling sensitive data, records, and transactions, and organize robust security technologies such as firewalls, antivirus software, intrusion detection tools, and authentication services. must provide resources for integration across computer systems [6].

VIII. The importance of cyber law in Nigeria

It sets the parameters for all actions and reactions in cyberspace, ensures that all online transactions are secure, ensures that all internet activity is monitored by cyber law enforcement, and protects all data and data of individuals, organizations, and governments. Protecting property helps eliminate due diligence checks. All activities and responses that take place in cyberspace have a legal component, maintain a database of all electronic records, and contribute to the establishment of electronic governance [6].

IX. The Way Forward to Tackling Cybercrime and Enforcing Cyber Law in Nigeria

Cybercrime has caused so much damage to Nigeria's international reputation that it is imperative to find strategies to eliminate it. The following suggestions will help our society gradually eliminate the threat of cybercrime and restore Nigeria's tarnished reputation [8].

A. Job offer

As the saying goes, lazy hands are the devil's workshop. Due to the lack of alternative employment, the majority of young people resort to cybercrime. Due to the large number of unemployed youth in Nigeria, most of them rely on cybercrime for their livelihood. Young people may not feel the need to engage in criminal activity if decent jobs and employment opportunities are available [8].

B. A renewed focus on the positive application of cyber skills:

Another way to combat cybercrime is to train young people how to use their computer skills for good and bad, such as committing fraud online. Training in digital skills such as coding, computer programming, and cybersecurity should be offered by both governmental and non-governmental organizations for cyber enthusiasts [8].

C. Severe penalties for cheaters

Another reason many young people turn to cybercrime is that they are fully aware of the lighter penalties associated with cybercrime. In most cases, these cybercriminals are sentenced to several months in prison after being caught and prosecuted, and most often come with a choice of an amount, which the scammer steals from the victim. cannot be capped at 20% of the total amount [8].

D. Adequate education on cybercrime

Parents, religious leaders, and institutions of higher education all have a role to play in educating adolescents about the impact of cybercrime. It must be discouraged through parental guidance, religious sermons, and academic rules and regulations. Apart from the above tips, society as a whole also has a role to play in minimizing the pressure on the younger generation to get rich while they are young. Society and the media, especially with the advent of media, have helped paint people in their 20s and 30s who don't own a home or a car as failures. For these and other reasons, the pressure placed on young people to engage in all forms of quick money-makings, such as cybercrime, will continue to grow [8].

X. Enforcement Agency for Cyber Law in Nigeria

The Office of the National Security Advisor serves as a coordinating body for the security and enforcement agencies. The Federal Attorney General will strengthen and improve Nigeria's existing legal framework on cybercrime [9]. This legal and enforcement network is known as the Cybercrime Advisory Board and is made up of, among others, the following members: The Nigerian Customs Service, The Nigerian Communications Commission, The Nigerian Data Protection Bureau, The Nigerian Identity Management Commission, The Economic and Financial Crimes Commission, The Defence Headquarters, The Defence Intelligence Agency, The Nigerian Security and Civil Defence Corps, The Nigerian Intelligence Agency, The Independent Corrupt Practices Commission, The Central Bank of Nigeria, The Nigerian Police Force, The Department of State Security, The Federal Ministry of Trade and Investment, The Federal Ministry of Foreign Affairs, The Federal Ministry of Justice, The Federal Ministry of Finance and The Office of The National Security Adviser [10].

XI. SURVEY RESULTS FOR CYBERCRIME IN NIGERIA

As per specialists in the online protection space, cybercrime was developing far and wide while measures to reduce it had neglected to light a flash. They expressed that cyberattacks were not selective as they impacted both rich and poor, old and youthful [11]. The Main Innovation Official, NJALO.NG, Chukwuemeka Orjiani, said the country's network safety space had not been viewed in a serious way before now, contending

that to this end the danger rotted. He expressed, "The country's network safety hasn't actually been viewed in a serious way. Truly our kin have not found it something intense on the grounds that this is another danger of Web security. "However, the truth of the matter is consistently, individuals lose their resources on the web. Individuals lose cash, and passwords get hacked. Individuals lose their data online as well. On a daily, people are hit, and companies are hit." He added that the level of sophistication of cybercriminals was levelling up as cyberattacks were becoming harder to spot. According to him, information regarding cyber threats was still scarce [11]. Orjiani further said, "The funny thing is cyberattacks do not discriminate. A cyberattack can affect very poor homes as well as rich ones. These guys can mine people's data, get it, and clear accounts. "People are not well informed on these issues. Social engineering is a major vulnerability hackers prey on. They prey on the intelligence of people." As of late, thought Russian aggressors hacked Bet9ja, locking out for clients of the firm from their records. While the firm had the option to get back its site sooner or later, a lot more organizations are confronted with cyberattacks every day and can do hardly anything about it. As indicated by a new Designated spot Exploration's Statement Insight Report, Nigerian organizations experienced 2,308 assaults across all businesses areas week after week. The report expressed that north of a six-month time span, 62% of Nigeria's organizations succumbed to Remote Code Execution assaults which permitted cybercriminals to oversee gadgets and the confidential information put away on them. It added that email was recorded as the beginning point for 60% of cyberattacks throughout a time span of time as it worked as a vector for the conveyance of pernicious documents. The report projected that 2022 would see an expansion in the weaponization of deep fake advancements by cybercriminals to make counterfeit news crusades as a feature of phishing assaults. A report by Sophos, a Unified Realm based network protection arrangements firm, said 71% of Nigerian associations were hit by ransomware assaults in 2021 [11].

The Pioneer, E86 Restricted, OluGbenga Odeyemi, expressed associations in the country were concealing the cyberattacks and attempting to hide them away from plain view in an endeavor not to affect client and financial backer certainty adversely. As indicated by him, it was difficult to precisely appraise the financial expense of the assaults in light of their underreporting. He expressed that as per the NSA, the yearly misfortunes to cybercrime were assessed at N127bn in 2017 and $649m in 2019 for each a report. He said, "Most associations just concealment the wreck and continue on. This is finished to guarantee they don't adversely affect the certainty they have acquired with their clients and inside their market [11]. " I additionally figure most associations do this to conceal their own failures, particularly the people who have not put resources into the security of their framework." As per him, Nigeria's the internet was improving, despite the fact that it required more experts and mindfulness. He expressed that Coronavirus didn't be guaranteed to expand the degree of refinement of cyberattacks as put stock in many quarters. He added, "In any case, with additional organizations bringing their tasks on the web, it is normal that the rate at which organizations are gone after will increment. there were a great deal of strategy issues hampering network protection in the country. He included that the country's dependence restrictive programming was additionally restricting its capacity to handle cyberattacks. He said, "There is likewise a ton of strategy issues we want to check out. We have a network safety organization in Nigeria, however the inquiry is, the reason they can't oversee that space? " Many variables are answerable for that failure. One, Nigeria is pretty much predominantly participated in the obtaining of exclusive programming and this product is, more often than not, dominated by the man in the center remotely and the man in the center inside. " Assuming you take a gander at the greater part of the servers that have been hacked, the greater part are exclusive. In any case, open source has been, somewhat, rough since programming determines its prosperity and fortitude from extraordinary root stages separated from Microsoft that has truly turned a few things." Uwaje expressed that this was not unconventional to Nigeria. He made sense of that cyberattacks were generally started by the man in the center who was the ruin originator. As per him, the man in the center was significantly externalized as an element however there was a need to investigate the assimilated man in the center, the insider. He said the insider sustained around 72% of assaults. He expressed that there were near about a portion of 1,000,000 digital dangers at the same time occurring all over the planet each moment and individuals that were not state-of-the-art and didn't have the comparable devices consequently turned out to be weaknesses. He added the country required an organization for network protection research on the grounds that these dangers were tormenting everybody. He said there was a should be miles in front of the gatecrashers and the method for doing this was to have a decent exploration stage. Uwaje further said, "The EU has been attempting to diminish cyberattacks. Furthermore, one of the manners in which they've been doing this is to guarantee that all administration stages work on open-source programming, not restrictive. Also, this is working for them. "Cyberattacks are generally arbitrary.

Nigeria is powerless in light of the fact that we are as yet connected inside the IPV4 space name. The world is moving to IPV6, the weakness of IPV4 is that occasionally when an assault comes in, you are don't know of the source in light of the fact that the addresses can be parted to the force of 4, 8, 16, and then some. " A similar IP is working. Assuming that IP is domiciled likely in Nigeria, somebody in Mexico can utilize it to hack into the Nigerian climate. We want to relocate to IPV6. The US has provided all its organization with a cutoff time of 2025 to relocate. The IPV4 has progressively been depleted as far as the Web address layer." In Africa, the risk of cybercrimes kept a gigantic ascent in the initial a half year of 2022, "with phishing and tricks hitting 438% and 174 percent in Kenya and Nigeria, separately." The EFCC formal executive chairman, Abdulrasheed Bawa, uncovered this when he showed up before the Senate Council on Enemy of Defilement on Thursday. His appearance before the board was to protect the organization's 2022/2023 financial plan. The spending plan safeguard was held away from public scrutiny and Mr. Bawa tended to columnists a while later. The indicted people, he said, are generally Nigerian youth who ought to help the commission to free the country of cybercrimes and other crimes related with the internet. While he said the exercises of cybercriminals are spoiling the appearance of the country in the worldwide field, Mr. Bawa made sense of that it is the Commission's command

to battle cybercrime, battle advance charge extortion and work in congruity with the law [7]. " He pleaded with the youth to quit doing such things during this season of progress of the nation building, as far as government endeavors to see that the economy is in the groove again [11]."

XII. CONCLUSION

The paper concludes that the rate of ccybercrime in Nigeria has taken on many facets over the last few years, with internet fraud spiking across the country. Hence the need for Federal government to enforce the cyber law through different security agents in the country. However, while complaining about unemployment and depression in this country, men and women of all ages have duped the public and used illegal trade only as an excuse to export to the international community. But don't let unemployment or the economic downturn be an excuse for fraud. The skills used to commit these evil deeds can be used for good, legitimate, and decent jobs that are of greater benefit to the nation as a whole. Federal and state governments, therefore, need to pay close attention to the country's low employment rates by helping young people not only improve their lives but develop the skills to become employers. Soft loans need to create more jobs and businesses to deter citizens from becoming embroiled in all kinds of cybercrime. Governments also need to strengthen law enforcement by building capacity to address emerging trends in cybercrime.

REFERENCES

[1] Mayiwa Imue (2020) The jurisdiction Challenge in the enforcement of cybercrime laws in Nigeria, Africa Law Practice Nigeria Company, PP 1-3.

[2] Omodunbi B. A., Odiase P. O., Olaniyan O. M. & Esan A. O. (2016) Cybercrimes in Nigeria: Analysis, Detection and Prevention, FUOYE Journal of Engineering and Technology, Volume 1, Issue 1, September 2016, PP. 37-41.

[3] Cybercrimes Act 2015) Cybercrimes (Prohibition, Prevention, etc) Act, 2015, Cyber Law Enacted by the National Assembly of the Federal Republic of Nigeria, PP. 1-43.

[4] Nikhita Reddy G. & Ugander Reddy G. J. (2020) A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies, PP 1-5.

[5] Ikuero F. E. (2022) Preliminary Review of Cybersecurity Coordination in Nigeria, Nigerian Journal of Technology (NIJOTECH) Vol. 41, No. 3, May, 2022, pp. 521-526.

[6] Maitanmi Olusola, Ogunlere Samson, Ayinde Semiu and Adekunle Yinka (2013) Cyber Crimes and Cyber Laws in Nigeria, The International Journal of Engineering and Science (IJES), Vol. 2, Issue 4, PP. 19-25.

[7] EFCC available at www.efccnigeria.org/efcc_homepage.../establishment_act_2004.pdf (2004)

[8] Hassan A. B., Lass F. D. & Makinde J. (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN Journal of Science and Technology, VOL. 2(7), pp. 626 – 631.

[9] Advance Fee Fraud and Other Fraud Related Offences Act 2006.

[10] UWADIA Francis and ETI I. Friday, (2018) Cyber Security in Nigeria: Issues, Challenges and Way Forward, International Research Journal of Advanced Engineering and Science, Volume 3, Issue 2, pp. 351-354.

[11] Temitayo Jadesola (2022) How Nigeria can curb rising cyberattacks, The PUNCH Newspaper of 31st May 2022, pp. 4-5.

[12] Y. Musa, A. Silas, and I. Oluwasegun, "Honey Algorithm for Securing and Identifying Hackers in a Pervasive Environment," Nile Journal of Communication and Computer Science, vol. 5, pp. 2-9, 2023.

[13] Adelaiye, O. I., Ajibola, A., & Yusuf, M. Detecting Lateral Movement in a Network for Combating Advanced Persistent Threats.