Global Scientific JOURNALS

GSJ: Volume 11, Issue 8, August 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

Assessing Police Officers' Familiarity with Cyber-terminologies and Its Impact on Cybercrime Investigations in Northeast Police Commands.

Augustine N. Egere.
Department of Computer Science, Federal Polytechnic, Bali, Taraba State, Nigeria

Email: austinendudi@yahoo.com

Abstract

This study assesses the familiarity of police officers with cyber terminologies and their impact on cybercrime investigations in northeastern police commands of Nigeria. The research employed a survey approach, incorporating a comprehensive review of relevant literature. Data was gathered using the Cybercrime Related Scales (QCRS), a questionnaire comprising twenty items. The survey was administered to police Command/Barracks across the Zone, encompassing three Police Barracks from each state, totaling eighteen Barracks, and involving a sample of 500 police officers. The questionnaire's reliability was confirmed at 0.87 and 0.91, respectively. A research question and hypothesis were formulated and tested at a significance level of 0.05. Data analysis involved Chi-square and correlation Statistical Methods through the Statistical Package for Social Sciences (SPSS) Software package. The null hypothesis was retained while the alternative was rejected. The researcher concluded that there is no significant divergence in the familiarity of cybercrime terminologies on crime investigations among police officers in the Northeast states of Nigeria Police commands and recommends that there is a need for training and re-training of police personnel to equip them with the knowledge of cyber terminologies among others.

KEYWORDS: *Cybercrime, cyber-terminologies, Threats, Nigerian Police, Northeast,*

INTRODUCTION

This study aimed to explore and improve how local Police Forces can build their capabilities around cybercrime prevention and investigation by identifying issues that may be acting as a blocker. We also seek to understand the nature and level of relevant knowledge gaps, the impact of such gaps and individual differences, and what can be done to plug that gap and address identified mitigating issues. The ability of grassroots police forces to be able to help victims of cybercrime is significantly important in addressing the national increase in cybercrime. This task should not be left to specialized forces at the regional or national levels alone. The Police at the local level should be able to acquire the minimal knowledge required to investigate cybercrime in that locality. However, The Nigerian Cybercrimes Act 2015 (Nigerian Government, 2015) provides explanations and a wide range of activities that constitute cybercrime. Also, the UK College of Policing Cyber Spectrum provides widely accepted definitions for cybercrimes and related terminologies. This is presented under four broad classifications, including Digital Footprint, Internet Facilitated, Cyber-Enabled, and Cyber Dependent crimes. The spectrum is produced by the UK College of Policing, which is the body responsible for the development of police learning and skills. Gordon and Richard, (2006) examined the existing definitions of cyber-related terms and proposed, according to them, "a more concise definition of the terms". Two cybercrime case studies were used to illustrate these terms. Although this is fairly old research, it provides a useful background from which our research can draw. To achieve this aim, we analyse relevant data and design a knowledge-based system for gauging the knowledge levels of police officers and suggesting training requirements. The data for this research are drawn from the six (6) Northeast Police Commands, literature, a review of crime statistics, and a surveyof police officers and police staff in the local forces, across the states.

PROBLEM STATEMENT/JUSTIFICATION

Improving cybersecurity practices should not only rely on the technical ability or deployment of technical measures by individuals or organizations. There is a need for a renewed focus on simple advice and preventative measures. It is a key role of the police to provide such advice and investigate instances where cyber security has failed. So, policing, up to the local level, has to move from a traditional 'analog' approach to crime investigation to tackle the digital threats that are growing in severity and frequency. Many Nigerians are increasingly becoming victims of different levels of cybercrimes – e.g., fraud, scams, account hacking, sextortion, blackmail, etc. (Omodunbi et al., 2016) however, the Police, mainly at the local level, are not adequately equipped/trained to deal with this challenge.

The opportunities available to cybercriminals 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).

There is a valid argument that the increase in cybercrime is not necessarily representative of 'new' crime types or offenses that haven't previously existed and that the so-called cybercrime, when dealt with in the criminal justice system, is treated no different from any other traditional crime type (Gordon & Richard, 2006; Wall, 2015 and McCuster, 2006). However, the investigative requirements for cybercrime pose significantly different challenges to that of traditional crimes and so it is significantly important that the Police, at all levels, rise to this challenge.

OBJECTIVES OF THE STUDY

The study seeks to assess Police officers' familiarity with cyber terminologies and their impact on Cybercrime Investigations in Northeast Police Commands. The study is limited to the Northeast states which comprise Adamawa, Bauchi, Borno, Gombe, Taraba, and Yobe states of Nigeria.

SIGNIFICANCE OF THE STUDY

This study focuses on how the Nigerian Police tackle cybercrime and support the ongoing work being conducted within Nigeria Policing to inform policing best practices and to identify risks, and opportunities to build upon the current strategic response to the cyber threat. It is hoped that the study would help the policymakers, government, industries (Nigerian Police force), and thevulnerable Northeast region realize the benefits accruing from this study thereby collectively engaging in combating this crime. It is also hoped that this research work has unarguably expanded and increased the stock of literature which is scanty.

RESEARCH QUESTION

The main research question to be addressed in this research is:

1. To what extent does the variation in knowledge of police officers on cyber terminologies impact cybercrime investigation in northeast police commands?

RESEARCH HYPOTHESIS

To achieve the purpose of this study, one hypothesis was formulated to guide the researcher:

$\boldsymbol{H_0}$: There are significant differences in variation in knowledge of cyber terminologies among police officers on cybercrime investigation across the Northeast states of Nigeria Police commands

$\boldsymbol{H_1}$: There are no significant differences in variation in knowledge on cyber terminologies among police officers on cybercrime investigation across the Northeast states of Nigeria Police commands.

CYBERCRIME: DEFINITION AND CONCEPTUALIZATION

A primary problem for the analysis of cybercrime is the lack of a consistent and statutory definition for the activities that may constitute cybercrime (PJCACC, 2004; Yar, 2005). According to Smith et al. (2004), defining cybercrime raises conceptual complexities. Varied definitions of cybercrime do exist. In addition to the difficult definition, it is also called by a variety of terms such as computer crime, computer-related crime, digital crime, information technology crime (Maat, 2004), Internet crime (Wall, 2001), virtual crime (Lastowka and Hunter, 2004; Grabosky, 2001), e-crime (AIC, 2006) and net crime (Mann and Sutton, 1998). Cybercrime could reasonably include a wide variety of criminal offenses and activities. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was divided into two categories and defined thus:

1. Cybercrime in a narrow sense is any illegal behaviour directed using electronic operations that targets the security of computer systems and the data processed by them.

2. Cybercrime in a broader sense is any illegal behaviour committed using, or about, a computer system or network, including such crimes as illegal possession and offering or distributing information using a computer system or network.

Cyber threats and attacks have been a global economic and safety concern – they have increased both in number and sophistication. A study by Wag et al., (2020) looks at cyber security in the Nigerian Internet banking industry and reveals a transformation of the Nigerian cybercrime industry from low-tech cyber-enabled crimes to high-tech sophisticated breaches, with viruses, worms or Trojan infections; electronic spam mail; and hacking being the top most experienced breaches. Similar studies in other countries, for example, India Balsing, (2020), United Kingdom (Matt, 2018), Colombia (Marin et al, 219), and Morocco (Hamzaoui & Faycal, 2019), etc., agree with the findings in (Wang, et al., 2020). These studies also looked at general economic implications, the proliferation of cybercrimes, and the response of the criminal justice system.

It is important to note the significant role of the criminal justice system in fighting against cybercrimes. However, the success of this fight will largely depend on the level of cyber-related awareness and knowledge of both the public and law enforcement agencies (Matt, et al., 2018; Hamzaoui & Faycal, 2019; and Balsing, 2020). Whereas Matt, et al., (2018) look at how the level of cyber-related knowledge affects the ability of Police officers and staff to police the cyber threat, (Hamzaoui & Faycal, 2019) focuses on the study of human behaviour toward digital crimes. Balsing, (2020) analyses the specialized legal, institutional, and awareness efforts by the criminal justice system to deal with cyber economic crimes.

Another critical factor here is the unavailability of a unified definition of what constitutes a cybercrime. Cybercrimes sometimes cut across different geological and legal jurisdictions (McCusker, 2006) but the proliferation of relevant terminologies has not helped the fight against cybercrime. Studies by Gordon & Richard, (2006) and Matt et al., (2018) have looked at the impact of this confusion on the fight against cybercrime. Gordon & Richard, (2006) explores the breadth of computer-based crime and defines the emerging terminologies. Gordon & Richard, (2006) has provided a starting point for defining relevant terminologies. This has been adopted in recent efforts by Matt et al., (2018) to provide broader documentation, culminating in the recent UK College of Policing Cyber Spectrum (Appendix A) which provides the basis for the definitions in our study.

Although many studies are looking at the legal response to cybercrimes, limited studies are focusing on the ability of the Police, down to the grassroots, to successfully prosecute cybercrimes. A similar study has been completed in England (Matt, et al., 2018). The study analyzed crime data and statistics in one Police force and revealed how confusion in the relevant terminologies and lack of cyber-related knowledge could affect the policing of the cyber threat. Our study will expand on that study to include a new system that will help in identifying the knowledge gap and training of grassroots (local) police officers. In building the new system, our study will draw from (Omodunbi et al, 2016 and Wang et al., 2020) and Appendix A for the relevant body of knowledge tailored to the Nigerian context.

Improving cybersecurity practices should not only rely on the technical ability or deployment of technical measures by individuals or organisations. There is a need for a renewed focus on simple advice and preventative measures. It is a key role of the police to provide such advice and investigate instances where cyber security has failed. So, policing, up to the local level, has to move from a traditional 'analog' approach to crime investigation to tackle the digital threats that are growing in severity and frequency. This is the focus of our study.

There is a valid argument that the increase in cybercrime is not necessarily representative of 'new' crime types or offenses that haven't previously existed and that the so-called cybercrime, when dealt with in the criminal justice system, is treated no different from any other traditional crime type (Gordon & Richard, 2006; Wall, 2015; McCuster, 2006). However, the investigative requirements for cybercrime pose significantly different challenges to that of traditional crimes. There is a need for Nigerian law enforcement agencies to be properly equipped at all levels.

In 2015 NASS passed the Nigerian Cyber Crime Act (Nigerian Government 2015 and Fredrick, 2015) and the president signed it into law. This was, according to the Nigerian Army, in response to cyberspace's increasing "*implication and challenges to Nigeria's national security*". The Nigerian Army is also prepared, and improving its capability, to also defend Nigeria in the cyberwar arena (Fredrick, 2015 and Nigeria Army, 2016). The Nigerian Police has several departments (Nigerian Police Department, 2020) but there is no specific department for policing the cyber threat. However, units are focusing on cyber-related crimes but these are mainly located at the top levels. There is a need to scale relevant skills down to the local formations.

The true scale and impact of cybercrime are largely unknown due to issues relating to awareness and how cyber incidents are reported. This can be attributed to the individual differences in perception and understanding of new technologies, cyber threats, and terminologies amongst relevant parties – victims of cybercrimes, call takers and recorders, first responders, and officers who are involved with investigation and prosecution (Matt, et al., 2018).

THE NIGERIAN PERSPECTIVE

In Nigeria, the relevant legislation is the Economic and Financial Crimes Commission (establishment) Act which is charged with the responsibility of investigating and prosecuting all economic and financial crimes.

Arguably, the closest office is found in s.1 (1) Advance Fee Fraud Act and Other Fraud-related Offenses Act 2006 which was enacted to ease the proof of these crimes. The Economic and Financial Crimes Commission is now charged with the responsibility of enforcing the provisions of the 2006 Act. Other major Acts are the Criminal Code as applicable in the South and the Penal Code operational in the North.

The critical question is how you apply the traditional provisions of the criminal code to offenses related to cybercrime, for instance, the offense of theft or stealing requires that tangible property be taken away to permanently deprive the victim of it. Applying traditional criminal concepts to acts involving intangible information can only mean that amendments to our criminal statutes are unavoidable. To strengthen this, point a look at s.484 of the criminal code, s.321 of the penal code, and s.348 of the shari'ah Penal Code Law of Zamfara State, which deals with personating reflects the shortcomings of our criminal sanctions to effectively deal with cybercrime.

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 thepolitical 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 societyis 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 ofpolitical 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 definiterelations, 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 relationsof production constitutes the economic structure of society, the real foundation, on which arisesa legal and political superstructure and to which correspond definite forms of social consciousness.

The mode of production of material life conditions the general process of social, Political,and intellectual life. Marx strongly argued that the economic structure of society determines the character of the superstructure which includes the political, legal, cultural, and religious relations and institutions of society. However, this does not imply a unidirectional model. The account is also taken of dialectical relations, a form of feedback process in which the superstructure also influences the economic substructure. Applied to police and policing, the model suggests that the problems of order, law, and lawlessness are to be understood as the reflections or products of the way the society organizes its economy, especially the dominant interests that drive it. Criminal law, whose enforcement constitutes the rationale for the establishment and sustenance of police and judicial institutions, contains rules prohibiting the behaviors and activities deemed detrimental to the dominant economic and political interests of society. However, societies are constituted into classes and groups with varying degrees of power or influence over political and economic decision-making. Classes and groups with dominant economic power control political decision-making, including the enactment of criminal law by the legislature, its enforcement, and interpretation by the police and judiciary respectively. No government governs by repression alone, precisely because this renders governance unstable, expensive, and unacceptable. Consequently, rulers also enforce compliance, law, and order usingpersuasion, indoctrination, and incorporation of diverse interests into public crime control and law enforcement policies. A holistic view is that police forces repress and at the same time servethe public. The priority attached to repressive and service functions varies across societies and even between regimes within society.

Arising from these arguments, it seems police work embodies ironies. Police are instruments of oppression and exploitation in totalitarian and unjust social systems. Yet they areessential to the preservation of justice and democracy... The police are guardians of social order.As an institution, the police force helps to preserve, fortify, and reproduce the prevailing social order and is hardly a catalyst for its charge. Hence, when social order is oppressive, exploitative,and unjust, the police preserve it by suppressing and defusing the demand for democracy and the elimination of oppression and injustices. Similarly, in a democratic, just, and equitable society, police have greater chances of serving as a vanguard for social democracy, human rights, and socioeconomic Analysis of the roles of state police must be located within the social, political, and economic order that police forces are required to secure, preserve, and fortify. Consequently, police roles and performance as well as police violence must be seen as the product of interactionamong political, economic, legal, institutional, and personality factors.

NIGERIA POLICE AND THE CHALLENGES OF CYBERCRIME POLICING

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.

First, the integration of computers into more and more aspects of modern life continues appreciated. 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 and 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 which takes care of crime detection and prevention, and Mobile Police unit used totrack down hardened criminals. This is accompanied by two axillaries; the Special Constabularyand Traffic Warden Service.

Nigeria, which is regarded as the hub or haven for cybercrime in the world, has witnessedthe creation of two outstanding crime commissions; the Economic and Financial Crimes Commission (EFCC) created in 2003, and the Nigerian Cyber-Crime Working Group (NCWG). While the EFCC is involved in all economic and financial-related crimes, the NCWG which was created in 2004 implements the objectives set up by the National Cyber-Security Initiative (NCI) and has its eyes more fixed on cyber-related crimes

Existing laws were inadequate and did not specify how perpetrators of cybercrime weresupposed to be prosecuted when arrested. This development is compelling state governments and regional organizations to enact legislations, and laws and form commissions that not only deal with specific crimes but that deal with cyber-crimes as a whole. Nigeria on the other hand has been in the spotlight from the international community for its involvement in cyber-crime. Itis ranked as the third in the world behind the United States and Britain, and the first within the African Continent in the rate of cyber-crime prevalence.

This commission was vested with the powers to investigate, prosecute, and penalize all economic and financial crimes relating to terrorism, money laundering, drug trafficking, and advanced fee fraud. Although these stipulations did not specifically mention cybercrime, EFCC does partner with other organizations in Marcel Onyema Eze, Ph.D.; Helen Nneka Agbo and Geraldine Chigbo Knowledge Review. The combat against cyber-crime because nowadays, most economic and financial crimes are committed with the use of the internet. To make up for the lapses of the EFCC Act, and to specifically address the issue of cyber and cyber-related crimes.

EFFECTS OF CYBERCRIMES ON THE NIGERIAN ECONOMY

i. Capital flight and loss of foreign investments: capital that was supposed to have come to Nigeria is diverted to other African countries as a result of a lack of confidence in Nigeria as a result of prevalent cybercrimes in the country.

ii. ii. Bad national image and reputation: This creates a lack of confidence in Nigeria and Nigerians. Foreigners avoid dealing with Nigerians like lepers and this leads to a lack of direct foreign investments. Also, many legitimate Nigerian online entrepreneurs are denied the opportunity to do business with nationals of other countries.

CHALLENGES IN CYBERCRIME INVESTIGATION

With escalations in reports of serious cybercrimes, one would expect to see a corresponding increase in conviction rates. However, this has not been the case with many investigations and prosecutions failing to get off the ground. The chief causes of this outcome may be attributed to trans-jurisdictional barriers, subterfuge, and the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology-aided crime. Cybercrime has been on the agenda of the Nigerian Government for many years. Investigations – in particular of fraud-related cybercrime – have been carried out in particular by the Nigeria Police Cybercrime Unit, Economic and Financial Crime Commission (EFCC). The Federal Government of Nigeria adopted the National Cyber Security Policy and Strategy otherwise known as "The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015". Gaps between the laws used for the prosecution of cybercriminals and enforcement procedures in the Cybercrime Act, of 2015 are often exploited by defense counsels when evidence tendered is found to be tainted and inconclusive to be admissible for the successful prosecution of cases. When cybercriminals are apprehended, they have unfettered access to renowned private attorneys who charge very high legal fees. This is not a problem for cybercriminals as they can readily afford to pay high professional fees to the best lawyers who specialize in cybercrime practice. Similarly, the presentation of digital evidence in legal proceedings is another important issue. Because lawyers and judges may havelimited technical knowledge, the presentation of digital evidence must be done in a clear, easily understandable manner. It is noted that most legal professionals have a limited understanding of technology and tend to lack confidence in the ability of technical specialists to produce evidence that is admissible in a court of law. Judges should have some understanding of the underlying technologies and applications from which digital evidence is derived to justly evaluate the merit of such evidence. Other serious challenges that are worth mentioning are the issues concerning best practices, testing of digital forensic tools, and expert witnesses. Numerous digital forensic techniques are used by investigators and examiners; however, no best practice guides are currently available. Laws and legislation regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cyber criminals in different countries. The current legislation on cybercrime in Nigeria needs to be reviewed to meet the standards in developed countries. Nigeria was a country sorely challenged by weak forensic capacity, but it now has a state-owned, high-powered DNA Forensic Laboratory Centre which was described as the first in the whole of West Africa, known as the Lagos State DNA Forensic Centre (LSDFC) in addition to the EFCC's Digital Forensic Lab equipped by the UK government.

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. The crime statistics within the region from 2015 to 2021, highlight 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 theiragendas, ranging from financial gain to disseminating misinformation (Aminu & Adagye, 2019).This compounded the security challenges already faced by the region. Efforts to combatcybercrime during this period were impeded by challenges such as limited resources, ineffectivelegislation, and the lack of technical expertise among law enforcement agencies (Okoli & Enwereuzoh, 2019). Additionally, the focus on countering insurgencies often diverted attentionfrom 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 enforcementpersonnel 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).

EMPIRICAL REVIEW

Sule, et al., (2021) examine the implications of cybercrime and weak cyber security defense for Nigeria's national security and digital economy from the perspective of non-traditional discourse within international security debates. The research adopted a qualitative approach to data collection and analysis, with both primary and secondary source data employed. The primary data involved in-depth interviews with selected informants from the relevant agencies in Nigeria and the available governmental policy documents on cyber security and cybercrime, including conversations with security personnel, academics, senior officials from security research institutes, members of private institutions, and government agencies in communication sectors. The secondary data consists of books, journals, and internet sources. Our analysis reveals that cybercrime is flourishing in Nigeria undetected, affecting its critical national infrastructure, and causing prolonged terrorism affecting national security and the safety of the national environment due to weak cybersecurity capability.

This 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 doesnot impact reasonably both the organization and the officers. This sustains their hypothesis thatthere is a relationship between corruption and poor human resource utilization in Nigeria.

Omodunbi, Odiase, Olaniya, and Esan (2016), present the prevailing challenges experienced in our society today, due to the growing reliance on and importance of the internet. The paper studied the present rise in moral decadence due to cybercrime using the average youth in secondary schools as a case study in Nigeria. Finally, the study also highlights ways to mitigate the worrisomegrowing rate of cybercrime carried out in some key sectors in Nigeria, especially SecondarySchool institutions and presents a brief examination of these crimes in some secondary schools within Kebbi and Sokoto State, and proposes 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 $ 2.1 billion (about N252 billion) in Lagos. The interception was done within three months. Some of the instruments uncovered by the UPS were documents like Wal – Wal-Mart money orders, Bankof America cheques, U.S postal service cheques, and American Express traveler’s cheques. Thisrecord scam is made possible as a result of the large number of young people who now see Cybercrimes or internet fraud as a source of livelihood. Nigeria itself is beset by a high rate of poverty- people living below the breadline, high unemployment, and corruption. Its people are willing to do anything, legal or otherwise, to make a living. However, since there is no clear legislation in Nigeria about cybercrime, it has become one of those grey areas increasingly exploited by unemployed young adults seeking an easy route to riches hence the emergence of a subculture called cyber criminals.

MATERIALS AND METHODS

Description of the study area

The area for this research is the North-east zone of Nigeria which consists of six (6) states including Adamawa, Bauchi, Borno, Gombe, Taraba, and Yobe.

RESEARCH DESIGN

The study adopted a simple survey design. 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. Five hypotheses were generated and tested at a 0.05 significant level.

DATA ANALYSIS TECHNIQUES

The data was analysed using descriptive statistics based on the themes and objectives of the study. The descriptive technique involved calculating means, standard deviation, and correlations. Correlation analysis was used to determine the relationship between dependent and independent variables. Data was screened, coded, and analysed through a statistical package for social science (SPSS, version 21.0) Chi-square and correlation Statistical Method through SPSS statistical Software computer package version 21 was used to test for the relationship between the dependent and independent variables at level $p < 0.05$ considered as the cut-off value for significance

RESULTS AND DISCUSSION

Table1.

Count					
		How would you rate your knowledge of cybercrime and cybersecurity?			
Types of cybercrime in Northeast Police Command?		**High**	**Moderate**	**Low**	**Total**
	Identity theft -	30	30	156	216

	Hacking -	10	19	89	118
	Social Engineering Attacks -	3	6	49	58
	Others -	12	17	79	108
	Total	55	72	373	500

Source: fieldwork, (2023).

Table 1. shows the variation in knowledge of police officers on cyber terminologies and their impacts on the type of Cyber Crime. The result shows that Identity theft Hacking is prevalent, as Social Engineering Attacks, and others across the northeastern states. The knowledge across cybercrime terminologies shows that only 55 are Highly knowledgeable, 72 are moderate and 373 are low in knowledge. The implication is that when the police officers are not familiar with the crime, there is no way they will be able to dictate and charge people who have committed such crimes. Figure 1 below shows the graphical representation of the types of crime and the individual knowledge of cybercrime by police officers in the zone.

Figure1

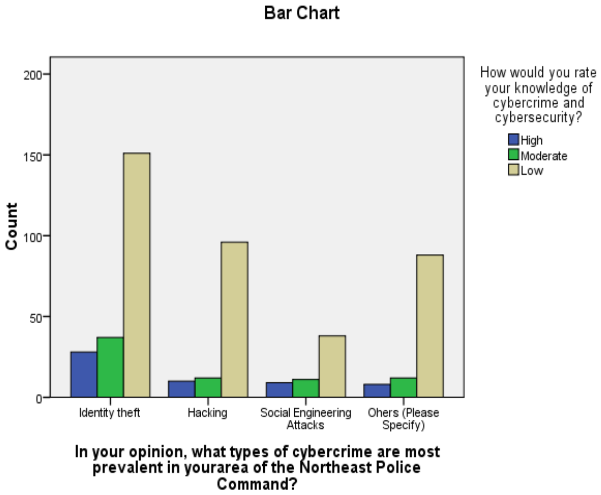

Table2

Chi-Square Tests

	Value	DF	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.153[a]	6	.000***
Likelihood Ratio	6.558	6	.000***
Linear-by-Linear Association	.926	1	.000***
No. of Valid Cases	500		

Source: SPSS version 21 Computation (2023)

Table 2 above revealed that the X^2 calculated value of 6.153 is less than the X^2 critical value of 12.592 at a 0.05 level of significance. Furthermore, Table 1 also revealed that there is a positive linear relationship of (0.926) in the variation in knowledge among police officers. The null hypothesis is therefore upheld and the alternative rejected. This implies that there is no significant variation in knowledge of these terminologies in cybercrime among police officers on the impact of cybercrime investigation across the Northeast states of Nigeria Police commands. The findings of this research revealed that there is no significant variation in the knowledge of these terminologiesin cybercrime among police officers on the impact of cybercrime investigation across the Northeast states of Nigeria Police commands. This implies that knowledge of these terminologies in cybercrime among police officers is almost the same in the investigation across the Northeaststates of Nigeria Police commands. The findings are in agreement with the study of (Matt, et al.,2018; Hamzaoui & Faycal, 2019; and Balsing, 2020).

CONCLUSION

In conclusion, this study embarked on a crucial journey to enhance the capabilities of local Police Forces in tackling the growing challenge of cybercrime prevention and investigation. By delving into the underlying issues obstructing progress, this research has shed light on the vital role that grassroots police forces play in aiding cybercrime victims and curbing the escalating trend of cyber offenses nationwide. The significance of bridging knowledge gaps within local law enforcement cannot be overstated, as it empowers officers to effectively address cybercrimes within their jurisdiction. The outcomes of this research contribute substantially to the broader objective of fortifying law enforcement's capacity to combat cyber threats. By ensuring that local Police Forces possess the necessary skills to handle cybercrimes effectively, the study echoes the imperative notion that the responsibility of countering cyber offenses extends beyond specialized regional or national units. Empowering local law enforcement with adequate cybercrime investigation knowledge serves as a cornerstone in the collective effort to mitigate cyber threats and provide swift assistance to victims.

RECOMMENDATIONS

1. There is a need for training and re-training of police personnel to equip them with the knowledge of tracking cybercrime.
2. We recommend a proactive strategy for cybercrime prevention, prosecution, and adjudication by Nigerian law officers.
3. 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.).
4. 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.

5. 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.
6. Establishing reporting channels for individuals and public- and private-sector organizations: Reports may trigger law enforcement investigations, provide intelligence for a better understanding of the scope, threat, and trends of cybercrime, and allow for collating data to detect patterns of organized criminality.

SUGGESTIONS FOR FURTHER STUDIES

This study is limited to the Nigerian Police in the Northeast region of Nigeria. These results may not be generalized to other regions as development indices differ and the understanding of the application of cybercrime measures may also differ. Potential researchers are enjoined to use different approaches, methods, and possibly larger same for better comparison

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 nsurgency 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