4-2020

Issues on Information Systems, ICTs, Cyber-Crimes, Cyber Security, Cyber Ethics, and National Security in Nigeria: Librarians' Research

Chidi Onuoha Kalu
NICTM Library, National Institute of Construction Technology and Management, Uromi, chidiokalu@yahoo.com

Esther I. Chidi-Kalu
Nigerian Library Association, National Office, Abuja, estyhigh90@yahoo.com

Ijeoma Ann Achi Okidi
Federal Fire Service, Abuja, ijeomaachidominion@yahoo.com

Blessing Anegbemente Usiedo
NICTM Library, National Institute of Construction Technology and Management, Uromi, usiedoblessingamiens@gmail.com

Issues on Information Systems, ICTs, Cyber-Crimes, Cyber Security, Cyber Ethics, and National Security in Nigeria: Librarians' Research

Chidi Onuoha Kalu (CLN)
NICTM Library,
National Institute of Construction Technology and Management (NICTM),
Uromi, Edo State, Nigeria
chidiokalu@yahoo.com
Corresponding Author

Esther I. Chidi-Kalu (CLN)
Administrative Assistant
Nigerian Library Association,
National Office, Abuja
estyhigh90@yahoo.com

Ijeoma Ann Achi Okidi (CLN)
Federal Fire Service, Abuja
ijeomaachidominion@yahoo.com

Blessing Anegbemente Usiedo (CLN)
NICTM Library,
National Institute of Construction Technology and Management (NICTM),
Uromi, Edo State, Nigeria
usiedoblessingamiens@gmail.com

ABSTRACT

Information and knowledge has become vital economic resources in this new era. Yet, along with new opportunities, the dependence on information systems brought new threats. Crime remains elusive and ever strives to hide in the face of development, while cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. Therefore, this paper examines issues on the Information system, ICT, cybercrime, cyber security, cyber ethics and national security in Nigeria. It is a research work carried out by librarians using selected youths in Wuse area of Abuja Municipal Area Council as a case study. The survey research method was used on the population of 150 respondents randomly selected using a convenient sampling method. All the questionnaires were validly filled and returned. The result shows that the main aim of our national security policy is to ensure that our national survival is free from threat and to ensure that our territorial integrity is free from infringement. Majority of the respondents indicated that the methods cyber criminals often used in defrauding its victims are through identity theft and fraud, and also through making direct contact with their victims using emails and phones calls, etc. The rate of cyber-security and adherence to cyber ethics by internet users is low. The paper recommends amongst others that for the government to combat the menace of cybercrimes, the government should do more in sensitizing the public about cyber-security through its appropriate agencies.

Keywords: Information, Information system, ICT, Cybercrime, Crime, Criminality, Cyber ethics, National security

INTRODUCTION

Crime and criminality have been associated with man since his fall. Crime remains elusive and ever strives to hide in the face of development. Different nations have adopted different strategies to contend with a crime depending on their nature and extent. One thing is certain; it is that a nation with a high incidence of crime cannot grow or develop. That is so because it is the direct opposite of development. It leaves a negative social and economic consequence (Dashora, 2011).

Cyber ethics is the philosophic study of ethics about computers, encompassing user behavior and what they are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have defined policies about cyber ethics. National security is the requirement to maintain the survival of the state through the use of economic power, diplomacy, power projection and political power. It is widely agreed that security should be the responsibility of all and sundry, not restricted to government, the Police force or security agencies (Otto & Ukpere, 2012).

The use of information and communication technology systems in all areas of human endeavours is now known and widely acceptable, this is because its application to the day to day activities of any organization is very efficient and effective (Ebunuwele, Ola & Uduebor, (2014). According to Ebijuwa & ToAnyakoha (2005), ICT are tools and means used for collecting, capturing, processing, storing, transmitting and disseminating of information.

On the other hand, information systems enable more diverse human activities and exert a profound influence over society. They also quicken the pace of daily activities, enable people to develop and maintain new and often more-rewarding relationships, affect the structure and mix of organizations, change the type of products bought, and influence the nature of work. Information and knowledge became vital economic resources. Yet, along with new opportunities, the dependence on information systems brought new threats.

Intensive industry innovation and academic research continually develop new opportunities while aiming to contain the threats (Zwass, 2019). Therefore, an information system could be seen as the information and communication technology (ICT) that an organization uses, and also the way in which people interact with this technology in support of business processes.

Therefore, the aim of this paper is to examine the issues on the information system, ICT, cybercrime, cyber security, cyber ethics and national security in Nigeria using selected youths in Wuse area of Abuja Municipal Area Council (AMC) as a case study.

OBJECTIVES OF THE STUDY

The following is the objectives of the study:

1. To understand the main aim of national security policy in Nigeria.
2. To find out the main method often use by cybercriminals in defrauding people.
3. To find out the impact of ICT in the life of the youths.
4. To ascertain the rate of cyber security management and adherence to cyber ethics by internet users in Nigeria.

RESEARCH QUESTIONS

1. What do you understand as the main aim of national security policy in Nigeria?
2. What is the main method in which cybercriminals often use in defrauding people?
3. What is the impact of ICT in the life of the youths?
4. How do you rate the management of cyber security and adherence of cyber ethics by internet users in Nigeria?

LITERATURE REVIEW

This papers generally examines issues on information system, ICTs, cybercrimes, cyber security, cyber ethics and national security in Nigeria and the literature is reviewed under the following sub-heading; information systems conceptualized, information and

communication technology, cybercrimes and cyber securities, and conceptual overview of cyber ethics and national security.

INFORMATION SYSTEMS CONCEPTUALIZED

Information systems capture data from the organization and its environment and they store the database items over an extensive period of time. When specific information is needed, the appropriate data items are manipulated as necessary, and the user receives the resulting information. Depending on the type of information system, the information output may take the form a query response, decision outcome, expert-system advice, transaction document, or a report.

Formal information systems rely on procedures (established and accepted by organizational practice) for collecting, storing, manipulating, and accessing data in order to obtain information. Formal systems do not have to be computerized, but today they usually are. Informal information systems also exist within an organization such as interpersonal networking. According to D'Atri, et al. (2008), an information system (IS) is a group of components that interact to produce information.

An information system is an academic study of systems with a specific reference to information and the complementary networks of hardware and software that people and organizations use to collect, filter, process, create and also distribute data. An emphasis is place on an information system having a definitive boundary, users, processors, stores, inputs, outputs and the aforementioned communication networks (Jessup and Valacich, 2008).

Bulgacs (2013) opined that any specific information system aims to support operations, management, and decision-making. An information system is the information and communication technology (ICT) that an organization uses, and also the way in which people interact with this technology in support of business processes (Kroenke, 2008). Information

systems typically include an ICT component but are not purely concerned with ICT, focusing instead on the end use of information technology. Information systems are also different from business processes. Information systems help to control the performance of business processes.

Alter (2013) argues for the advantages of viewing an information system as a distinct type of work system. A work system is a system in which humans or machines perform processes and activities using resources to produce specific products or services for customers. An information system is a form of a communication system in which data represent and are process as a form of social memory. It can also be considered a semi-formal language which supports human decision making and action.

According to Zwass (2019), information system is an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. Information systems are used to run inter-organizational supply chains and electronic markets. For instance, corporations use information systems to process financial accounts, to manage their human resources, and to reach their potential customers with online promotions.

An information system is a specific type of system in general. A system is a set of components (subsystems) that operate together to achieve certain objectives. The objectives of a system are realized in its outputs. In particular, the objective of an information system is to provide the appropriate outputs to the members of the organization.

There are six components that can come together to produce an information system, which includes; hardware, software, data, procedure, people and feedback. Hardware are seen as machinery, which includes the computer itself (Central Processing Unit (CPU), and all of

its support equipment such as input and output devices, storage devices and communications devices. Software are computer programs and the manuals that support them and are machine-readable instructions that direct the circuitry within the hardware parts of the system to function in ways that produce useful information from data. Data as one of the components of information system are facts that are used by programs to produce useful information. They are generally stored in machine-readable form on disk or tape until the computer needs them. Procedures are the policies that govern the operation of a computer system. "Procedures are to people what software is to hardware" is a common analogy that is used to illustrate the role of procedures in a system, and every system needs people if it is to be useful but is unfortunate that the most neglected element of the system is the people, probably the component that most influence the success or failure of information systems. The last and not the least of the six components of information system is feedback, which defines that an information system may be provided with feedback, although this component isn't necessary to function.

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

Information and Communication Technology (ICT) refers to technologies that provide access to information through telecommunications. Reference.com (2019) defined information and communication technology like all equipment, applications, and services that involve communication. Computers, mobile phones, televisions, radios, and satellite systems are all part of ICT.

Murray (2011) defined Information and communications technology (ICT) is an extended term for information technology (IT) which stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.

ICT is the digital processing and utilisation of information by the use of electronic computers. It comprises the storage, retrieval, conversion and transmission of information. It referred to as technology that supports activities involving information, such activities include gathering, processing, storing and presenting data. For clarity, Zuppo (2016) provided an ICT hierarchy where all levels "contain some degree of commonality in that they are related to technologies that facilitate the transfer of information and various types of electronically mediated communications".

The advantages and disadvantages of using ICT

Information and communication technology has advantages and disadvantages. The advantages are that communications can take place instantaneously, 24 hours a day, 365 days a year across the globe and messages can be sent to one or multiple recipients, groups of users can access the same programs, applications and even hardware such as printers and faxes using networking and wireless technology, they are used in schools to motivate students as well as facilitate the completion of work and the communications between teachers and students, network set-up can control access to specific information and processes, and it is also easy to monitor work as well as communications.

On the other hand, the disadvantages are that as systems become more and more complex, users require more and more specialized training, which may cost a lot to acquire, networks are exposed to abuse in the form of hacking, viruses spread on it and it is open to email spams and phishing and other viruses, and breaking down of one of the systems can affect other ones, and no one can work on the system if the server of a network is down.

CYBER-CRIMES AND CYBER-SECURITIES

Cybercrime also referred to as computer crime is a crime that involves a computer and a network. In some cases, the computer may have been use to commit the crime, and in other cases, it may be the target of the crime (Moore, 2005). According to Halder & Jaishankar

(2011), cybercrimes can be defined as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

Latha (2008) states that cybercrimes are nothing but crimes of the real world perpetuated in the medium of computer and hence there is no difference in defining a crime in cyber world and real world. Cybercrime may threaten a person or a nation's security and financial health (Morgan, 2016).

On the other hand, cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security (Lord, 2019). Lord further states that cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it.

Cyber Security is also the process and techniques involved in protecting sensitive data, computer systems, networks and software applications from cyber-attacks. According to Schatz, Bashroush & Wall (2017), cybersecurity or computer security or information technology security (IT security) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

CONCEPTUAL OVERVIEW OF NATIONAL SECURITY AND CYBER ETHICS

National security is the aggregate effort of a country to protect itself from invasions, espionage, spying for military secrets, sabotage, subversion, harassment, and other hostile influences. A tentative definition of national security is derive from collating the above: the ability to keep track of domestic and external situations and maintain national stability, prosperity and constitutional order. According to Paleri (2008), National security is the measurable state of the capability of a nation to overcome the multi-dimensional threats to the apparent well-being of its people and its survival as a nation-state at any given time, by balancing all instruments of state policy through governance and is extendable to global security by variables external to it.

The Nigerian society is getting more and more insecure, more people are getting into crimes and they are getting more ruthless, desperate and sophisticated. In Nigeria of today especially since the advent of the present democratic dispensation, new forms of violent crimes have become common; these include kidnapping (actually adult or privileged people's napping) for ransom, pipeline vandalization, Boko Haram bombings, rape, political violence and more. It is widely agreed that security should be the responsibility of all and sundry, not restricted to government, the Police force or security agencies (Otto & Ukpere, 2012).

National security policy aims to ensure that; country's survival is free from threat, country's territorial integrity is free from infringement, country's political independence, and sovereignty integrity is intact and our government and national budgets continue to run, country's economic system and development proceed smoothly, and country's traditional way of life is protected and free from foreign interference and control.

According to The Knowledge Review (2019), Cyber ethics is the study of ethics pertaining to computers, covering user behaviour and what computers are programmed to do, and how this affects individuals and society. With the increase of young

children using the internet, it is now very essential than ever to tell children about how to properly operate the internet and its dangers. It is especially hard to talk to teens because they do not want to be lectured about what is right and wrong. They seem to think they have it all sorts out. It further states that cyber ethics concerns to the code of responsible behaviour on the Internet and some people try to hide behind a false sense of obscurity on the internet, believing that it does not matter if they behave badly online because no one knows who they are or how to search them.

Cyber Ethics aims at giving orientation about right and wrong, good and bad, related to the cyber space. It tries to apply and modify fundamental values and virtues to specific new challenges and situations arising from cyber technologies and cyber society. As cyber space influences all parts of society, cyber ethics includes almost all ethics domains.

RESEARCH METHODOLOGY

The survey method used was a convenient sampling method in which respondents of 150 youths were selected in Wuse District of Abuja Municipal Local Area Council (AMAC). The total population of youths in AMAC was 305, 603 as at 2016 (Source: https://www.citypopulation.de/php/nigeria-admin.php?adm2id=NGA015002). A total number of 150 questionnaires were distributed and collected at the same time. All the questionnaires were validly filled with the assistant of the researchers. The instrument used for data collection was questionnaire to find out the issues on information systems, ICT, Cybercrime, cybersecurity, cyberethics and national security. The scale that was used for the questionnaire is Likert's Summated Rating Scale (LSRS) with the following parameters (SA = Strongly Agree, A =Agree, D = Disagree, SD =Strongly Disagree) which the research weighed as 4, 3, 2 and 1 point respectively. The outcome of the results was analyzed in percentages and mean, and are represented in the tables below.

Table 1: What do you understand as the main aim of national security policy in Nigeria?

S/N	The main aim of the national security policy in Nigeria	SA	A	D	SD	TOTAL	MEAN ($\bar{x}$)
1.	To ensure that our national survival is free from the internal and external threat	105 (420)	45 (135)	- (0)	- (0)	150 (555)	3.70
2.	To ensure that our territorial integrity is free from external infringement	53 (212)	58 (174)	28 (56)	11 (11)	150 (453)	3.02
3.	To ensure that our political independence and sovereignty is intact	4 (16)	81 (243)	52 (104)	13 (13)	150 (376)	2.51
4.	To ensure that our economic system and development proceed smoothly	18 (72)	46 (138)	59 (118)	27 (27)	150 (355)	2.37
5.	To ensure that our traditional way of life is protected and free from foreign interference and control	87 (348)	58 (174)	5 (10)	- (0)	150 (532)	3.55

Significant mean level = 3.03

From table 1, with the mean score of 3.70, the respondents agreed that what they think is the main aim of our national security policy is to ensure that our national survival is free from the threat. With the mean score of 3.02, the respondents slightly disagreed that the main aim of our national security policy is to ensure that our territorial integrity is free from infringement, while with the mean scores of 2.51 and 2.37, the respondents strongly disagreed that it is to ensure that our political independence and sovereignty is intact, and to ensure that our economic system and development proceed smoothly respectively. With the mean score of 3.55, the respondents agreed that it is to ensure that our traditional way of life is protected and free from foreign interference and control. From the result above, it is

obvious that the main aim of our national security policy in Nigeria is to ensure that our national survival is free from the threat.

Table 2: What is the impact of ICT in the life of the youths?

S/N	The impact of ICT in the life of the youths	SA	A	D	SD	TOTAL	MEAN ($\bar{x}$)
1.	ICT has transformed the way youths communicate and access information	120 (480)	16 (48)	11 (22)	3 (3)	150 (553)	3.69
2.	It has exposed the youths to various kinds of internet fraud	59 (236)	91 (273)	- (0)	- (0)	150 (509)	3.40
3.	It has changed the way young people interact socially	32 (128)	58 (174)	42 (84)	18 (18)	150 (404)	2.70
4.	ICT use has a risk factor of developing psychological health challenges among the youths	11 (44)	32 (96)	76 (152)	31 (31)	150 (323)	2.15
5.	It has offers opportunities for youth empowerment and education	48 (192)	71 (213)	31 (62)	- (0)	150 (467)	3.11
6.	ICT has led to unemployment and loss of job to our youths	35 (140)	66 (198)	41 (82)	8 (8)	150 (428)	2.85
7.	ICT has led to eradication of our culture among young people	81 (324)	62 (186)	7 (14)	- (0)	150 (524)	3.50

Significant mean level = 3.06

Table 2 revealed that the respondents agreed that ICT has transformed the way youths communicate and access information, exposed the youths to various kinds of internet fraud, offers opportunities for youth empowerment and education, and led to eradication of our culture among young people with mean scores of 3.69, 3.40, 3.11, and 3.50 respectively, while the respondents disagreed that ICT has changed the way young people interact socially, ICT use has a risk factor of developing psychological health challenges among the youths, and ICT has led to unemployment and loss of job to our youth with mean scores of 2.70, 2.15 and 2.85 respectively. From the above results, it can be deduced that ICT has majorly

impacted in the lives of the youths by transforming the way youths communicate and access information.

Table 3: How do you rate the management of cyber security and adherence of cyber ethics by internet users in Nigeria?

S/N	Rating of cybersecurity management and cyberethics use in Nigeria	SA	A	D	SD	TOTAL	MEAN ($\bar{x}$)
1.	The rate of cyber security management and adherence to cyber ethics by internet users in Nigeria is very high	3 (12)	32 (96)	33 (66)	82 (82)	150 (236)	1.71
2.	The rate of cyber security management and adherence to cyber ethics by internet users in Nigeria is moderate	21 (84)	40 (120)	53 (106)	56 (56)	150 (366)	2.44
3.	The rate of cyber security management and adherence to cyber ethics by internet users in Nigeria is low	59 (236)	71 (213)	11 (22)	9 (9)	150 (480)	3.20
4.	The rate of cyber security management and adherence to cyber ethics by internet users in Nigeria is very low	45 (180)	60 (180)	21 (42)	24 (24)	150 (426)	2.84
5.	The rate of cyber security management and adherence to cyber ethics by internet users in Nigeria is nothing to write home about.	54 (216)	81 (243)	15 (30)	- (0)	150 (489)	3.36

Significant mean level = 2.69

Table 3 indicated the rate of management of cybersecurity and adherence to cyber ethics by internet users. With the mean score of 1.71, the respondents disagreed that the rate of cyber security management and adherence to cyber ethics by internet users is very high. The respondents also disagreed that that the rate of cyber security management and adherence to cyber ethics by internet users is moderate with a mean score of 2.44, while the respondents agreed that that the rate of cyber security management and adherence to cyber ethics by internet users is low, very low, and nothing to write home about with mean scores of 3.20,

2.84, and 3.36 respectively. The above results therefore, indicate that majority of the respondents were of the opinion that there is nothing like cyber security management in Nigeria and no adherence to cyber ethics by internet users.

Table 4: What is the main method in which cybercriminals often use in defrauding people?

S/N	Main method cyber criminals often use in defrauding people	SA	A	D	SD	TOTAL	MEAN ($\bar{x}$)
1.	Making direct contact through emails and phone calls (social engineering)	91 (392)	20 (60)	21 (42)	11 (11)	150 (505)	3.37
2.	Downloading of malicious code through internet advertisement on an infected website (malvertising)	61 (244)	59 (177)	12 (24)	18 (18)	150 (460)	3.07
3.	Through unwanted emails and messages and bait offering for the victims to give out sensitive information (spamming and phishing)	28 (112)	70 (210)	32 (64)	20 (20)	150 (406)	2.71
4.	Through identity theft and fraud (yahoo-yahoo)	111 (444)	39 (117)	- (0)	- (0)	150 (561)	3.74
5.	Through lottery scam in which a victim is told that he/she has won a lottery	45 (180)	85 (255)	11 (22)	9 (9)	150 (466)	3.11
6.	Through online dating (social dating networks)	27 (108)	72 (216)	51 (102)	- (0)	150 (426)	2.84
7.	Through Facebook impersonation scam (Hacking on someone's Facebook account)	117 (468)	18 (54)	15 (30)	- (0)	150 (552)	3.68
8.	Through luring someone to believe that he/she can make money easily and fast on the internet	21 (84)	62 (186)	54 (108)	13 (13)	150 (391)	2.61

Significant mean level = 3.14

From table 4, with the mean scores of 3.37, 3.74, and 3.68, the respondents indicated that making direct contact through emails and phone calls, through identity theft and fraud

(yahoo-yahoo), and through Facebook impersonation scam (hacking on someone's Facebook account) are the methods often used by cyber-criminals to defraud their victims. While with the mean scores of 3.07, 2.71, 3.11, 2.68, and 2.61, the respondents indicated that downloading of malicious code through internet advertisement on an infected website, through unwanted emails and messages and bait offering for the victims to give out sensitive information, through lottery scam in which a victim is told that he/she has won a lottery, through online dating (social dating networks), and through luring someone to believe that he/she can make money easily and fast on the internet are the methods often used by cyber-criminals to defraud their victims. From the results above it is establish that the main method often used by cyber-criminals to defraud their victims is through identity theft and fraud (yahoo-yahoo).

CONCLUSION

From the findings of this paper, it is clear that the main aim of our national security policy is to ensure that our national survival is free from threat and to ensure that our territorial integrity is free from infringement. It is also discovered that ICT has impacted positively in the lives of the youths by transforming the way they communicate and access information and the negative aspect of the use of ICT by the youths is that it has led to the gradual eradication of our culture among young people. The rate of cybersecurity and adherence to cyber ethics by internet users is low and the majority of the respondents were of the opinion that there is nothing like cyber security management in Nigeria and no adherence to cyber ethics by internet users. The main method cyber-criminals often used to defraud its victims is through identity theft and fraud, and also through making direct contact with their victims using emails and phones calls.

RECOMMENDATIONS

From the results gathered, the following recommendations are made:

1. That the government should do more in sensitizing the public about cybersecurity through its agencies.
2. Internet users should adhere to the rules and regulations guiding computer usage by following the ten commandments of cyber ethics.
3. Youths should make positive use of ICT in improving their lives and take advantage of opportunities it offers.
4. The government should develop a strong policy and system to checkmate the over-bearing activities of cyber criminals and internet fraudsters.
5. Internet users should be careful on how they upload their vital and sensitive information on the internet including Facebook and Whatsapp.
6. The government should pay greater attention to cybercrime because of its effect on the economy of the nation.
7. Government should create more job opportunities to curtail the increasing rate of unemployment and thereby reduce the activities of jobless youths in cybercrime and internet fraud.

REFERENCES

Alter, S (2013). Work system theory: an overview of core concepts, extensions, and challenges for the future". *Journal of the Association for Information Systems*. 14 (2): 72–121. Retrieved from en.wikipedia.org/wiki/information-systems, January, 2019.

Bulgacs, S. (2013). The first phase of creating a standardized international technological implementation framework/software application. *International Journal of Business and Systems Research.* 7 (3): 250. Retrieved from en.wikipedia.org/wiki/information-systems, January, 2019

D'Atri A., De Marco M. and Casalino N. (2008). *The Interdisciplinary aspects of information systems studies.* Physica-Verlag, Springer: Germany.

Dashora, K. (2011). Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences,* 3 (1), 240-259

Ebijuwa, A. A. (2005). Information and communication technology in university libraries: The Nigeria experience. *Journal of library and Information Science, 7*(1&2), 23-30.

Ebunuwele, E. G., Ola, O. S. & Uduebor, E. A. (2014). Application of information communication technology in academic libraries in Nigeria. *International Journal of Education and Research, 2*(12), 423-436.

Halder, D. & Jaishankar, K. (2011). *Cybercrime and the victimization of women: laws, rights, and regulations.* Hershey, PA, USA: IGI Global.

https://www.citypopulation.de/php/nigeria-admin.php?adm2id=NGA015002)

Jessup, L. M. and Valacich J. S. (2008). *Information systems today (3rd ed.).*New York: Pearson Publishing.

Kroenke, D. M. (2008). Experiencing MIS. Prentice-Hall, Upper Saddle River, NJ

Latha, D. (2008). Jurisdiction Issues in Cybercrimes. *Law Weekly Journal, 4,* p. 86. *Available at* www.scconline.com (retrieved on August 29, 2019).

Lord, N. (2019). What is cyber security? Definition, best practices & more. Retrieved from https://digitalguardian.com/blog/what-cyber-security on 29 August, 2019.

Moore, R. (2005). *Cybercrime: investigating high-technology computer crime.* Cleveland, Mississippi: Anderson Publishing.

Morgan, S. (2016). Cybercrime costs projected to reach $2 trillion by 2019. *Forbes.* Retrieved 28 August, 2019.

Murray, J. (2011). Cloud network architecture and ICT - modern network architecture. ITKnowledge Exchange. TechTarget. Retrieved 2016-09-08 from sites.google.com/udavinww/home

Otto, G. & Ukpere, W. I. (2012). National security and development in Nigeria. *African Journal of Business Management, 6* (23), 6765-6770.

Paleri, P. (2008). *National security: imperatives and challenges*. New Delhi: Tata McGraw-Hill.

Reference.com (2019). https://www.reference.com/technology/meaning-ict-d11bb87f61c29a70#.

The Knowledge Review (2019). Cyber Ethics. Retrieved from https://theknowledgereview.com/cyber-ethics/ on 29 August, 2019.

ToAnyakoha, M. W. (2005). Information and communication technology (ICT) in library services. *Coal City Libraries, 2*(1&2), 2-12.

Schatz, D. Bashroush, R. & Wall, J. (2017). Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.*

Zuppo, C. M. (2016). Defining ICT in a boundaryless world: the development of a working hierarchy. *International Journal of Managing Information Technology (IJMIT)*. 2(1): 19. Retrieved January, 2019 from en.wikipedia.org/wiki/information_and_ communicationtechnology.

Zwass, V. (2019). Information system. Retrieved from https://www.britannica.com/topic /information-system on 29 August, 2019.