Grassroots Police Officers' Cyber-Terminology Knowledge and Its Impact on Cybercrime Investigations in Northeast Nigeria

Augustine N. Egere

Department of Computer Science, Federal Polytechnic, Bali, Taraba State, Nigeria

Abstract:

This study assesses the familiarity of grassroots 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 grassroots Police Forces can build their capabilities around cybercrime prevention and investigation by identifying issues that may be acting as a blocker. The researcher seeks to understand the nature and level of relevant knowledge gaps in terms of cybercrime terminologies, the impact of such gaps, and what can be done to plug 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 grassroots level should be able to acquire the minimal knowledge required to investigate cybercrime in their 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

Suggested Citation

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. 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 grassroots 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. Therefore, the study seeks to assess grassroots Police officers' familiarity with cyber terminologies and suggest training requirements. The data for this research are drawn from the six (6) Northeast Police Commands, which comprise Adamawa, Bauchi, Borno, Gombe, Taraba, and Yobe states of Nigeria.

**Literature review**

**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 cybersecurity 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 familiarity 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. Studies by 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 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. This study expands on the existing study to further identify the knowledge gap and training of grassroots (local) police officers. In proffering a solution, 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 at the grassroots police commands. Although units are focusing on cyber-related crimes, 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 among relevant parties – victims of cybercrimes, call takers and recorders, first responders, and officers involved with investigation and prosecution (Matt, et al., 2018).


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 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 the grassroots local police formations are key components (Oduh & Oni, 2020). Collaborative efforts involving government bodies, international organizations, and the private sector are essential in bolstering cyber security measures (Ibrahim & Aliyu, 2021).

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 terminology-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, the first step is being arraigned by the police on a charge bordering on cybercrime. If the police officer did not get it right, it results in judges striking the case out in court for lack of merit. It is also worthy of note that, cybercriminals have unfettered access to renowned private attorneys who charge very high legal fees. This is not a problem as they can readily afford to pay high professional fees to the best lawyers who specialize in cybercrime practice and terminologies.

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/hp-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), 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 worrisome growing rate of cybercrime carried out in some key sectors in Nigeria, especially Secondary School 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 recorded 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, Bank of America cheques, U.S postal service cheques, and American Express traveler’s cheques. This record 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. 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 police officers. These instruments were validated and found to be reliable at 0.87 and 0.91 respectively. One hypothesis was generated and tested at a 0.05 significant level.

Research Question

The main research questions addressed in this research are:

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, two hypotheses were formulated to guide the researcher:

\[ H_0: \text{There are significant differences in familiarity} \]

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 the dependent and independent variables. Data was screened, coded, and analysed through a statistical package for social science. 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 \( p < 0.05 \) is considered the cut-off value for significance.

Results and Discussion

<table>
<thead>
<tr>
<th>S/N</th>
<th>States</th>
<th>No police officer were selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Adamawa</td>
<td>84</td>
</tr>
<tr>
<td>2</td>
<td>Bauchi</td>
<td>83</td>
</tr>
<tr>
<td>3</td>
<td>Borno</td>
<td>83</td>
</tr>
<tr>
<td>4</td>
<td>Gombe</td>
<td>83</td>
</tr>
<tr>
<td>5</td>
<td>Taraba</td>
<td>84</td>
</tr>
<tr>
<td>6</td>
<td>Yobe</td>
<td>83</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>500</strong></td>
<td></td>
</tr>
</tbody>
</table>

terminologies was sort for in the questionnaire and Table 2 below shows the outcome

<table>
<thead>
<tr>
<th>Count</th>
<th>How would you rate your knowledge of cyber-terminologies</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>What is your State?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Taraba</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>Adamawa</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Bauchi.</td>
<td>8</td>
<td>13</td>
</tr>
<tr>
<td>Gombe.</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Borno.</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>Yobe.</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>Total</td>
<td>55</td>
<td>72</td>
</tr>
</tbody>
</table>


Table 2 shows by states the Variation in the knowledge of cyber terminologies across the Six Northeastern States of Nigeria. The result shows that only 13% of police officers from Taraba were very familiar with cybercrime terminologies, 14.3% were familiar, and a whole 72% were not familiar with cyber terminologies. This result was the same for the Gombe state as only 12% are very familiar with cyber terminologies, 12.45% are familiar and 73.5% are not familiar with cyber terminologies. The result equally shows that 75% of the police officers from Yobe, Borno, and Bauchi is not familiar with cyber terminologies. These results point to the fact that North Eastern Police Command has little or no personnel knowledgeable enough to effectively tackle Cyber Crime. However, a further test was conducted to evaluate the type of cybercrime existing in the zone to ascertain how to build competencies of the police officers to fight crime as shown in Table 3.

Table 1 shows the types of cybercrime prevalent in Nigeria's Northeast region and the variation in the familiarity of grassroots police officers with cybercrime terminologies. The result shows that Identity theft, Hacking, Social Engineering Attacks, and others are prevalent across the northeastern states of Nigeria. The knowledge across cybercrime terminologies shows that 55 (11%) are Highly knowledgeable, 72 (14.4%) are moderate and 373 (74%) are low in knowledge out of 500 police officers surveyed. The implication is that when police officers are not familiar with the crime terminologies, there is no way they will be able to dictate and charge people who have committed such cybercrimes. Hence the continuous trends of cybercrime in the region. Figure 1 below shows the graphical representation of the types of crime and the individual knowledge of cybercrime by police officers in the zone. A test was carried out to ascertain the variation in knowledge and impact of cyber terminologies among police officers in cybercrime investigation as shown in Table 4.
Table 3. Knowledge Rating of Officers on Types of Cybercrime Across States

<table>
<thead>
<tr>
<th>Types of cybercrime in Northeast Police Command?</th>
<th>How would you rate your knowledge of the following cybercrime?</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity theft -</td>
<td>High           Moderate            Low</td>
<td>216</td>
</tr>
<tr>
<td>Hacking -</td>
<td>30             30            156            118</td>
<td></td>
</tr>
<tr>
<td>Social Engineering/Attacks -</td>
<td>3              6             49             58</td>
<td></td>
</tr>
<tr>
<td>Others -</td>
<td>12             17            79             108</td>
<td></td>
</tr>
<tr>
<td>Total -</td>
<td>55             72            373            500</td>
<td></td>
</tr>
</tbody>
</table>


Figure 2. Cybercrime prevalence in the zone

Table 4. Chi-Square Tests

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
<th>DF</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson Chi-Square</td>
<td>6.153*</td>
<td>6</td>
<td>.000***</td>
</tr>
<tr>
<td>Likelihood Ratio</td>
<td>6.558</td>
<td>6</td>
<td>.000***</td>
</tr>
<tr>
<td>Linear-by-Linear Association</td>
<td>.926</td>
<td>1</td>
<td>.000***</td>
</tr>
<tr>
<td>No. of Valid Cases</td>
<td>500</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: SPSS version 21 Computation (2023)

Table 4 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 4 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 familiarities of these terminologies in cybercrime among police officers and this impacts on cybercrime investigation across the Northeast states of Nigeria Police commands. This implies that knowledge of these terminologies among police officers are almost the same in the investigation across the Northeast states 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 in the northeast part of Nigeria. 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 grassroots Police Forces possess the necessary skills to handle crimes effectively, the study echoes the imperative notion that the responsibility of countering cyber offenses extends beyond specialized regional or national units. Empowering grassroots 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. The imperative arises to impart training and continuous education to police personnel, equipping them with the requisite skills to track cybercrime.
2. It is essential to formulate a proactive strategy within the Nigerian law enforcement community to prevent, prosecute, and judiciously address cybercrime.
3. Collaborative efforts, consciousness-raising, and enlightenment campaigns are pivotal. A robust legal framework alone is insufficient to combat cybercriminal activities. Successful implementation, guided by this legal framework, hinges on effective cooperation among investigative agencies and digital forensic laboratories. This includes sharing protocols for preserving and gathering digital evidence, and expeditiously exchanging analysis outcomes.
4. A comprehensive curriculum on computer technology must be integrated. While many law enforcement professionals lack technological acumen, cybercriminals are well-versed in these matters. Countering such offenses necessitates the education and nurturing of human resources as a reliable strategy. Academic institutions, including universities and higher education establishments, should introduce specialized courses to train upcoming generations of judges, prosecutors, and lawyers in this critical domain.
5. Strengthening programs should target stakeholders to enhance their capabilities. Empowering law enforcement agencies to combat cyberattacks demands augmenting the ranks of experts proficient in investigating and prosecuting cybercrimes. This can be achieved through recurrent specialized training sessions and sending relevant officials for specialized instruction. These initiatives facilitate the specialization of cybercrime experts, augmenting their grasp of domestic and international cyber legislation, along with effective implementation methods.
6. The establishment of reporting mechanisms for individuals and entities in the public and private sectors is paramount. Reports can catalyse law enforcement inquiries, offer intelligence to fathom the breadth, nature, and trends of cybercrime, and enable the consolidation of data to discern organized criminal patterns.

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


