AN ANALYSIS OF THE SOCIO-ECONOMIC RELEVANCE OF THE CYBERCRIMES PROHIBITION AND PREVENTION ACT 2015

ABSTRACT
The rapid evolution of technology has brought about numerous benefits, but also poses significant challenges, particularly in the realm of cyber security. The Cybercrimes (Prohibition and Prevention) Act of Nigeria which was enacted in 2015 had the principal aim of combating the escalating threat of cybercrime in Nigeria. This article examines the socio-economic relevance of the legislation in the 21st century. It also engages the provisions of the Act, its implementation, and enforcement as well as highlighting the strengths and weaknesses in the legislation. This article further explores the impact of cybercrime on Nigeria's economy, society, and political landscape, including increased investor confidence, enhanced security, and improved trust in digital transactions. The findings stressed the need for a more comprehensive approach to addressing the evolving nature of cyber-criminality which involves the creation of public awareness, the need for effective implementation, enhancing confidence of the investors as well as enhancing international cooperation. In conclusion, this research emphasized the importance of a balanced approach that considered the economic and social implications of cybercrime, whilst protecting human rights as well as ensuring digital inclusion.

1.0 INTRODUCTION
The emergence of Information and Communication Technology ("ICT") has significantly impacted the old and usual ways of doing things, by providing an alternative, easy, and efficient means of interaction over a network of computers in real-time for people all around the world. However, the growth of ICT continues to be negatively affected by cybercrime, and this has negatively impacted the socio-economic well-being of nations, companies, and individuals in unimaginable ways. The first incidence of cybercrime occurred in 1834 when a group of thieves intending to steal financial market information hacked into the French Telegram system.[1] Also in 1981 at the beginning stage of the ICT, Lan Murphy hacked into an internal clock that monitored the billing rate of an American Telephone Company known as AT & T's. He intended to allow users of the Telephone to make discounted calls at peak times. He was later tried and convicted for a felony, but not for a "cybercrime" related offence by the Court of Common Pleas in Montgomery, Pennsylvania.[2] By 1986, Congress had passed the Computer Fraud and Abuse Act into law, prohibiting unauthorized access to computer, which led to the conviction of a Harvard University graduate in 1988 known as Rover Tappan Morris. He hacked into a computer at the Massachusetts Institute of Technology (MIT) to release a harmful computer program leaving over 60,000 computers connected to the internet affected.[3] In the face of increasingly sophisticated attacks on computers and computer networks, arguably all countries of the world have either modified or enacted separate laws to expressly prohibit cybercrime activities. In Nigeria, the Cybercrimes (Prohibition & Prevention) Act 2015 was passed and signed into law by President Goodluck Jonathan, as a means of cybercrime control. It is an independent legislation, distinct from existing criminal laws in the country to among other things; prohibit and prevent unauthorized access to protected computers.[4] The Act failed to define cybercrime, but according to Merriam-Webster.com, cybercrime is any criminal activity committed using a computer to illegally access, transmit, or manipulate data.[5] In this

* Ejike Francis Okaphor PhD, Senior Lecturer, Department of Clinical Legal Education, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. E-mail: ef.okaphor@unizik.edu.ng
** O S Ngwuta Esq, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, oforbuikengwuta@gmail.com; +234 806 8429 319
*** Nkiruka Edith Okaphor LLM, A private legal practitioner and an Associate in FXE Legal (Solicitors & Advocates) Plot 13 Thrillers Road, Awka, Anambra State, Nigeria; Email: edithnkiruka14@gmail.com

[1] Ann Lindberg, "Security Profile of Lan Authur Murphy", St. Petersburg Times (2005) <https://attrition.org/errata/charlatan/ian_murphy/threat_profile/> accessed 14th May 2022
[2] Supra, 1
[3] Morris Worm, "Famous Cases and Criminals", Federal Bureau of Investigation <https://www.fbi.gov/history/famous-cases/morris-worm> accessed 24th May 2022
[4] Cybercrime (Prohibition & Prevention) Act 2015 accessible at: <https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf> accessed 24th May 2022
[5] Merriam-Webster Dictionary <https://www.merriam-webster.com/dictionary/cybercrime> accessed 24th May 2022

regard, a computer can either be an object of the attack or used to perpetrate the act.[6] The Act appears to have utmost relevance, especially with a growing number of internet users in Nigeria and the consequent increase in the rate of cybercrimes. This research explores the social and economic relevance of the Cybercrime Act 2015 and further makes recommendations for its full implementation.

2.0 CRIME AND CRIME CONTROL MECHANISM

The term 'crime' has a wide range of meanings, and has no generally accepted definition due to the complexity of its definition. The definition of crime differs according to the school of thought of each scholar. Scholars who belong to the Positive school perceive crime as an act or omission that the ruler prescribes as wrong and enforced through penal sanctions. The Liberalists define it as a limitation to the rights, freedom, and liberty of a person while the Moralists differ by portraying crimes from the angle of morality. On the other hand, crime control refers to the measures for preventing and controlling crimes in society, to meet the aims and objectives for the establishment of criminal laws. Crime control methods are broadly categorized into formal and informal crime control. The informal crime control method relies on the efforts, opinions, and sanctions of social and moral institutions such as the family unit, churches, and peer groups to control crimes in society. The formal crime control method places heavy reliance on the law and government institutions established by law to detect, prosecute, and punish offenders. It is argued that a crime is an act or omission which is inimical to the interests of the state and must be prescribed as wrong and prohibited with a punishment attached under a written law in force.[7] In Nigeria, criminal law is two-fold: the Criminal Code applies to the Southern States whereas the Penal Code applies to the North. Both of them are written laws that have prescribed various acts and omissions as offences. Thus, both laws use "offence" in place of "crime" to denote legal wrongs. The Criminal Code defines an offence to mean an act or omission which renders the person doing the act or making the omission liable to punishment under the Code or any Act or Law.[8] Equally, section 4(2) of the Penal Code also incriminates acts and omissions to the extent that the "doing of a thing" or the "refusal to do it" may constitute a crime. Criminal law aims to prohibit acts deemed inimical to the interests of the State, the citizens, and their property. In other words, criminal law ensures orderliness in society and ensures adequate protection for citizen's lives, property, and social interactions.

3.0 THE CYBERCRIMES (PROHIBITION AND PREVENTION) ACT 2015

The Cybercrimes (Prohibition & Prevention) Act 2015 was enacted as a response to the growing trend of dangerous criminal activities being perpetrated by cybercriminals all over the world, which Nigeria is not left out. In 2014, a study conducted by the Canada Security System ("CSIS") showed that the world lost about $500 billion to cybercrimes, standing at 0.75% of global income.[9] The Chief Strategy Officer of Deloitte West Africa reported in 2021 that Nigeria lost about #5.5 trillion in 10 years to cybercrime.[10] Cybercrime has wide-reaching negative implications on the government, individuals, and businesses operating in the country, especially as most businesses are beginning to introduce innovative ways of doing business such as daily business management and operations, finance structuring, storage of important documents, and customers' data. Also, research has shown that the major targets of cybercriminals are the government, business entities, and financial institutions.[11] Private individuals are also subjects of attacks. Cybercriminals gain unauthorized access to private data of people to amongst other things; impersonate, and sell such data for profit, steal private information for illegal use, and financial fraud. The Cybercrime Act was elaborate in its provisions to extend activities that constitute

[6] Financier Worldwide, The Nigerian Cybercrime Act 2015 and its implications for financial institutions and service Providers (2016) <https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its-implications-for-financial-institutions-and-service-providers#.YozNrqjMLIU> accessed 24th May 2022

[7] Section 36(12) Constitution of the Federal Republic of Nigeria 1999

[8] Section 2 Criminal Code 2004

[9] Ugo Aliogo, "West Africa: 'Nigeria Lost N5.5 Trillion to Cybercrimes in 10 Years" YallaAfrica (2021) <https://allafrica.com/stories/202104260948.html#:~:text=The%20Chief%20Strategy%20Officer%2C%20Deloitte,and%20cybercrimes%20in%2010%20years.> accessed 24th May 2022

[10] Bode Adewumi, |Nigeria Lost N5.5 Trn To Fraud, Cybercrimes In 10 Years" Nigerian Tribune (2021) <https://tribuneonlineng.com/nigeria-lost-n5-5-trn-to-fraud-cybercrimes-in-10-years/> accessed 24th May 2022

[11] Institutional Asset Manager, Financial institutions are prime targets for cybercriminals and future attacks are 'inevitable' <http://www.institutionalassetmanager.co.uk/2021/08/19/305127/financial-institutions-are-prime-targets-cybercriminals-and-future-attacks-are> accessed 25th May 2022

"cybercrimes" to acts that amount to a violation of fundamental rights of citizens such as the right to the dignity of the human person and the right to privacy and family life.

Cybercrime Act 2015 established regulatory and institutional structures for the use, transmission, and storage of data in computers, and computer networks and also prohibited activities in relation to communication over a network of computers. The Act gives the President rights to by Order published in the Federal Gazette, designate certain computer networks as critical national infrastructure to protect such infrastructure and management, transfer, access, and control of data contained in them.[12] Also, the Act incriminated any unlawful and unauthorized access to a computer in which any violation and upon conviction; such person is liable for a term of 15 years without the option of fine, and in cases where such access results to grievous bodily harm, a fine of #5,000,000 and imprisonment term of two years.[13] It is also a crime under the Act to unlawfully intercept computer communications[14], and without any authority to modify computer data[15], any intentional unauthorized interference with a computer which hinders the functioning of the computer by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.[16] It is also a crime to unlawfully produce, supply, adapt, manipulate, or procure for use, import, export, distribute, or offer for sale any device or computer program to commit any offence contained in the Act.[17] The use of a computer or computer network to intentionally or fraudulently impersonate any person who is either living or dead with the intent to deceive, defraud, gain personal advantage or interest in property, cause disadvantage to the person impersonated, or obstruct arrest is also incriminated under the Act.[18] The Act went further to prohibit the use of the computer to create, procure, possess, offer or distribute child pornography, including using a computer as a medium for texting a child to carry out any sexual activity with the child.[19] Similarly, it is an offence to use a computer to send a false message to any person to threaten and cause anxiety to such a person.[20] Cybersquatting which includes the intentional use of a business name, trademark, domain name, and phrases registered, owned, or in use by any individual, body corporate, or belonging to either the Federal, State, or Local Governments in Nigeria is also prohibited.[21] Also, it is an offence to make use of the computer to carry out terrorist attacks, share any racist and xenophobic material, attempt, aid, conspire, or aid the commission of the offences contained in the Act.[22] Under the Act, a body corporate is capable of committing the offences contained in it, including its Chief Executive Officer, Director, Manager, and Secretary.[23] To protect the safety of internet users, the Act further provides guidelines for Service Providers in obtaining, using, and transferring users' data. A service provider as defined by the Act means "any public or private entity that provides to users of its service the ability to communicate through a computer system, electronic communication devices, mobile networks; and any other entity that processes or stores computer data on behalf of such Communication service or users of such service."[24] The Act also established the Cybercrime Advisory Council and gave it powers to make guidelines in respect of provisions contained therein and has a responsibility to advise the government on measures for fighting cybercrime-related offence, threats to the nation's cyberspace, and cyber security.[25]

4.0 THE SOCIO-ECONOMIC RELEVANCE OF CYBERCRIME ACT 2015 IN NIGERIA

The growing cases of cybercrime in the world and Nigeria particularly, as a result of moral and social decadence, quest for wealth, and unemployment may have had more damaging effects on the country generally. However, the Cybercrime Act has, on a wider level, curbed frequent cases of cybercrime. For instance, one of the reoccurring cases of cybercrime in Nigeria before the emergence of the Cybercrime Act was cybersquatting – which stood more like a business for most people. The Act has succeeded in substantially crippling the illegal act through investigations, identification, and prosecution of offenders. Illustratively, in 2011 before coming into force of the Act, one Emmanuel Efremov, was reported to have registered a domain name known as "lindaikeji.net" which is directly similar to "www.lindaikejisblog.com", belonging to one of Nigeria's foremost bloggers, Linda Ikeji. He

[12] Section 3, Cybercrime (Prevention and Prohibition) Act, 2015
[13] Section 6, Cybercrime (Prevention and Prohibition) Act, 2015
[14] Section 7, Cybercrime (Prevention and Prohibition) Act, 2015
[15] Section 8, Cybercrime (Prevention and Prohibition) Act, 2015
[16] Section 9, Cybercrime (Prevention and Prohibition) Act, 2015
[17] Section 10, Cybercrime (Prevention and Prohibition) Act, 2015
[18] Section 13, Cybercrime (Prevention and Prohibition) Act, 2015
[19] Section 14, Cybercrime (Prevention and Prohibition) Act, 2015
[20] Section 15, Cybercrime (Prevention and Prohibition) Act, 2015
Section 15, Cybercrime (Prevention and Prohibition) Act, 2015
[22] Section 17, 18 & 19, Cybercrime (Prevention and Prohibition) Act, 2015
[23] Section 20, Cybercrime (Prevention and Prohibition) Act, 2015
[24] Section 58, Cybercrime (Prevention and Prohibition) Act, 2015
[25] Section 25 & 26, Cybercrime (Prevention and Prohibition) Act, 2015

later redirected the blog to the actual owner –after profiting from the act and he was never prosecuted, this could be because the Cybercrime Act was not in existence at the time.[26] However, a similar case came up in 2018 when the Nigerian Government launched the National Carrier/Airline on 18th July 2018, and on the same day, one Mr Olumayowa Elegbede intentionally bought the domain names, "NigeriaAir.ng" and "NigeriaAir.com.ng." He later advertised them for sale to a government agency. An act of this nature from the definition of Section 58 of the Act amounts to cyber squatting although the perpetrator was never prosecuted.[27]

In 2021, a Federal High Court sitting in Ilorin, Kwara State convicted and jailed a student of the Federal Polytechnic, Offa, for one year after he was found guilty of internet fraud upon a suit filed by the Economic and Financial Crimes Commission ("EFCC"). The 21-year-old Olaleye Rosheed using his iPhone device, pretended to be a white female, who has the Gmail account christianalopez105@gmail.com. Although the charge was brought under Section 95 of the Penal Code, punishable under Section 324 rather than the Cybercrime Act.[28] However, in 2022, the same Federal High Court sitting in Ilorin Kwara State convicted and sentenced 6 cybercriminals namely; Adetoye Damilare Timilehin, Adebayo Ridwan Abiola, Adeshina, Hammed Akorede Hammed, Komolafe Shina David, and Fatimehin Kayode to different imprisonment terms and fines, upon a successful proof of cybercrime-related offences of impersonation and internet fraud by the EFCC.[29] The convicts had utilized their illegal acts to immerse wealth and defraud their victims of about $750,000, $200,000, $100,000, and $50,000 respectively. This decision came at a time when Nigeria was ranked as the 16th most vulnerable cybercrime State globally,[30] and 3rd in Africa according to a report from Kaspersky Lab in a 2019 data.[31] Just in 2021, a Nigerian, Obinwanne Okeke, was convicted and jailed in the United States for using a registered company based in Nigeria to defraud people of over $11m.[32] Also in 2021, a popular Nigerian Instagram Influencer Raymond Abbas called Hushpuppi was arrested in Dubai in connection with allegations of internet fraud.[33]
From the provisions of the Cybercrime Act 2015, a rational conclusion is that cybercrime does not only relate to financial offences but also other areas which are of great interest to the security architecture of the nation, companies, and individuals in business operations, private use, communication, and storage of data. In other words, it is right to state that the act extends to the social life and economic activities of the nation. Thus, the social and economic relevance of the Act is numerous and has benefited the country in dimensional ways.

[26] News Rescue, Man Who Got Linda Ikeji Suspended Admits His Director, Cyber squatter Owner of LindaIkeji.net (2014) <https://newsrescue.com/man-got-linda-ikeji-suspended-admits-director-cybersquatter-owner-lindaikeji-net/#ixzz3oH9OwNRu> accessed 23rd September 2019; Nigerian law Today, "Squashing the squatter in Cyberspace <http://nigerianlawtoday.com/squashing-the-squatter-on-cyberspace/> accessed 23rd September 2019

[27]Toba Obaniyi, "Nigeria Air Domain Registration Saga. Who Wins?" Whogoghost (2018) <https://blog.whogohost.com/nigeria-air-domain-name-saga/> accessed 25th May September 2022

[28] Streetott, A court has sentenced Olaleye Rosheed, a 21-year-old student of the Federal Polytechnic, Offa, in Kwara State, to one-year imprisonment on Thursday for cybercrime (2021) <https://streetott.com.ng/offa-poly-student-sentenced-to-one-year-imprisonment-for-internet-fraud/> accessed 25th April 2022

[29] Vanguard News, Six convicted for cybercrime in Ilorin (2022) <https://www.vanguardngr.com/2022/03/six-convicted-for-cybercrime-in-ilorin/> accessed 25th May 2022

[30] Vanguard News, Breaking: Nigeria ranks 16th in FBI International Cybercrime report (2021) <https://www.vanguardngr.com/2021/03/breaking-nigeria-ranks-16th-in-fbi-international-cybercrime-report/> accessed 25th May 2022
[31] Jumoke Akiyode Lawanson, "Cybercrime: Nigeria ranks 3rd most attacked countries in the world" Business Day (2019) <https://businessday.ng/technology/article/cybercrime-nigeria-ranks-3rd-most-attacked-country-in-africa/> accessed 25th May 2022

[32] Vanguard News, Breaking: Nigeria ranks 16th in FBI International Cybercrime report <https://www.vanguardngr.com/2021/03/breaking-nigeria-ranks-16th-in-fbi-international-cybercrime-report/> accessed 25th May 2022
[33] Supra, 30

4.1: Intellectual Property Theft

Intellectual property rights are important for economic growth and also propel innovations due to the guarantee of exclusive use and ownership of a product. It would amount to a total defeat of intellectual property rights; patents, trademarks, copyrights, industrial design, and trade secrets, if the Cybercrime Act did not come in to prohibit unlawful access to computers where intellectual property rights of companies and security designs of security agencies are stored. Studies have shown that China is at the lead of intellectual property theft, through unlawful access to computers to extract information related to industrial design, trade secrets, and other commercially valuable information – these in addition to other kinds of cybercrimes by China caused the loss of about $20 billion in losses in 2014 to other countries.[34] Hence, the Act has incriminated the activities of cybercriminals which may affect the value, use, and ownership of intellectual property rights of the government, companies, and people in the creative industry.

4.2: Safety of Financial Institutions

A 2021 report showed that Nigerian Commercial Banks lost over $30 million to cybercrime only in 10 years, which stood at a whooping sum of #15 billion.[35] This record number excludes other attacks and cybercrimes committed against Financial Technology Companies who depend on ICT and Internet of Things ("IoT") to carry out business transactions, payment processing and serving as payment gateways for companies. Every year, cybercrime attacks on Financial Technology Companies keep rising according to a report from Serianu Cyber security.[36] A report from the FBI has also shown that Financial Technology companies from all around the world have lost $20 billion cumulatively in value to cybercrime related attacks. Hence, the Act having come into existence is helping to reduce the attacks on financial institutions through system hack, phishing links, impersonations and other unlawful methods. At the moment, people who have been found to have committed financial frauds against financial institutions and private persons using the computer have been prosecuted, convicted and punished in line with tenets of the extant law,[37] and this is helping to increase the confidence of customers on online banking and banking institutions.

4.3: Security and Privacy of Internet Users' Data

The safety of internet users' data and the privacy of citizens have also been subjects of cybercrime attacks around the world. Worthy of note is the fact that the right to privacy is a fundamental right guaranteed by the Constitution.[38] Hence, the Cybercrime Act has solidified the protection of this right in respect of online activities and records of citizens stored on the internet to criminalize unlawful activities that may result in their violation.

4.4: Improvement in the Security of the Country

The provisions of the Act which relate to the prohibition of the use of computers to carry out terrorism activities have also to a great extent, reduced incidences of terrorism in the country through ICT facilities.[39] Although no one has been prosecuted under this section of the Act, it is believed that it will help to manage any future occurrence, to ensure the prosecution of offenders. Maybe the reason this provision has not been tested is because terrorism activities in the country are not so sophisticated with respect to using computers to carry out such activities. In the Arabian Peninsula, there was a 2010 online magazine publication by Al-Qaida that contained training guidelines for terrorists.[40]

4.5: Maintenance of Common Moral Standards of the Country

Socially, the sharing, soliciting, and distribution of child pornography is both immoral and illegal.[41] The world has transformed beyond holding certain acts as immoral such as Child pornography, but the Cybercrime Act has made it a crime to engage in such activities which may endanger the life of the child in the future. The Act also ensured social order by laying the basic principles for the use of ICT facilities for social interactions and business activities, unlawful interference with data, and privacy of citizens.

---

[34] McAfee, Economic Impact of Cybercrime – No slowing down (2018) <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf> accessed 25th May 2022

[35] Supra, 8

[36] TNP, "Nigeria: Cyber security Challenges Of The Nigerian FinTech Sector " Mondaq (2020) <https://www.mondaq.com/nigeria/fin-tech/848040/cybersecurity-challenges-of-the-nigerian-fintech-sector> accessed 25th May 202

[37] Supra, 27, 28, 29, 30, 31

[38] Section 37 Constitution of the Constitution of the Federal Republic of Nigeria 1999

[39] Section 17, Cybercrime (Prevention and Prohibition) Act, 2015

[40] UNODC, The use of the Internet for terrorist purposes (2012) <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> accessed 25th May 2022

[41] Supra, 17

5.0 CONCLUSION

The Cybercrime Act 2015 emerged as a formal means of crime control to curb the increasing rate of cybercrime-related activities in the country. It is of utmost relevance to the socio-economic well-being of the country, through the establishment of regulatory and institutional framework for the use of the computer and the internet, which now forms an integral part of the society. While the Act has not succeeded in eliminating cybercrime activities in the country which may never happen, it has continued to help maintain a level of sanity in internet usage, thereby contributing substantially to the social and economic well-being of the country.

6.0 RECOMMENDATIONS

It is recommended that the government should increase research in the areas of identifying cybercrime-related activities to find common ways of fighting them. This is necessary for achieving the purposes of the Act and maintaining a level of sanity in the internet space, which now forms an integral part of society and citizen's lives. Furthermore, there should be increased training and funding for Officers of the Nigerian security forces, especially the Police and the EFCC to help its Officers in tracking and prosecuting cybercriminals. There also a need to create more jobs for the teeming youths to dissuade their minds from engaging in cybercrimes for survival. The government must also engage in awareness creation on the common forms of cybercrime, including their dangers to the socio-economic growth of the country.

References

Ann Lindberg, "Security Profile of Lan Authur Murphy", St. Petersburg Times (2005) <https://attrition.org/errata/charlatan/ian_murphy/threat_profile/> accessed 14th May 2022

Bode Adewumi, |Nigeria Lost N5.5 Trn To Fraud, Cybercrimes In 10 Years" Nigerian Tribune (2021) <https://tribuneonlineng.com/nigeria-lost-n5-5-trn-to-fraud-cybercrimes-in-10-years/> accessed 24th May 2022

Cybercrime (Prevention and Prohibition) Act, 2015

Cybercrime (Prohibition & Prevention) Act 2015 accessible at: <https://www.cert.gov.ng/ngcert/resources/CyberCrime Prohibition Prevention etc Act 2015.pdf > accessed 24th May 2022

Financier Worldwide, The Nigerian Cybercrime Act 2015 and its implications for financial institutions and service providers (2016) <https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its-implications-for-financial-institutions-and-service-providers#.YozNrqjMLIU> accessed 24th May 2022

Institutional Asset Manager, Financial institutions are prime targets for cybercriminals and future attacks are 'inevitable'<http://www.institutionalassetmanager.co.uk/2021/08/19/305127/financial-institutions-are-prime-targets-cybercriminals-and-future-attacks-are> accessed 25th May 2022

Jumoke Akiyode Lawanson, "Cybercrime: Nigeria ranks 3rd most attacked countries in the world" BusinessDay (2019) <https://businessday.ng/technology/article/cybercrime-nigeria-ranks-3rd-most-attacked-country-in-africa/> accessed 25th May 2022

Lambert Elechi, Oko Kelechi and Shanhe Jiang, "Formal and Informal Crime Control Views in Nigeria and the United States: An Exploratory Study Among College Students" Journal of Ethnicity in Criminal, Volume 8, 2010, Issue 1

McAfee, Economic Impact of Cybercrime – No slowing down (2018) <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf> accessed 25th May 2022

Merriam-Webster Dictionary <https://www.merriam-webster.com/dictionary/cybercrime> accessed 24th May 2022

Mondaq (2020) <https://www.mondaq.com/nigeria/fin-tech/848040/cybersecurity-challenges-of-the-nigerian-fintech-sector> accessed 25th May 2022

Morris Worm, "Famous Cases and Criminals", Federal Bureau of Investigation <https://www.fbi.gov/history/famous-cases/morris-worm> accessed 24th May 2022

News Rescue, Man Who Got Linda Ikeji Suspended Admits His Director, Cybersquatter Owner of LindaIkeji.net (2014) <https://newsrescue.com/man-got-linda-ikeji-suspended-admits-director-cybersquatter-owner-lindaikeji-net/#ixzz3oH9OwNRu> accessed 23rd September 2019; Nigerian law Today, "Squashing the squatter in Cyberspace <http://nigerianlawtoday.com/squashing-the-squatter-on-cyberspace/> accessed 23rd September 2019

Streetott, A court has sentenced Olaleye Rosheed, a 21-year-old student of the Federal Polytechnic, Offa, in Kwara State, to one-year imprisonment on Thursday for cybercrime (2021) <https://streetott.com.ng/offa-poly-student-sentenced-to-one-year-imprisonment-for-internet-fraud/> accessed 25th April 2022

TNP, "Nigeria: Cybersecurity Challenges Of The Nigerian FinTech Sector

Toba Obaniyi, "Nigeria Air Domain Registration Saga. Who Wins?" Whogoghost (2018) <https://blog.whogohost.com/nigeria-air-domain-name-saga/> accessed 25th May September 2022

Ugo Aliogo, "West Africa: 'Nigeria Lost N5.5 Trillion to Cybercrimes in 10 Years" YallaAfrica (2021) <https://allafrica.com/stories/202104260948.html#:~:text=The%20Chief%20Strategy%20Officer%2C%20Deloitte,and%20cybercrimes%20in%2010%20years.> accessed 24th May 2022

UNODC, The use of the Internet for terrorist purposes (2012) <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> accessed 25th May 2022

Vanguard News, Breaking: Nigeria ranks 16th in FBI International Cybercrime report (2021) <https://www.vanguardngr.com/2021/03/breaking-nigeria-ranks-16th-in-fbi-international-cybercrime-report/> accessed 25th May 2022

Vanguard News, Breaking: Nigeria ranks 16th in FBI International Cybercrime report<https://www.vanguardngr.com/2021/03/breaking-nigeria-ranks-16th-in-fbi-international-cybercrime-report/> accessed 25th May 2022

Vanguard News, Six convicted for cybercrime in Ilorin (2022) <https://www.vanguardngr.com/2022/03/six-convicted-for-cybercrime-in-ilorin/> accessed 25th May 2022