Global Scientific JOURNALS

GSJ: Volume 11, Issue 8, August 2023, Online: ISSN 2320-9186

www.globalscientificjournal.com

VARIATION IN THE UNDERSTANDING OF CYBERCRIME TERMINOLOGIES AND NEW TECHNOLOGY AND ITS IMPACT ON INVESTIGATING CYBERCRIME IN NORTHEAST POLICE COMMANDS OF NIGERIA

By

EGERE AUGUSTINE N.
BSc, PGDE, MSc.
Department of Computer Science
Federal Polytechnic Bali, Taraba State
Contact: +234 9066422616

Abstract

Cybercrime is a menace that should be eradicated or reduced to a very minimal level for our great nation to breakeven. This study titled, "Variation in the understanding of cybercrime terminologies and new technology and its impact on investigating cybercrime in Northeast Police commands, examined the extent to which understanding new technologies varies across the northeast zone and how such variations impact cybercrime investigation. Survey research methods was used while Data collected were based on a set of Scales in the Questionnaire Cybercrime - Related Scales (QCRS) consisting of twenty (20) items and were administered to police Command across the Zone with a sample of 500 police. The instruments were found to be reliable at 0.87 and 0.91 respectively while two hypotheses were generated and tested at a 0.05 significant level. Data were analysed using Chi-square, regression, and Spearman rank correlation Statistical method through statistical package for social sciences (SPSS) version 21 to test for the relationship between the dependent and independent variables at level $p < 0.05$ considered as the cut-off value for significance. Finding indicates that there is no significant relationship between the understanding of Cybercrime terminologies, new technology and investigating cybercrimes across the Northeast region of Nigeria Police commands. It is recommended among others that; there is a need for training and re-training of police personnel to equip them with the knowledge of tracking cybercrime, a proactive strategy for cybercrime prevention, prosecution, and adjudication by Nigerian law officers.

KEYWORDS: Cybercrime, Terminologies, new technology, variations, Nigerian Police, Northeast

Introduction

In recent times, our society is gradually becoming dependent on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for massive gain in productivity, efficiency and communication they also create dodge which may totally destroy an organisation. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network (Okeshola, 2013). This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. The capability of grassroots police forces to be able to help victims of cybercrime is significantly important in addressing the national increase in cybercrime. This study "The variation in the understanding of cybercrime terminologies and new technology and its impact on investigating cybercrime in Northeast Police commands, aim at examining the extent to which understanding cybercrime terminologies and new technologies and varies across the northeast zone and how such variations impact cybercrime investigation.

Objective

The objective of this study is to;

1. Examine the extent to which understanding new technologies vary and how such variations impact cybercrime investigation in the Northeast.

Research Question

1. To what extent does variation in the understanding of cybercrime terminologies and new technology impact cybercrime investigation in the Northeast?

Research Hypothesis

H_0: There is no significant relationship between the understanding of Cybercrime terminologies and new technology across the Northeast states of Nigeria Police commands.

H_1: There is a significant relationship between the understanding of Cybercrime terminologies and new technology across the Northeast states of Nigeria Police commands.

Scope of the study

This study titled “The variation in the understanding of cyber technology and its impact on investigating cybercrime in Northeast Police commands”, is restricted to the Northeast police commands which comprises of Adamawa, Bauchi, Borno, Gombe, Taraba, and Yobe respectively.

Literature Review

Basic Concept of Cybercrime

Cybercrime is an emerging trend that is gradually growing as the internet continues to penetrate all sectors in our societies and no one can predict its future. The crimes usually require a hectic task to trace. Cybercrime may be divided into two categories:

1. Crimes that affects computer networks and devices directly. Examples are malicious code, viruses as malware etc.

2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Advance fee fraud such as Yahoo Yahoo, Money theft through the ATM, Fake documents or Certificates, SMS requesting you to provide bank details as Bank Verification Number (BVN).

Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cyber-crime (Hassan, 2012)

a. Unemployment: This is one of the major causes of Cybercrime in Nigeria. It is a known fact that over 20 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.

b. Quest for Wealth: This is another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.

c. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.
d. Incompetent security on personal computers. Some personal computers do not have proper or competent security controls, it is prone to criminal activities hence the information on it can be stolen.

Growing menace of Cyber Crime in Nigeria

The absence of an enabling legislation on Nigeria's cyberspace has continued to increase concerns over online safety, dwindling consumer confidence in e-commerce and other online financial transactions. Now that the internet has gone fully commercial, affordable and mostly accessible, cases of cybercrime are on the increase. A number of institutions, particularly internet banking and other online transactions, have become targets of cyber criminals, with varying degree of success (This day, 2012). Dubious persons send scam email messages to victims requesting information like login accounts and passwords amongst others in order to defraud the unsuspecting preys. Theft of identity, spamming, unauthorized access, cyber bullying, cyber stalking, amongst others, are some of the rampant cases of cybercrimes in Nigeria today. As the country integrates electronic payment system into its financial institution; a step that is expected to accelerate the nation's e-commerce growth, the negative impact of cybercrime on businesses, and the absence of appropriate laws to guarantee the legality of online transactions, continue to create fear in the mind of users and potential online users.

The Nigeria Police and Cyber Crime

Modern societies are characterized by what can be termed 'police fetishism, the ideological assumption that the police are a functional prerequisite of social order so that without a police force chaos would ensue. Many societies have existed without a formal police force of any kind, and certainly without the present model. It is important to distinguish between the ideas of 'police' and 'policing'. 'Police' refers to a particular kind of social institution, while 'policing' implies a set of processes with specific social functions. 'Police are not found in every society, and police organizations and personnel can have a variety of shifting forms.

The police are agents of the state, established for the maintenance of order and enforcement of law. Therefore, like the state, the character, roles, and priority of police forces are determined by the political and economic structures of their nations. Similarly, the form and activities of policing by state and non-state agencies are also dependent on the character and composition of the political economy of society. The tasks of police are dictated by the contradictions and conflict of interests among groups and classes in society which if not regulated can threaten the preservation of the prevailing social order or status quo. In very substantive ways, the police mirror the contradictions and conflicts as well as human cooperation in society.

A student of the political institutions of any country desirous of understanding the "ethos" of any country's government can hardly do better than make a close study of its police system, which will provide him with a good measuring rod of the actual extent to which its government is free or authoritarian. The political economy frame of analysis is therefore appropriate to the analysis of police and policing in any society. There are different political economy models of analysis. However, there are common grounds among them, the principal ones being

(1) that there are intricate linkages between the political and economic structures of society;

(2) that the political and economic structures of a society determine its general values, cultures, and norms as well as the direction and practice of governance, and

(3) that a more robust analysis of society is provided by an understanding of the linkages between the economy and polity and their dialectical interrelations with other structures and social institutions. The most popular strand of political economy is the Marxist model. Its main argument is summarized by the famous statement by Karl Marx in the Preface to A Contribution to the Critique of Political Economy According to Marx, In the social production of their existence, men inevitably enter into definite relations, which are independent of their will, namely relations of production appropriate to a given stage in their development of material forces of production. The totality of these relations of production constitutes the economic structure of society, the real foundation, on which arises a legal and political superstructure and to which correspond definite forms of social consciousness.

Cyber Crime Policing, Nigeria Police and the Challenge

The relevance of electronic information systems is obvious to all in the modern economy. When information fails to circulate, whole sectors of the economy are vulnerable. Finance, wholesale and retail trade, transportation, much of manufacturing, and many service industries would slow to a crawl without computers. Vital public services – utilities, national defense, and medicine are equally dependent. Information security which is the safeguarding of computer systems and the integrity, confidentiality, and availability of the data they contain has long been recognized as a critical national policy issue. Two current trends indicate that its importance is on the increase.

The integration of computers into more and more aspects of modern life continues appreciating. Second, cyber-attacks, or breaches of information security, appear to be increasing at an alarming rate, and few observers are willing to ignore the possibility that future attacks could spell doom to any economy if left unchecked.

The agencies responsible for the prevention, protection, investigation, and possible prosecution of cyber-crime offenders are the police, military as well as paramilitary agencies in Nigeria. The argument is how equipped and motivated are our law enforcement agencies to face the challenges of protecting Nigerians from cyber-attacks.

Nigeria has a national and unified Police Force with two main departments; Criminal Investigation that takes care of crime detection and prevention, and Mobile Police unit used to track down hardened criminals. This is accompanied by two axillaries; the Special Constabulary and Traffic Warden Service.

Crime Trends in Northeast Nigeria (2015–2021)

Northeast Nigeria has faced significant security challenges, including insurgency and communal conflicts, which have contributed to the evolving crime landscape. This literature review seeks to delve into crime statistics within the region from 2015 to 2021, highlighting the emergence and consequences of cybercrime as a distinctive aspect of the criminal milieu. During this period, the northeast region experienced a range of criminal activities, including terrorism, kidnapping, armed robbery, and communal clashes (Abba & Yahaya, 2020). The activities of Boko Haram and other extremist groups continued to have a significant impact on crime statistics (Mshelizza & Alkali, 2018). However, cybercrime emerged as a growing concern, reflecting the increased reliance on technology and the internet in the region (Eneh & Udofia, 2017). While traditional crimes remained prevalent, cybercrime gained traction as the region's digital landscape expanded (Ene, 2019). Cybercriminal activities such as online fraud, phishing, identity theft, and hacking began to pose serious challenges, targeting individuals, businesses, and government institutions (Gwamna & Tukur, 2018). The lack of robust cyber security measures by law enforcement agencies and digital literacy exacerbated the vulnerability of the region's population to these cyber threats. The impact of cybercrime on the Northeast region was multifaceted. Individuals and businesses faced financial losses and reputational damage due to cyber-attacks (Iliyasu et al., 2017). Furthermore, cybercriminals exploited the region's existing instability to further their agendas, ranging from financial gain to disseminating misinformation (Aminu & Adagye, 2019). This compounded the security challenges already faced by the region. Efforts to combat cybercrime during this period were impeded by challenges such as limited resources, ineffective legislation, and the lack of technical expertise among law enforcement agencies (Okoli & Enwereuzoh, 2019). Additionally, the focus on countering insurgencies often diverted attention from the urgency of addressing cyber threats (Adelabu et al., 2018). Addressing the rise of cybercrime requires a comprehensive approach. Strengthening cyber security awareness, updating legal frameworks to address cybercrime, and investing in training for law enforcement personnel at local police stations are key components (Oduh & Oni, 2020). Collaborative efforts involving government bodies, international organizations, and the private sector were essential in bolstering cyber security measures (Ibrahim & Aliyu, 2021).

Brief Empirical Literature

Study undertaken by Idowu and Maikano, (2021), employed a survey method to source for data from 150 respondents from Wuse, Abuja FCT, Nigeria. The findings of the study revealed that the major perpetrators of cybercrime are young males, unemployed youths, and students within the age ranges of 21 – 35 years. They made use of Laptops, advanced Android/hi-phones, and the internet. It was also found that cybercrime is caused by unemployment, the quest for quick wealth syndrome, a corrupt society, and criminal mind of the youths, and weak criminal laws and implementation, among others. The study concluded that there are several multi-faceted factors militating against the control of cybercrime in Nigeria.

Olayemi, (2014) found that the productivity gaps between training, skills, deployment, and career advancement have proved the assumption in the Nigerian Police Force that training does not impact reasonably both the organization and the officers. This sustains their hypothesis that there is a relationship between corruption and poor human resource utilization in Nigeria.

Omodunbi, Odiase, Olaniya and Esan (2016), presents the prevailing challenges experience in our society today, due to the growing reliance and importance of the internet. The paper studied the presents rise in moral decadence due to cybercrime using the average youth in secondary schools as case study in Nigeria. Finally, the study also highlights ways to mitigate the worrisome growing rate of cybercrime carried out in some key sectors in Nigeria, especially the Secondary School institutions and presents a brief examination of these crimes in some secondary schools within Kebbi and Sokoto State, and proposed methods of cybercrime prevention to effectively combat cybercrime rate in the educational sector.

Mbaskei (2016) in his publication on "Cybercrimes: Effect on Youth Development" noted that secret agents of the UPS (United Parcel Service) smashed a record scam with a face value of $2.1billion (about N252 billion) in Lagos. The interception was done within three months. Some of the instruments uncovered by the UPS were documents like Wal – Mart Money orders, Bank of America cheques, U.S postal service cheques and American Express traveler's cheques

Methodology

Survey design method was used while Data collected and collated were based on a set of Scales in the Questionnaire Cybercrime - Related Scales (QCRS) consisting of twenty (20) items and were administered to police Command/Barracks across the Zone; three Police Barrack from each of the State, making a total of eighteen (18) Barracks with a sample size of 500 polices officers. These instruments were validated and found to be reliable at 0.87 and 0.91 respectively. Two hypotheses were generated and tested at a 0.05 significant level.

Data were analysed using Chi-square, regression, and Spearman rank correlation Statistical Method through statistical package for social sciences (SPSS) version 21 to test for the relationship between the dependent and independent variables at level $p < 0.05$ considered as the cut-off value for significance.

Data presentation, analysis and interpretation

Ho: There is no relationship between the understanding of Cybercrime terminologies and new technology within and across the Northeast states of Nigeria Police commands

Name of State and how the rate the knowledge of cybercrime and cyber security Cross tabulation

Count					
		The rate of knowledge of cybercrime and cybersecurity?			Total
		High	Moderate	Low	
State	Taraba	11	12	61	84
	Adamawa	9	12	63	84
	Bauchi.	8	13	62	83
	Gombe	10	12	61	83
	Borno	9	11	63	83
	Yobe.	8	12	63	83
Total		55	72	373	500

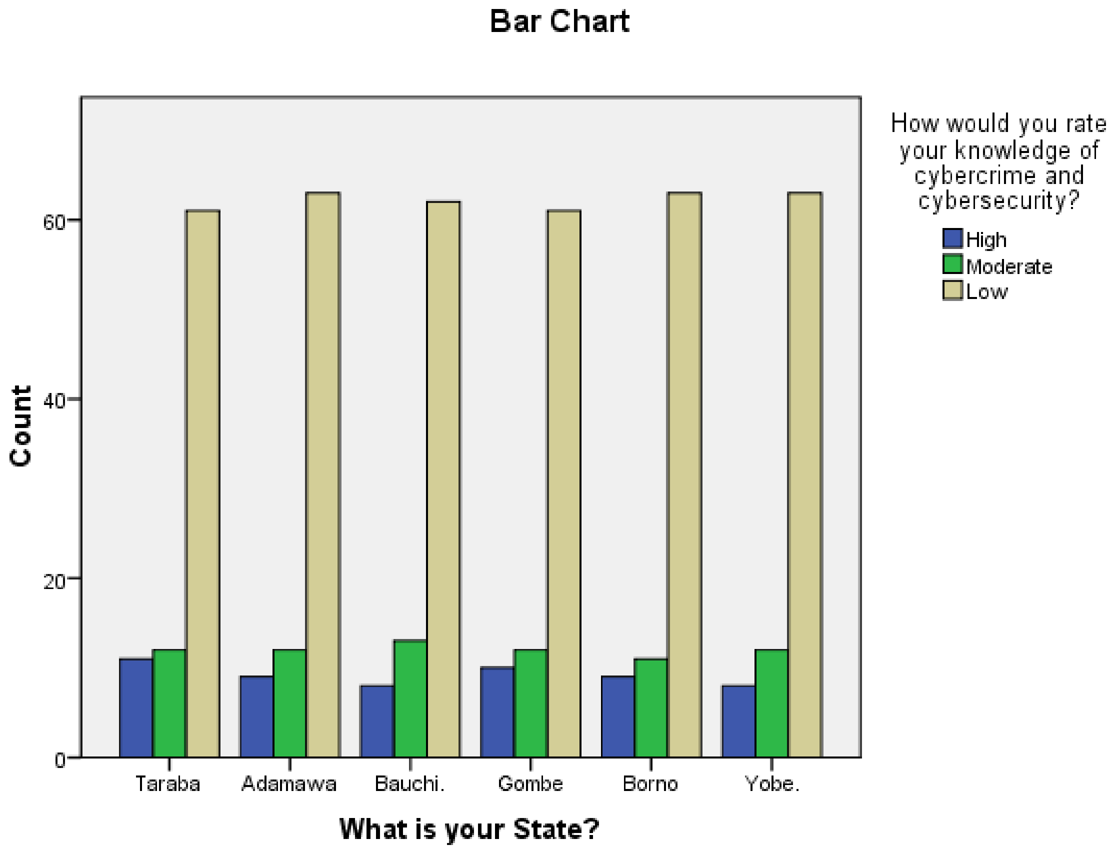

Figure 1

Table 1.1 shows the variation of the knowledge of cyber Crime and Cyber Security across the Six North-eastern States of Nigeria, the result shows that only 55 police officers out of 500 are highly knowledgeable in Cyber Crime and Cyber Security, 72 are moderately knowledgeable and 373 are low or has no knowledge of Cyber Crime and Cyber Security. These results point to the fact that North Eastern Police Command has very little knowledge to effectively tackle Cyber Crime and Cyber Security.

Figure 1 demonstrates the variation in the knowledge of Cyber Crime and Cyber Security in the North Eastern Police Command.

Table 1.2

Chi-Square Tests

	Value	DF	Asymp. Sig. (2-sided)
Chi-Square	.973[a]	10	.000***
Likelihood Ratio	.963	10	.000***
Linear-by-Linear Association	.278	1	.000***
No. of Valid Cases	500		

Source: SPSS version 21 Computation (2023)

H_0: There is no significant relationship between the understanding of Cybercrime terminologies and new technology within and across the Northeast states of Nigeria Police commands.

H_1: There is a significant relationship between the understanding of Cybercrime terminologies and new technology within and across the Northeast states of Nigeria Police commands.

The table above revealed that the X^2 calculated value of **0.973** is less than the X^2 critical value of **18.307** at a 0.05 level of significance. The null hypothesis is therefore upheld and the alternative rejected. This implies that there is no significant difference between cybercrime across the states in the Northeast zone. In other words, there is no relationship between the understanding of Cyber terminologies and new technology within and across the Northeast states of Nigeria Police commands.

Findings

From the data analysis above, the following was the major finding of the study:

There is no significant relationship between the understanding of Cybercrime terminologies and new technology within and across the Northeast states of Nigeria Police commands

Discussion of Findings

Finding of this study shows that there is no significant relationship between the understanding of Cybercrime terminologies and new technology within and across the Northeast states of Nigeria Police commands. This suggests that there is no disparity in the understanding (knowledge) of Cybercrime terminologies and new technology within and across the Northeast states of Nigeria Police commands. This is in line with the findings of Idowu & Maikano (2021), (Gordon & Richard, 2006; Wall, 2015 and McCuster, 2006).

Conclusion

Cybercrime is a menace that should be eradicated or reduced to a very minimal level for our great nation to break even. This study titled, "Variation in the understanding of cybercrime terminologies and new technology and its impact on investigating cybercrime in Northeast Police commands, examines the extent to which understanding new technologies varies across the northeast zone and how such variations impact cybercrime investigation. Descriptive and survey research methods were used while Data collected and collated were based on a set of Scales in the Questionnaire Cybercrime - Related Scales (QCRS) consisting of twenty (20) items and were administered to police Command/Barracks across the Zone; three Police Barrack from each of the State, making a total of eighteen (18) Barracks with a sample size of 500 polices. These instruments were found to be reliable at 0.87 and 0.91 respectively. Two hypotheses were generated and tested at a 0.05 significant level.

Data were analysed using Chi-square, regression, and Spearman rank correlation Statistical Method through statistical package for social sciences (SPSS) version 21 to test for the relationship between the dependent and independent variables at level $p < 0.05$ considered as the cut-off value for significance. Finding indicates that there is no significant relationship between the understanding of Cybercrime terminologies and new technology within and across the Northeast states of Nigeria Police commands.

Limitations

The following are some of the limitations identified by the study;

i. **Lack of Specialization**: Traditional law enforcement agencies, including the police, lack specialized units or personnel with the technical expertise needed to investigate and respond to complex cybercrimes effectively.

ii. ii. **Limited Resources:** Adequate resources, including technology, training, and personnel, are necessary to combat cybercrime. Inadequate funding and resources hinder the police's ability to establish and maintain effective cybercrime units.

iii. iii. **Rapidly Evolving Tactics**: Cybercriminals constantly adapt their tactics to exploit new vulnerabilities and technologies. Law enforcement agencies need to stay updated and trained to keep up with these changes.

iv. iv. **Legal and Regulatory Challenges**: The legal framework around cybercrime might not be comprehensive or up-to-date, making it challenging to prosecute cybercriminals effectively. Additionally, navigating legal procedures and obtaining necessary warrants can be complicated in the digital realm.

v. Lack of Reporting: Many cybercrimes go unreported due to various reasons, including lack of awareness, fear of repercussions, or a belief that reporting won't lead to a resolution. This makes it difficult for law enforcement to take action.

Recommendations

Having examined the various aforementioned concepts on this subject matter, there is a strong and desperate need for governments to provide funding to the anti-cybercrime agencies involved to enable them to purchase modern technological equipment that will match them to the strength of the crimes committed and not continue to play a catch-up game. Hence,

1. Computer technology curriculum: Most law enforcement actors are not equipped with the necessary technological knowledge, whereas Internet criminals are experts in computer technology. To combat these crimes, it is necessary to educate and develop human resources as one of the most reliable strategies. In addition, universities, schools of higher education, and academic institutions should open special courses designed to allow future generations of judges, prosecutors, and lawyers to be trained in this very vital area.
2. Capacity-building programmes for stakeholders: There must be an improvement in the operational capacity and response of law enforcement authorities against cyber-attacks. In this context, it is necessary to increase the number of experts in the field of investigating and prosecuting cybercrime. This is possible by frequently organizing specialized training and sending relevant officials abroad for specialization training. The specialization of experts in the field of cybercrime, as well as increasing their knowledge of domestic and international legislation in the field, and on the methods

and ways of implementing this legislation in the most adequate and effective ways can be achieved through these trainings.

3. There is a need for training and re-training of police personnel to equip them with the knowledge of tracking cybercrime.
4. We recommend a proactive strategy for cybercrime prevention, prosecution, and adjudication by Nigerian law officers.
5. Cooperation, awareness, and enlightenment campaigns: The existence of a suitable legal framework is not enough to fight criminality, such as cybercrime. An effective implementation based on the practice of the legal framework is also crucial. This can be achieved by, among other things, cooperation among investigative agencies and digital forensic laboratories (e.g. sharing information about procedures for the preservation and collection of digital evidence, cooperation to obtain the results of analysis promptly, etc.).

Suggestions for further Studies

This study is restricted to the Nigerian Police in the Northeast region of Nigeria. Hence, the result may not be generalized to other regions due to differences in development index and the understanding of the application of cybercrime measures may also differ. Prospective researchers are charged to use different methods, and possibly larger sample for healthier comparison

Study Impacts

= The target audience for this work is the Nigerian Police Force, starting with the Northeast States Police Command. Police officers are faced with new and evolving challenges relating to cyber threats. According to Gottschalk, the opportunities available to cyber criminals are almost endless, and the interconnected world in which we live has generated a multitude of new crime types and modus operandi, as well as new threat actors (Gottschalk, 2010). The proposed work is expected to enhance the Police Forces' understanding of cyber security technologies, cybercrime, capacity to investigate and prosecute cybercriminals, and ability to mitigate or counter cyber security threats. It will also help the stakeholder to better identify relevant knowledge gaps amongst employees and how to provide adequate training. The training tool will be given to the Police and they will use it to identify the training needs of officers.

REFERENCES

Abba, S., & Yahaya, I. (2020). Terrorism and Security Challenges in Northeast Nigeria: An Empirical Analysis. Journal of Conflict Transformation & Security, 10(1), 45-60.

Adelabu, M. A., Osamor, V. C., & Chukwuma, J. I. (2018). Cybercrime, Cybersecurity and Challenges to National Security in Nigeria. International Journal of Advanced Computer Science and Applications, 9(9), 166-171.

Aminu, I., & Adagye, A. (2019). The Implications of Cybercrime on National Security in Nigeria. International Journal of Scientific & Engineering Research, 10(7), 1598-1605.

Aladenusi, T. (2019), *Nigeria Cyber Security Outlook 2019*, Deloitte. Available from https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2019.html

Apondi J. A. (2015) Impact of Instructional Materials on Academic Achievement in Mathematics in Public Primary Schools. A Research Project Submitted to the University of Nairobi. Siaya County, Kenya. (Unpublished)

Balsing K. R. (2020), *Cyber Economic Crime: Criminological Studies and Frameworks*. In the book: Cyber Economic Crime in India. DOI: 10.1007/978-3-030-44655-0_3

Balsing, K. R. (2020), *Exploring the Phenomenon of Cyber Economic Crime*. In the book: Cyber Economic Crime in India. DOI: 10.1007/978-3-030-44655-0_4

Balsing, K. R. (2020), *Integrated Cyber Crime and Cyber Security Model*. In the book: Cyber Economic Crime in India. DOI: 10.1007/978-3-030-44655-0_10

Better Evaluation (2016). Combining Qualitative and Quantitative Data. Retrieved from http://betterevaluation.org/plan/describe/combining_qualitative_and_quantitative_data

Blumer, H. (1956). *Sociological Analysis and the "Variable*". American Sociological Review, 21(6), 683-690.

Bryman, A. (2016). *Social Research Methods* (5th ed.). Oxford: Oxford University Press.

Clarice, C. (2017*), Investigating a research-informed teaching idea: The use of transcripts of authentic workplace talk in the teaching of spoken business English.* Elsevier, Volume 46, April 2017, Pages 72-89

Ekeji, C. C (2008) Cyber Cri me i n Nigeria

Eneh, S. E., & Udofia, E. J. (2017). Digital Crime and Cybersecurity in Nigeria: Emerging Issues and Challenges. European Journal of Computer Science and Information Technology, 5(2), 1-9.

Fredrick, I. (2015), *Nigerian Cyber Crime Bill An Imperative to the Nigerian Armed Forces*. Available from http://www.army.mil.ng/nigerian-cyber-crime/

Fredrick, I. (2016), *Cyberwarfare and National Security: An Imperative of Nigerian Army preparedness*. Available from: https://www.docdroid.net/hPuNFKv/1-cyber-warfare-and-national-security-an-imperative-of-the-nigerian-army-preparedness-by-ikerionwu-fredrick.pdf

Gwamna, J. M., & Tukur, H. B. (2018). Cybercrime in Nigeria: Challenges and Countermeasures. Journal of Cybersecurity Research, 3(1), 1-15.

Gordon, B. (2017), *Why research-informed teaching in engineering education? A review of the evidence*. European Journal of Engineering Education, Volume 42, 2017 - Issue 3

Gordon, S., and Richard, F. (2006). *On the definition and classification of cybercrime*. Journal in Computer Virology, 2(1), 13- 22.

Gottschalk, P. (2010). *Policing Cyber Crime*. Petter Gottschalk & Ventus Publishing ApS

Hamzaoui, M. and Faycal, B. (2019), *Cybercrime in Morocco A Study of the Behaviors of Moroccan Young People Face the Digital Crime*. International Journal of Advanced Computer Science and Applications. DOI: 10.14569/IJACSA.2019.0100457

Ibrahim, H. A., & Aliyu, M. (2021). Cybersecurity Measures and Challenges in Nigeria: A Review. International Journal of Advanced Research in Computer Science, 12(1), 60-65.

Idowu, O. A. & Maikano, M. (2021), Cybercrimes and Challenges of Cyber-Security in Nigeria

Iliyasu, Z., Dayyab, F. M., & Sadiq, I. A. (2017). The Economic Impact of Cybercrime on Nigerian Businesses. Journal of Cybersecurity Economics, 3(2), 123-136.

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). *Likert Scale: Explored and Explained*. British Journal of Applied Science & Technology, 7(4), 396-403.

Krosnick, J., & Presser, S. (2010). *Question and Questionnaire Design* 2nd Edition. In Handbook of Survey Research (pp. 263-313). Emerald.

Likert, R. (1932). *A Technique for the Measurement of Attitudes*. Archives of Psychology. New York.

Lindsey O'Donnell (2019), *ThreatList: Nigerian Cybercrime Surged 54 Percent in 2018*, Threatpost. Available from https://threatpost.com/threatlist-nigerian-cybercrime-surged-54-percent-in-2018/144561

Marin J., Nieto Y. Huertas, F. Montenegro, C. (2019), *Ontological model of cybercrimes: Case study Colombia*. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao

Matt H., Thaddeus E. and Lee S. (2018). *Policing the Cyber Threat: Exploring the threat from Cyber Crime and the ability of local Law Enforcement to respond*. European Intelligence and Security Informatics Conference (EISIC), 2018, Karlskrona, Sweden

McAfee (2014), *Net Losses: Estimating The Global Cost of Cybercrime*, Center for Strategic and International Studies. Available from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf

McCusker, R. (2006, December). *Transnational organised cybercrime: distinguishing threat from reality*. Crime, Law and Social Change, 46(4), 257-273

Mshelizza, I. S., & Alkali, U. (2018). Assessing the Socio-Economic Impact of Boko Haram Insurgency on Northeast Nigeria. African Security Review, 27(3), 237-252.

National Cybersecurity Centre (2018), *The Cyber Threat to UK Business* Available from http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file

Nigerian Army, 2016, *Cyberwarfare and National Security*. Available from http://www.army.mil.ng/cyber-warfare-and-national-security/

Nigerian Government (2015), *Cybercrimes (Prohibition, Prevention, Etc) Act, 2015*.

Oduh, J. O., & Oni, O. A. (2020). Cybersecurity in Nigeria: Current Challenges and Policy Implications. International Journal of Computer Science and Information Security, 18(4), 187-194.

Okoli, C. N., & Enwereuzoh, D. E. (2019). Cybersecurity Challenges and Strategies in Nigeria. International Journal of Computer Applications, 182(3), 13-19.

Olayemi, O. A. (2014), A socio-technological analysis of cybercrime and cyber security in Nigeria

Omodunbi, B., Odiase, P., Olaniyan, O. and Esan, A. (2016), *Cybercrimes in Nigeria: Analysis, Detection and Prevention*, FUOYE Journal of Engineering and Technology, Volume 1, Issue 1, September 2016

Sule, B., Bakri, M., Usman, S. Mohammed, K. T. & Muhammad, Aminu Y. (2021), Cybersecurity and Cybercrime in Nigeria: The Implications on National Security and Digital Economy

Thaddeus, E. and Egere, A. (2018), *Cybersecurity Atlas, Nigeria*. The 27th Nigeria Computer Society National Conference, July 2018, Ibadan, Nigeria

The Guardian 2017, the global ransomware attack. Available from https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

The Nigerian Police Departments (2020), https://npf.gov.ng/departments/

Wall, D. S. (2015). *The Internet as a Conduit for Criminal Activity*. Information Technology and the Criminal Justice System, 77-98.

Wang, V., Harrison, N., and Jeyong, J. (2020), *Internet Banking in Nigeria: Cyber Security Breaches, Practices, and Capability*. International Journal of Law Crime and Justice. DOI: 10.1016/j.ijlcj.2020.100415