International Digital Organization for Scientific Research ISSN: 2579-0757
IDOSR JOURNAL OF CURRENT ISSUES IN ARTS AND HUMANITIES 7(1):126-143, 2021.

Cybersecurity of Innovations: A Content Analysis of Nigeria Cybercrimes (Prohibition, Prevention Etc.) Act, 2015

Chibueze Linus Ogbuoshi
Department of Mass Communication, Enugu State University of Science and Technology, Enugu.
Email:linus.ogbuoshi@yahoo.com

ABSTRACT

The notion of cybersecurity is to serve as a regulatory mechanism against cybercrimes. Using a content analytical approach, the study discussed cybersecurity of innovation by examining Part III: Offences and Penalties of the Nigeria Cybercrimes (Prohibition, Prevention etc.) Act, 2015. The study examined the treatment of cybercrimes and corresponding penalties. It was anchored on the theory of technology-enabled crimes which establishes a correlation between technology (especially computers and telecommunications) and crimes. The research method was the content analysis with the following content categories: cyber trespasses and thefts, cyber violence, cyber terrorism, cyber espionage and cyber pornography. The findings of the study revealed that cases of cyber trespasses and thefts were dominant in treatment by the Act, however cyber espionage and cyber terrorism were least treated. Based on the findings of the study, it is recommended that upon amendment of the Act, issues on cyber espionage and cyber terrorism should be duly inculcated with corresponding strict penalties. A neglect of these important cyber issues can threaten the security of a nation.
Keywords: Act, Cybercrime, Cybersecurity, Cyberspace.

INTRODUCTION

The pervasive nature of the Internet has widened its scope of access to information. On a click of computer mouse, an Internet savvy user accesses a limitless array of information [1]. The Internet has revolutionised information collection, processing and dissemination [2]. The breakthroughs associated with the Internet range from information system management to advanced computer programming [3]. [4], observe that the Internet has changed the economics and ease of reproduction. With the Internet, users have access to new opportunities for work and business activities. It has equally proven to be a veritable medium of innovative enterprises. [5], assert that the Internet has supported research and development leading to the discovery of innovative enterprises. An innovation is a conceptualised idea about a product or service. Every surviving enterprise is based on the ability at which the enterprise translates an innovation into tangible outputs [6]. With online activities, modern economy is largely ICT-driven. Information and communication technology covers a wide range of activities done on the Internet. The challenge of an ICT-economy is its porous nature and vulnerability to cybercrimes. Its programming content can easily be hacked or plagiarised [7,8,9,10].

Cybercrime is a global phenomenon that affects online businesses through a syndicated Internet fraud [11]. Although the Internet has altered how people interact and execute different tasks, its vulnerability to cybercrime poses threats to information management. As the rise in cybercrime continues unabated, many governments and regulatory bodies have proffered different strategies of checkmating Internet frauds. To curb incidences of cybercrime, cybersecurity considerations have inevitably gained global attention [12]. Cybersecurity is primarily concerned with making cyberspace safe from threats namely cyber threats [13,14]. Cybersecurity covers a wide range of the Internet activities and protects information in hardware and software devices. It is a check to cybercrime and should be discussed together. The Nigeria Cybercrimes (Prohibition, Prevention etc.)

Act, 2015 regulates Internet-related activities and criminalises all forms of cybercrimes. This study, therefore content-analysed the above Act vis-à-vis its aim of increasing innovative creditability of Nigeria's cyberspace [15,16].

Statement of Research Problems

The emergence of cyberspace is transforming Nigerian economy with attendant cyber threats. Cybercrimes have increased tremendously leading to increased incidences of online criminal activities. Hackers compromise account data of the Internet users and corporations leading to cyber frauds. The rise in Internet penetration has expanded the scope of entrepreneurial innovations. Now, businesses sprang up and the economy continues to grow. More business opportunities abound on the Internet, however the threats associated with cybercrimes continue unabated. The danger is the erosion of confidence in Nigerian genuine economic credibility. A wide range of illegal Internet-related activities exist such as cyber hacking, cyber bullying, cyber pornography and cyber thefts. These cybercrimes increase the incidence of financial frauds and rob potential entrepreneurs of innovative originality and intellectual property rights. The Cybercrime (Prohibition, Prevention etc.) Act 2015 is a form of cybersecurity that checkmates the activities of online fraudsters and restores confidence and creditability among Internet users. Although the Act regulates cyber activities, its effective implementation has dominated scholarly discussions and formed the crux of this study.

Research Objectives

The broad objective is to examine the manifest contents of Nigeria Cybercrime (Prohibition, Prevention etc.) Act, 2015 vis-à-vis cybersecurity of innovations. The specific objectives include:

a. To examine the treatment of cybercrimes in the Cybercrime (Prohibition, Prevention etc.)Act, 2015.
b. To examine the nature of penalties of cybercrimes in the Cybercrime (Prohibition, Prevention etc.)Act, 2015.

Research Questions

The following research questions were formulated to guide the study:

a. What is the treatment of cybercrimes in the Cybercrime (Prohibition, Prevention etc.) Act, 2015?
b. What is the nature of penalties of cybercrimes in the Cybercrime (Prohibition, Prevention etc.) Act, 2015?

Review of Related Literature

Cybercrime: An Overview

Basically, a crime is an action prohibited and punishable by law. [15] define a crime as the intentional commission of an act usually deemed socially harmful or dangerous and specifically defined, prohibited, and punishable under criminal law. A criminal code is a code that defines crimes as contained in a code which must be interpreted in the light of many principles, some of which may not actually be expressed in the code itself. It is a specific act committed in violation of the law of a nation. [3] defines a crime as commission of an act or act of omission that violates the law and is punishable by the state. Crimes are considered injurious to society or the community. On the other hand, 'cyber' is a prefix that connotes 'computers and information systems.' It is often used as a prefix that refers to all forms of computer activities especially the networking aspect of computer technology. It is, therefore used to form a specific type of online activity such as cyberspace, cybernetics, cybercrimes, cybersecurity etc.

The concept of cybercrime refers to Internet frauds and all forms of computer-enabled or smartphone-enabled frauds punishable by law. It simply involves all Internet-based crimes. It is a crime committed using computer networks through hacking into a person's database to steal vital information

or money or use the Internet to engage in cyber bullying or blackmail. [13] ,observes that cybercrime has surpassed illicit drug trade through a highly syndicate of Internet fraudsters who compromise account data of unsuspecting victims. The activities of Internet hackers have affected global economy. Apart from a simple definition of cybercrime to connote monetary fraud, the findings of [13], confirm a non-monetary aspect of cybercrime. The non-monetary offences include creating and distribution of viruses on computers or posting confidential business information on the Internet. There is a wide range of cybercrimes from illegal downloads of music to advanced online financial frauds.

In Nigeria, issues of cybercrimes have remained a recurrent issue. Most online businesses lack adequate security of websites thereby making online businesses susceptible to cyber attacks. [5] agrees that the majority of online businesses in Nigeria are susceptible to cyber attacks and the increasing spate of cyber-criminals was threatening the Nigeria economy. The finding of [13,14] affirm that the Internet introduces its own peculiar risks in the collection, processing and distribution of information. Its susceptibility to fraud is highly dependent on the media of information, the security nature of websites and a hacker's expertise in cyber frauds.

Forms of Cybercrimes

There are different forms of cybercrimes. As information technology evolves, so the incidences of cybercrimes increase. A simpler form of cybercrime may involve an unauthorised download or streaming of music on a website to advanced cybercrime of intrusion into computer users' account and unauthorised monetary transactions using the Internet. Basically, cybercrime is a computer-related crime that affects the confidentiality and integrity of computer data. It is a crime that is committed by manipulating data and sometimes, by hypnotising a victim through mind games. There are different forms of cybercrime viz:

a. Cyber thefts: This is a criminal act of hacking into a person's computer database to steal relevant files or make unauthorised monetary withdrawals/transfers. It also covers all fraudulent means of hijacking a person's business or social media account for dubious purposes. Today, websites of corporations are hacked; banks' treasuries are looted through unauthorised online transfers and social media accounts are unruly hijacked by hackers to commit fraud.
b. Cyber bullying: This covers all computer-related bullies through posts, images and emojis to defame a person. It also covers the use of the Internet to blackmail a person into making monetary transfer to redeem one's image.
c. Cyber plagiarism: Plagiarism is the art of making a replica of an author's work without reference to the original author/creator. [8], defines it as an act of making a verbatim reproduction of a person's literary work without due acknowledgement of the owner of literary work. It is a violation of copyright and intellectual property rights when a plagiarism is committed. It is regrettable that writers often copy and paste online materials without proper attribution. A writer that lifts a work without due credit to the original owner has committed a crime.
d. Cyber terrorism: It covers the use of technology in aiding terrorism. The Internet has become a veritable medium of information on terrorist activities
e. Cyber espionage: It is a technology-driven act of spying. It is a criminal act of electronic spying on government and persons. [7] identifies the following forms of cybercrime:

a. Cyber pornography: It connotes all computer-based forms of obscenity and indecency whether explicit or subtly implied in language use, images or codes. The flexibility of the Internet has made it a veritable medium of dissemination of

salacious contents that endanger the morality of society.

b. Cyber deceptions and thefts: It covers all computer-based frauds such as hacking of a person's bank or social media account to commit fraud. Another aspect of cyber deception and theft is called cybersquatting. It is the illegal buying and selling of a product using a registered company to defraud people.
c. Cyber trespass: It covers the introduction of viruses in a person's online account to defraud him or deprive him the ownership of intellectual property rights. It is also a form of hacking and defacement of a person's online account.
d. Cyber violence: It covers all forms of psychological harms or machine malfunctions due to cyber manipulations. Cyber stalking is a form of cyber violence which involves trailing a person over a long period of time in a frightening manner. Introduction of viruses to manipulate a computer system is an aspect of cyber violence.

Effects of Cybercrimes

Cybercrimes affect both humans and economy. It inflicts psychological injuries on victims and robs a person of his intellectual property rights. [7] state that cybercrimes affect information collection and processing adversely by creating and distributing viruses on computer networks in the attempt to manipulate computer programs or cause a permanent damage to the system and vital information. Computer attacks are like pathogen infections that can be propagated through a network [6]. Cybercrimes lower the integrity of a county before the international communities. The reason for the rise of Internet-related activities in Nigeria was due to initial reluctance on the part of government to fight cybercrimes with the full force of law. The Cybercrimes (Prohibition, Prevention etc.) Act, 2015 was enacted to use the full weight of the law against all forms of cybercrimes. [7] identify (a) financial loss, (b) loss of reputation, (c) reduced productivity and (d) vulnerability of information and communication technology (ICT) systems and networks as effects of cybercrimes.

Understanding Cybersecurity

The aim of cybersecurity is to serve as a control mechanism against cybercrimes. Security is simply a protection against an unfavourable situation. Simply put, cybersecurity refers to all forms of protections against cybercrimes. It covers all legitimate means of checking criminal invasions of computer networks. [7], observe that cybersecurity has risen to become a national concern against cyber thefts as some Nigerian cyber criminals are daily devising new ways of averting government surveillance. Cybersecurity refers to the use of tools and policies to protect the cyber environment and provide a legal framework to punish offenders. It protects persons and corporations from unauthorised access to data. As a policy-driven strategy, cybersecurity adopts functional policies and legal frameworks to protect cyberspace and reduce vulnerability of persons and corporations to cyber thefts.Primarily, cybersecurity is concerned with making the cyberspace safe from threats and malicious use of information and communication technology (ICT) either as a target or as a tool by a wide range of malevolent actors [12]. The rise in sophistication of communication technology raises fear of safety of information on the Internet. With hacking software, a computer hacker can break computer firewalls and truncate vital information. He can send a fake and dubious credit transfer alert to a customer without actual money transfer. The incidences of cybercrime continue to elude the tracking devices of computer analysts and security agencies. Cybersecurity, therefore is treated within three dimensions: (a) as an economic issue, (b) as an information technology issue and (c) as a law enforcement issue. Whatever dimension of study, cybersecurity aims at

creating a safe cyberspace and to guarantee system fidelity and integrity.

Cybersecurity as a Control Mechanism against Cybercrimes in Nigeria

Cybercrimes have continued to elicit scholarly discussions. It is a global phenomenon and nations have enacted cybercrime prohibition laws such as Kenyan National Cyber Security Strategy in 2014, the National Cyber Security Strategy of Japan in 2010, and the Cyber Security Strategy of United Kingdom in 2011. Although the provisions of cybersecurity laws differ among nations; they reflect the desire to fight cybercrimes and create a safe cyberspace.

Major legislations as checks against cybercrimes and related offences in Nigeria include:

a. Nigeria Criminal Code Act 1990
b. Economic and Financial Crime Commission (Establishment) Act 2004
c. Advanced Fee Fraud and Other Fraud Related Offences Act 2006
d. Money Laundering (Prohibition) Act 2011
e. Cybercrimes (Prohibition, Prevention etc.) Act, 2015

Basically, the Cybercrimes (Prohibition, Prevention etc.) Act, 2015 provides a cohesive measures and strategies towards assuring security and protection of the country presence in cyberspace [12].

Theoretical Framework

The study was anchored on the theory of technology-enabled crimes. It posits that there is a correlation between technology (especially computers and telecommunications) and crime. Within the context of discussion, the theory states that a crime is committed directly against computers and computer systems [11]. It argues that criminals often take advantage of new technologies to commit crimes. These criminals experience with existing tools in order to experiment on the vulnerability of technology to defraud unsuspecting users. The cyberspace is a network of computers and telecommunications signals. The computer and other communication devices may be agents of cybercrimes. Technology plays dual roles in crime commission and control. It poses unimaginable threat to society when it is manipulated in form of cybercrimes. It is equally a veritable medium of containing incidences of cybercrimes through functional cybersecurity laws. [11] argues that new adaptive and ordinary crimes emerge over time to create technology crime waves, the magnitude of which can be theoretically measured, compared and predicted. Summarily, the theory of technology-enabled offers a cause-and-effect paradigm of cybercrimes.

METHODOLOGY

The study adopted a content analysis which examined only the manifest contents of Part III: Offences and Penalties of the Cybercrimes (Prohibition, Prevention etc.) Act, 2015. The units of analysis were sections and subsections of Part III of the Act. The identified content categories were: (a) Cyber trespass which covers thefts, forgeries and computer hacking, (b) Cyber violence which covers all forms of cyber stalking, introduction of viruses in computer systems, cyber bullying and blackmails done on the Internet/computers, (c) Cyber plagiarism which covers unauthorised verbatim downloads from the Internet, (d) Cyber terrorism which covers the use of technology for terrorist activities and information sharing, (e) Cyber espionage which examines online crime of spying, and (f) Cyber pornography which covers all online obscenity and indecency that endanger the morality of users. The analysis was thematically done.

Data Analysis and Presentation

The analysis measured the nature of treatment of cybercrimes in the Act. It also examined the nature of penalties of each identified cybercrime in Part III: Offences and Penalties of the Act.

Table 1: The treatment of cybercrimes in the Cybercrime (Prohibition, Prevention etc.) Act, 2015

Nature of cybercrime	Offences in the Act	Part/Section and Subsection
Cyber trespass and thefts	1. Unauthorised access to computer network(s) for fraudulent purposes and vital data on national security.	Part III: Offences and Penalties. Sec. 5 (1)
	2. Obtaining computer data, securing access to program, commercial or industrial secret or classified information	Part III: Sec. 6 (1)
	3. Use of device to avoid detection or otherwise prevent identification or attribution with the act or commission.	Part III: Sec. 6 (3)
	4. Intentional trafficking of password or similar information through which a computer may be accessed without lawful authority by persons or organisations.	Part III: Sec. 6(4)
	5. Perpetration of electronic fraud or online fraud using a cybercafé	Part III: Sec. 7(2)
	6. An employee of a Local Government of Nigeria, private organisation or financial institution working with critical infrastructure, electronic mail who is not authorised and tempers with such computer.	Part III: Sec. 10
	7. An employee of government or private organisation who intentionally hides or detains any electronic mails, messages, electronic payment, credit and debit card which, was found by him or delivered to him in error and which to his knowledge ought to be delivered to another person.	Part III: Sec. 12(3)
	8. Computer related forgeries through access to a computer or computer network and inputs, alters , deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible.	Part III: Sec. 13
	9. Computer related fraud of unauthorised access or in excess of authority causes loss of property to another by altering, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits on himself or another person.	Part III: Sec. 14(1
	10. Intention to defraud by sending electronic message materially misrepresents any fact or set of facts	Part III. Sec. 14(2)

	upon which reliance the recipient or another person is caused to suffer any damage or loss.	
	11. Any intention to defraud, franks electronic messages, instructions, super scribes any electronic message and/or instruction.	Part III. Sec. 14(3)
	12. Intention to defraud, manipulate a computer or other electronic payment devices with the intent to short pay or overpay or actually short pays or overpays an employee of the public or private sector.	Part III. Sec. 14(4)
	13. An employee of bank or other financial institutions who with intent to defraud, directly or indirectly, diverts electronic mails.	Part III: Sec 14 (4a)
	14. An employee of a financial institution who connived with another person or persons to perpetrate fraud using computer(s) or network.	Part III: Sec. 14(5)
	15. Stealing of a financial institution or public infrastructure terminal.	Part III: Sec. 15(a)
	16. Stealing of Automated Teller Machine (ATM)	Part III: Sec. 15(b)
	17. Attempts to steal an ATM	Part III: Sec. 15(c)
	18. Unauthorised modification of computer systems, network data and system interference.	Part III: Sec. 16(1, 2a-d)
	19. Electronic signature: forgeries to defraud or misrepresent another person.	Part III: Sec. 17(1a-c, 2a-h)
	20. Any person or institution who fails to any attack, intrusion and other disruptions to the National Computer Emergency Response Team (CERT) within 7 days of its occurrence.	Part III: Sec. 21(1-3)
	21. An employee of a financial institution who as a result of his special knowledge commits identity theft of it employer, staff, service providers and consultants with the intent to defraud.	Part III: Sec. 22(1)
	22. Fraudulent use of electronic signature, password or any other unique identification of other person.	Part III: Sec. 22(2-3a-d)
	23. Attempt, conspiracy, aiding and abetting.	Part III: Sec. 27(1a-b; 2)
	24. Breach of confidence by service provider(s) and related matters.	Part III: Sec. 29(1-3)
	25. Electronic cards and related fraud.	Part III: Sec. 33(1-13)
	26. Dealing with card of another user	Part III: Sec. 34
	27. Purchase or sale of Card of another user	Part III: Sec. 35(1-2)

	28. Use of fraudulent device or attached emails and websites.	Part III: Sec. 36(1-2)
Cyber violence	1. An intentional or fraudulent act through direct or indirect 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.	Part III: Sec. 8
	2. Intentional destruction or abortion of any electronic mails or processes through which money and/or valuable information is being conveyed.	Part III. Sec. 9
	3. Willful misdirection of electronic messages either with the intention to fraudulently obtain financial gain as a result of such art or the with the intention of obstructing the process in order to cause a delay or speeding the messages with a view to cause an omission or commission that may defeat the essence of such messages.	Part III: Sec. 11
	4. Inducement of any person by or under the government…or any person in charge of electronic devices to deliver to him any electronic messages which includes but is not limited to email, credit and debit cards information , facsimile messages…	Part III: Sec. 12(2)
	5. Cyber stalking of bullying, threats and harassment leading to death, violence or bodily harm.	Part III: Sec. 24(2a-c), 3 a-b) 4-6)
	6. Possession of computer program designed to overcome security measures in any computer system or network and related matters.	Part III: Sec. 28(2-6)
	7. Manipulation of ATM or Point of Sales terminals.	Part III: Sec. 30(1-2)
	8. Employee responsibility: refusal to relinquish or surrender all codes and access rights to their employers … and any employee who, without any lawful reason, continues to hold unto the code or access right of his employer.	Part III: Sec. 31(1-2)
	9. Introduction of viruses, computer phishing, spamming etc.	Part III: Sec. 32(1-3)
Cyber plagiarism	1. International use of name, business name, trademark, domain name or other	Part III: Sec. 25(1-3)

	word or phrase registered, owned and in use by another individual, body corporate or belonging to FG, State or Local Government of Nigeria…	
	2. Importation and fabrication of e-tool through unlawful production, supplies, adaptation, manipulations, procurement etc…computer password, access code or similar data etc…	Part III: Sec. 28(1a-c)
Cyber terrorism	1. Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism.	Part III: Sec. 18(1&2)
	2. Distribution of racists or xenophobic materials to the public through a computer system or network.	Part III: Sec. 26(1a-c)
	3. Committing crime against humanity through systematic attacks against human population etc.	Part III: Sec. 26(2)
Cyber espionage	1. Unlawful interception by technical means, non-public transmission or computer data, content, traffic data including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network.	Part III: Sec. 12(1)
Cyber pornography	1. Any person who intentionally uses any computer system or network in or for child pornography and related offences.	Part III. Sec. 23(1a-e(i-ii)
	2. Making or sending pornographic images to another computer by way of unsolicited distributions.	Part III: Sec. 23(2)
	3. Intentional grooming or soliciting through computer system or network to meet a child for engaging in sexual activities and related matters.	Part III: Sec. 23(3a-b(i-iii) c (i-ii), 4(a-c) and 5)
	4. Cyber stalking of sending grossly offensive, pornographic or indecent materials and other related matters.	Part III: Sec. 24(1a-b)

Source: Cybercrimes (Prohibition, Prevention etc.) Act, 2015. https://www.cert.gov.ng.

Table 1 identifies the essential classifications of cybercrimes in Part III of the Cybercrimes (Prohibition, Prevention etc.) Act, 2015 based on the content categories. It shows that the dominant cybercrimes cited in the Act were treated as cyber trespasses and thefts. This covers all crimes related to thefts, forgeries and computer hacking. There is even record of cybercrimes classified as cyber violence which covers cyber stalking, introduction of viruses in computer systems, cyber bullying and blackmails. Cyber pornography was significantly represented. However; there is minimal representations of cyber terrorism; whereas Part III: Sec. 18(1&2) and Part III: Sec. 26(2) were direct in treating the use of computers or computer systems for acts of terrorism and committing crime against humanity through systematic attacks against

human population respectively; Part III. Sec. 26(1a-c) was indirect and indicated the use of computer or computer systems for racial and xenophobic attacks. Cyber espionage was least treated in the Act.

Table 2: The nature of penalties of cybercrimes in the Cybercrime (Prohibition, Prevention etc.)Act, 2015.

Nature of cybercrime	Offences in the Act	Part/Section and Subsection	Penalties
Cyber trespass and thefts	1. Unauthorised access to computer network(s) for fraudulent purposes and vital data on national security.	Part III: Sec. 5 (1)	10 years terms without an option of fine, and (b) If results in bodily harms, term of not more than 15 years without option of fine.
	2. Obtaining computer data, securing access to program, commercial or industrial secret or classified information	Part III: Sec. 6 (1)	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 …
	3. Use of device to avoid detection or otherwise prevent identification or attribution with the act or commission.	Part III: Sec. 6 (3)	Term of not more than 7 years or to a fine of not more than N7,000,000.00 or to both such fine and imprisonment
	4. Intentional trafficking of password or similar information through which a computer may be accessed without lawful authority by persons or organisations.	Part III: Sec. 6(4)	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.
	5. Perpetration of electronic fraud or online fraud using a cybercafé	Part III: Sec. 7(2)	Three Years imprisonment or a fine of One Million Naira or both.
	6. An employee of a Local Government of Nigeria, private organisation or financial institution working with critical infrastructure, electronic mail who is not authorised and tempers with such computer.	Part III: Sec. 10	A fine of N2,000,000.00 or imprisonment for 3 years.
	7. An employee of government or private organisation who intentionally hides or detains any electronic mails, messages, electronic payment, credit and debit card which, was found by him or delivered to him in error and which to his knowledge ought to be	Part III: Sec. 12(3)	Imprisonment for 1 Year or a fine of N250,000 Naira or to both fine and imprisonment.

	delivered to another person.		
	8. Computer related forgeries through access to a computer or computer network and inputs, alters , deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible.	Part III: Sec. 13	Imprisonment term of not less than 3 years or to a fine of not less than 7,000,000.00 or both
	9. Computer related fraud of unauthorised access or in excess of authority causes loss of property to another by altering, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits on himself or another person.	Part III: Sec. 14(1)	A term of not less than 3 years or to a fine of not less than 7,000,000.00 or both fine and imprisonment.
	10. Intention to defraud by sending electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss.	Part III. Sec. 14(2)	A term of not less than 5 years and to a fine of not less than N10,000,000.00 or to both fine and imprisonment.
	11. Any intention to defraud, franks electronic messages, instructions, super scribes any electronic message and/or instruction.	Part III. Sec. 14(3)	A term of not more than 3 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment
	12. Intention to defraud, manipulate a computer or other electronic payment devices with the intent to short pay or overpay or actually short pays or overpays an employee of	Part III. Sec. 14(4)	A term of not more than 7 Years and shall forfeit the proprietary interest in the stolen money or property to the bank, financial institution or the customer.

	the public or private sector.		
	13. An employee of bank or other financial institutions who with intent to defraud, directly or indirectly, diverts electronic mails.	Part III: Sec 14 (4a)	A term of not more than 5 Years or a fine of not more than N7,000,000.00 or to both fine and imprisonment.
	14. An employee of a financial institution who connived with another person or persons to perpetrate fraud using computer(s) or network.	Part III: Sec. 14(5)	A term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.
	15. Stealing of a financial institution or public infrastructure terminal.	Part III: Sec. 15(a)	A term of 3 years or a fine of N1,000,000.00 or to both fine and imprisonment.
	16. Stealing of Automated Teller Machine (ATM)	Part III: Sec. 15(b)	A term of not more than 7 years or a fine of not more than N10,000,000.00 or to both fine and imprisonment. Forfeiture of proceeds of such theft to the lawful owners of the ATM.
	17. Attempts to steal an ATM	Part III: Sec. 15(c)	A term of not more than 1 year or a fine of not more than N1,000,000.00 or both fine and imprisonment.
	18. Unauthorised modification of computer systems, network data and system interference	Part III: Sec. 16(1, 2a-d)	A term of not more than 3 years or to a fine of not more than N7,000,000.00 or to both such fine and imprisonment.
	19. Electronic signature: forgeries to defraud or misrepresent another person.	Part III: Sec. 17(1a-c, 2a-h)	A term of not more than 7 years or a fine of not more than N10,000,000.00 or to both fine and imprisonment.
	20. Any person or institution who fails to any attack, intrusion and other disruptions to the National Computer Emergency Response Team (CERT) within 7 days of its occurrence.	Part III: Sec. 21(1-3)	Pay a mandatory fine of N2,000,000.00 into the National Cyber Security Fund.
	21. An employee of a financial institution who as a result of his special knowledge commits identity theft of it employer, staff, service providers and consultants	Part III: Sec. 22(1)	7 years imprisonment or N5,000,000.00 fine or both.

	with the intent to defraud.		
	22. Fraudulent use of electronic signature, password or any other unique identification of other person.	Part III: Sec. 22(2-3a-d)	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.
	23. Attempt, conspiracy, aiding and abetting.	Part III: Sec. 27(1a-b; 2)	A term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.
	24. Breach of confidence by service provider(s) and related matters.	Part III: Sec. 29(1-3)	A fine of N5,000,000.00 and forfeiture of further equivalent of the monetary value of the loss sustained by the consumer.
	25. Electronic cards and related fraud	Part III: Sec. 33(1-13)	A term of not more than 7 Years or a fine of not more than N5,000,000.00 or to both such fine and imprisonment and shall further be liable to payment in monetary terms the value of loss sustained by the owner of the credit card.
	26. Dealing with card of another user	Part III: Sec. 34	3 years imprisonment or to a fine of one N1,000,000.00 and shall further be liable to repayment in monetary terms the value of loss sustained by the cardholder or forfeiture of the assets or goods acquired with the funds from the account of the cardholder.
	27. Purchase or sale of Card of another user	Part III: Sec. 35(1-2)	A fine of one N5,000,000.00 and shall further be liable to repayment in monetary terms the value of loss sustained by the cardholder or forfeiture of the assets or goods acquired with the funds from the account of the cardholder.
	28. Use of fraudulent device or attached emails and websites.	Part III: Sec. 36(1-2)	3years or to a fine of N1,000,000.00 or both.

Cyber violence	1. An intentional or fraudulent act through direct or indirect 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.	Part III: Sec. 8	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.
	2 .Intentional destruction or abortion of any electronic mails or processes through which money and/or valuable information is being conveyed.	Part III. Sec. 9	A term of 7 years in the first instance and upon second conviction shall be liable to 14 years imprisonment.
	3. Willful misdirection of electronic messages either with the intention to fraudulently obtain financial gain as a result of such art or the with the intention of obstructing the process in order to cause a delay or speeding the messages with a view to cause an omission or commission that may defeat the essence of such messages.	Part III: Sec. 11	Imprisonment for Three Years or a fine of N1,000,000.00 or both.
	4. Inducement of any person by or under the government…or any person in charge of electronic devices to deliver to him any electronic messages which includes but is not limited to email, credit and debit cards information , facsimile messages…	Part III: Sec. 12(2)	A term of Two Years or a fine of not more than N1,000,000 or to both such fine and imprisonment.
	5. Cyber stalking of bullying, threats and harassment leading to death, violence or bodily harm.	Part III: Sec. 24(2a-c), 3 a-b) 4-6)	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
	6. Possession of computer program designed to overcome security measures in any computer system or network and related matters.	Part III: Sec. 28(2-6)	A term of not more than 3 years or a fine of not more than N7,000,000.00 or to both….etc
	7. Manipulation of ATM or Point of Sales terminals.	Part III: Sec. 30(1-2)	(1)Five Years imprisonment or N5,000,000.00 fine or both and (2) Seven Years imprisonment without an option of fine.
	8. Employee responsibility: refusal to relinquish or surrender all codes and access rights to their employers … and any employee who, without any lawful reason, continues to hold unto the code or access right of his employer.	Part III: Sec. 31(1-2)	3 years imprisonment or 3,000,000.00 or both.
	9. Introduction of viruses, computer phishing, spamming etc.	Part III: Sec. 32(1-3)	3 years imprisonment or a fine of N1, 000,000.00 or both.
Cyber plagiarism	1. International use of name, business name, trademark, domain name or other word or phrase registered, owned and in use by another individual, body corporate or belonging to FG, State or Local Government of Nigeria…	Part III: Sec. 25(1-3)	2 years or a fine of not more than N5,000,000.00 or to both fine and imprisonment.
	2. Importation and fabrication of e-tool through unlawful production, supplies, adaptation, manipulations, procurement etc…computer password, access code or similar data etc…	Part III: Sec. 28(1a-c)	A term of not more than 3 years or a fine of not more than N7,000,000.00 or to both.
Cyber terrorism	1. Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism.	Part III: Sec. 18(1&2)	Liable on conviction to life imprisonment.
	2. Distribution of racists or xenophobic materials to the public through a computer system or network.	Part III: Sec. 26(1a-c)	A term of not more than 5 years or to a fine of not more thanN10,000,000.00 or both such fine and imprisonment.

	3. Distribution of materials which denies or approves or justifies acts constituting genocide or crimes against humanity against human population etc	Part III: Sec. 26(2)	A term of not more than 5 years or to a fine of not more thanN10,000,000.00 or both such fine and imprisonment.
Cyber espionage	1. Unlawful interception by technical means, non-public transmission or computer data, content, traffic data including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network.	Part III: Sec. 12(1)	A term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment.
Cyber pornography	1. Any person who intentionally uses any computer system or network in or for child pornography and related offences.	Part III. Sec. 23(1a-e(i-ii)	A term of 10 years or a fine of not more than N20,000,000.00 or to both fine and imprisonment; and a term of 5 years or a fine of not more than N10,000,000.00 or to both such fine and imprisonment.
	2. Making or sending pornographic images to another computer by way of unsolicited distributions.	Part III: Sec. 23(2)	One year imprisonment or a fine of Two Hundred and Fifty Thousand Naira or both.
	3. Intentional grooming or soliciting through computer system or network to meet a child for engaging in sexual activities and related matters.	Part III: Sec. 23(3a-b(i-iii) c (i-ii), 4(a-c) and 5)	A term of not more than 10 years and a fine of not more than N15,000,000.00; and (ii) a term of not more than 15 years and a fine of not more than N25,000,000.
	4. Cyber stalking of sending grossly offensive, pornographic or indecent materials and other related matters.	Part III: Sec. 24(1a-b)	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.

Source: Cybercrimes (Prohibition, Prevention etc.) Act, 2015. https://www.cert.gov.ng.

Table 2 outlines the penalties for all cybercrime treated in the Cybercrimes (Prohibition, Prevention etc.) Act, 2015. It identified the main penalties in forms of: payment of fines, stipulated terms of imprisonment and forfeiture of assets. It is only cyber terrorism that has no option of fine or forfeiture but a life imprisonment on conviction (Part III: Sec. 18(1&2). This

affirms the position of the Federal Government on the fight against terrorism. Analysis equally shows that cyber pornography (especially against children) attracts the highest penalty of a term of not more than 15 years and a fine of N25,000,000.00 (Part III: Sec. 23(3a-b(i-iii) c (i-ii), 4(a-c) and 5). This penalty confirms the Federal Government determination to protect the morality of children and eradicate all forms of obscenity and indecency on cyberspace. The least penalty in Part III of the Act is a 1 year imprisonment or a fine of N250, 000.00 or both (Part III: Sec. 23(2). Although the Act is silent on the use of the word 'cyber espionage', there are records of unlawful interceptions by technical means, non-public transmission or computer data from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network (Part III: Sec. 12(1).

RECOMMENDATIONS

The study recommends as follows:

a. The Act upon amendment, should clearly state the scope of cyber espionage. This is important as an unauthorised spying on government security network or information network is detrimental. There is, therefore the need to indicate commensurate penalties for acts of cyber espionage.
b. There is the need to expand the scope of cyber terrorism to include modern ways of planning and execution of terrorist activities using computer and computer networks. The Internet is an easy target of terrorist activities through espionage and introduction of computer viruses. Terrorists need the Internet for information dissemination of terrorist activities.
c. There should be periodic checks on the effective implementation of the provisions of the Act by appropriate regulatory agencies. These provisions of the Act become distasteful if they are not implemented adequately.

REFERENCES

1. Akinsehinde (2011). '80% of Nigerian business risk cyber-attacks? *The Punch*, October, 11.
2. Chigozie-Okwum, C., Ugboaja, S., Michael, D. and Osuo-Genseleke, M. (2017). Proliferation of cybersecurity in Nigeria: A root cause analysis. *International Journal of Science Technology*, 6(2), 53-60.
3. Encarta (2009). *Crime*. Redmond, WA: Microsoft Corporation.
4. Erhabor, M.I. (2008). *Cybercrime and the youths*. PDGE Thesis, Department of Education, Ambrose Ali University, Ekpoma, Nigeria.
5. Federal Government of Nigeria (2015). *Cybercrimes (Prohibition, Prevention etc.) Act, 2015* https://www.cert.gov.ng. Accessed on 4-8-2020.
6. Gandhi, G. (2014). *Complexity theory of cybersecurity*. https://www.researchgate.net/publication/263652176. Accessed on 28-8-2020.
7. Ibikunle, F. and Eweniyi, O. (2013). Approaches to cybersecurity issues in Nigeria: challenges and solutions. *International Journal of Cognitive Research in Science, Engineering and Education*, 1(1), 1-11.
8. Kenechukwu, S.A. (2014). *Mass communication: an introduction to sociology of mass media.* Nnewi: CathCom Press.
9. Longe. O.B. and Chiemeke, S.C. (2008). Cybercrime and criminality in Nigeria: what roles are Internet access points in playing? *European Journal of Social Sciences*, 6(4), 133-139.

10. McQuade, S. (2006). *Understanding and managing cybercrime*. Boston: Allyn & Bacon.

11. McQuade, S. (2006). Technology-enabled crime, policing and security. *Journal of Technology Studies*, 32(1), 32-42.

12. Odumesi, J.O. (2015). Approaches to increase public awareness on cybersecurity. *African Journal of Computing and ICT*, 8(4). 143-152.

13. Odumesi, J.O. (2014). Combating the menace of cybercrime. *International Journal of Computer Science and Mobile Computing*, 3(6), 980-991.

14. Osho, O. and Onoja, A. (2015). National cybersecurity policy and strategy of Nigeria: a qualitative analysis. *International Journal of Cyber Criminology*, 9(1) 120-143.

15. Thomas, D. and Thomas, B. (2015). *Crime*. Encyclopedia Britannica Ultimate Reference Suite. Chicago: Encyclopedia Britannica.

16. Wall, D.S. (2011). *Crime and the internet*. London: Routledge.