GOMBE JOURNAL OF ADMINISTRATION AND MANAGEMENT (GJAM)

Vol. 5 No. 1

Print ISSN: 2705-3407

Online ISSN: 2714-2442

May, 2023

POVERTY AND YOUTH ENGAGEMENT IN CYBERCRIME IN NIGERIA: AN OVERVIEW OF ITS EFFECT ON NATIONAL SECURITY

Abdullahi Alabi[1], Abdulrasheed Hamza Bamidele[2] & Abdulrazaq Bashir Oladimeji[3]
[1, 2 & 3]Department of Politics and Governance
Faculty of Humanities, Management and Social Sciences
Kwara State University, Malete, Nigeria
alabi.abdullahi@kwasu.edu.ng[1],
hamza.abdulrasheed19@kwasu.edu.ng[2]
oladimejiokoh@gmail.com[3]

Abstract
The number of internet users grows along with the number of cybercriminals, who appear to be transferring traditional stealing to the digital arena. Computer crime in Nigeria has evolved into a perplexing, if not the most difficult crime, with a projected financial loss of N250 billion ($649 million) in 2017 and N288 billion ($800 million) in 2018 in Nigeria, both young and old adults commit cybercrime; nonetheless, younger engagement, especially among those in higher education, is frequently linked to high levels of poverty, unemployment, insufficient cybercrime rules, and diminished social impact. This paper explores the relationship between poverty and youth engagement in cybercrime in Nigeria. Due to the nature of the investigation, secondary data and qualitative analysis methods were used. The results showed that teenage involvement in cybercrime is influenced by poverty and a lack of necessities of life. Also, it was found that youth involvement in cybercrime is significantly influenced by jobless and peer influences. The study suggests that the Nigerian government at various levels should provide basic facilities, enhance its cybercrime laws and policies, and retrain its social agents.

Key Words: Cybercrime, National Security, Poverty, Youth Engagement, Nigeria.

Introduction

High rates of poverty, the desire for riches, and inadequate security or among other factors, have been viewed as having combined to raise the rate of cybercrime among adolescents in Nigeria, constituting a serious concern for the nation (Bello, 2017). In the digital age, cybercrime is one of the biggest, most confusing, and possibly the most complicated problems. Cybercrime is the use of illegal activities committed using electronic, computer, and auxiliary equipment. It includes email bombing, virus dissemination, network traffic interruption, identity theft, computer hacking, and internet scams. Similarly, cybercrime comprises all sorts of crime done through the use of the internet. They are also known as online fraud. This entails presenting false solicitation to potential victims through one or more internet-based tools, including chatting and faxes, among others, or using them to defraud people or businesses. Information and communication technology (ICT) is used by cybercriminals throughout the continent to perform an infinite number of crimes that have caused and continue to cause many enterprises on the continent to fail (Ufuoma, 2020).

According to data from the Nigeria Multi-Dimension Poverty Index (2022), This survey was a collaborative effort between the National Bureau of Statistics (NBS), the National Social Safety-Nets Coordinating Office (NASSCO), the United Nations Development Programme (UNDP), the United Nations Children's Fund (UNICEF), and the Oxford Poverty and Human Development Initiative (OPHI). The survey, which sampled over 56,000 households across the 36 states of the Federation and the FCT, was conducted between November 2021 and February 2022, and provides multidimensional poverty estimates at senatorial district level. The highlights of the 2022 Multidimensional Poverty Index survey reveal that:63% of persons living within Nigeria (133 million people) are multi-dimensionally poor and The National MPI is 0.257, indicating that poor people in Nigeria experience just over one-quarter of all possible deprivations. This indicates that poverty rates have been rising. In addition, it is believed that the majority of Nigerians still live in squalor, and the country's rising rate of poverty has also been cited as a major contributing reason to the rise in cybercrime activities. This is based on the fact

that the nation's poverty index is still on the high side. Hassan et al (2012), Opined that those who participate in these illegal operations are frequently said to be struggling to make ends meet and turn to cybercrime as their only option. More than eighty per cent (80%) of Nigeria's e-businesses are vulnerable to cyber-attacks as a result of the alarming increase in cybercrime occurrences and the financial consequences that follow, endangering their existence.

Also, it has been noted that one of the main factors contributing to Nigeria's rising rate of cybercrime is the country's skyrocketing youth unemployment, which is demonstrated by the fact that most cybercrime perpetrators are young people who lack jobs. According to Aborisade (2009), five undergraduate students from the Universities of Abuja and Port Harcourt were detained by the Nigerian Police for allegedly utilizing the internet to access the websites of several banks and moving money from other people's accounts into their accounts. In the same vein, throughout a four-month operation called "Rewired," the Federal Bureau of Investigation (FBI) in the United States and the Economic and Financial Crimes Commission (EFCC) of Nigeria made 281 arrests. 167 of the 281 people detained for various offences were Nigerian teenagers (Olarewaju, 2020).

Statement of Problem

Over the past decade, there have been an exponential increase in the total number of hosts connected to the internet. In Nigeria, cybercrime has become one of the most widely used ways to steal money and engage in corporate espionage. Nigeria was ranked as the 16th most susceptible nation in Africa to cyberattacks as of 2016 by Check Point, a leading provider of network security (Ewepu, 2016). Young people commit cybercrime, according to Oludayo (2013), Suleiman (2016), John (2017), and Philip (2020), because of social influencers like family, religion, and peer groups. This is noteworthy given that on July 16, 2020, the EFCC, acting on a referral from the FBI, arraigned Kenneth Gift, a 22-year-old Uniport student, along with his mother and girlfriend, for internet scams. In the same vein, on January 28, 2020, Damilola Ahmed Adeyeri and his mother, Alaba Kareem Adeyeri, were found guilty on four counts of conspiracy and acquiring money through pretence totalling $82, 570 by the Federal High Court in Ikoyi, Lagos.

Bolaji (2016) asserts that Nigerians are well-known for being prolific cybercrime criminals both domestically and globally. A disproportionately high number of Nigerians have been detained for dishonest behavior by television broadcasters when compared to nationals of other countries. Nigeria's development has benefited from the Internet in many different ways. However, these sectors such as banking, e-commerce, and education, face challenges as a result of cybercrime. Each new cybercrime is more sophisticated than the one before it, and the number of these crimes is rising alarmingly. Olubokola (2017) stated that four of the top ten countries in the world with the highest incidence of cybercrime are in Africa (Nigeria, Cameroon, Ghana, and South Africa) in a 2011 World Bank report.

As it was predicted that Nigeria suffered an annual financial loss of N250 billion ($649 million) in 2017 and N288 billion ($800 million) in 2018, cybercrime activities in the country have been investigated as a driving force that posed a lot of negative economic consequences on the nation (Proshare, 2020). Alongside damaging the nation's brand, cybercrime makes it challenging for startups and small and medium-sized businesses to conduct business and discourages international corporations from making economic investments in the nation. Cybercrime operations have cost individuals money, intellectual property, or private information, and the harm can be severe. Senior citizens and other vulnerable people are frequently the targets of cybercrime. Over 62,000 Americans aged 60 or older reported losses totalling more than $649 million in 2018 (Proshare, 2020).

The Nigerian government has established mechanisms to address the issue as a result of the rising rate of cybercrime activities in the nation. Among them is the Economic and Financial Crimes Commission, which is tasked with the obligation of arresting and prosecuting anyone discovered committing an act of cybercrime, as well as providing jobs, retention programs, loans, and subsidies, among other things. The government's legal structure and level of policy implementation, however, are thought to be the primary causes of the rise in youth-related cybercrime.

Research Objective

This paper explores the relationship between poverty and youth engagement in cybercrime in Nigeria. The paper also conceptualizes some of the essential concepts, such as Cyber-security, Unemployment, poverty, and social influence to help readers catch the discussion.

Methodology

To realize the central objectives of this paper, the qualitative method was used and the secondary source was largely adopted in the area of cybercrime in Nigeria. The paper made use of data obtained from unpublished and published documents such as journals, newspapers, essays, textbooks, thesis and online materials.

Conceptual Discourse

Concept of Cybersecurity

The goal of cybersecurity is to protect cyberspace from threats, namely cyberthreats. The term "cyberthreat" refers to a broad variety of malicious actors using information and communication technology (ICT) either as a target or a tool to cause harm. National security may frequently be involved in some cases of cybersecurity; however, the two terms are frequently misunderstood, according to Nigeria Cybercrime Working Group (NCWG) coordinator Udotai (2002) and Odumesi (2006). The phrase "cybersecurity" only relates to the security of networks and systems, which include computers, electronics, and auxiliary equipment. As per Udotai (2002) and Odumesi (2006), common cyber-security concerns include information confidentiality, system integrity, and network survivability (CIS). Safeguarding systems and networks against illegal access, data manipulation from within, and defence against infiltration from without are among the major goals of cybersecurity. According to how it is frequently used, there are three aspects of cybersecurity:

a. A collection of activities and other non-technical actions designed to safeguard computers, data centres, related hardware, and software from threats to national security as well as the information they store, transmit, and convey, including software and data;
b. The level of protection brought about by the use of these practices and precautions;
c. The complementary sphere of professional endeavour, including research and analysis, focused on putting these activities into action and enhancing their effectiveness.

Because information security is at the core of the issue, cybersecurity is therefore more than just information security or data security but is also strongly tied to those two sectors. All facets of information protection are referred to as information security. These factors are typically divided into three groups: information availability, confidentiality, and integrity. Information is protected against disclosure to unauthorized parties by confidentiality, whereas information is safeguarded against unauthorized alterations by integrity. "Availability" means that upon request, the information should be made available to the appropriate parties. Accountability, which refers to the need for an entity's activities to be individually traceable to that entity, is occasionally added to the list.

According to Frank (2013), cyber-security is the grouping of techniques, concepts, and safeguards that can be utilized to secure an organization's and a user's assets online. It also includes training programs, best practices, assurance measures, and technological advancements. The assets of an organization or user comprise their staff, infrastructure, applications, services, digital infrastructure, and all of the information that is transmitted and/or stored in the cyber environment. To protect assets belonging to an organization and its users from appropriate security risks in the cyber realm, cyber-security aims to assure their attainment and maintenance. Consequently, from, the foregoing cyber-security can be seen as the following:

i. An issue with ICT that can be addressed as an information assurance or IT security issue, with a significant emphasis on Internet security. Hence, policies try to use technological tools like ports, anti-virus software, or intrusion detection software to combat threats to information systems.

The main hazards viewed include cyber-attacks as well as accidents, system failures, poor programming, and human error.

ii. Cybersecurity as an economic constraint. Business continuity, and notably e-business, which depends on constant access to ICT infrastructures and constant availability of business processes to enable optimal company performance, are both crucial to this issue. Private sector representatives are the key players. Viruses and worms, human error, hacker attacks of various kinds, and cybercrime are the biggest risks.

iii. Cybersecurity is considered a problem for law enforcement and as having an impact on cybercrime. The term "cybercrime" has many different definitions and can refer to anything from crimes made possible by technology to crimes against individual systems. Law enforcers are the major players. Cyberterrorism as well as a computer crime are the biggest threats.

iv. Cybersecurity is a problem for national security. Because they rely on ICT, society as a whole and its fundamental principles are at risk. Many layers are targeted in the threat's defense (the technical, legislative, organizational, or international levels). Security experts are the major players. In addition to information warfare threats from other states, terrorists pose the biggest menace.

Concept of Poverty

There are many ways to define poverty. Some scholars argue that it should be quantified, while others argue that a broader definition should be used. While some people interpret poverty in terms of income, many people think of it as multidimensional, based on indicators like (i) low income, (ii) low levels of education and health, (iii) impairment to wellbeing or financial difficulties, natural catastrophe, violence and crime, and education curtailment), and (iv) voice-lessness and powerlessness, such as: feeling discriminated against, lacking income earning opportunities, being mistreated by state institutions, and having no legal standing (Olubukola, 2017). According to the United Nations, poverty goes beyond a lack of money and useful resources for sustaining livelihoods. It shows up as starvation and malnutrition, restricted access to healthcare and other necessities, social isolation and prejudice, and a lack of involvement in decision-making. More than 736 million people in 2015 were living below the poverty level. Before the pandemic, 10% of the world's population struggled to meet even the most basic needs, including access to water and sanitation, education, and health care.

According to Rafiu, et al. (2017), poverty is considered a limitation that worsens people's purchasing power and living conditions. These characteristics include persistent structural imbalances, a slowdown in economic growth, low GDP growth and high population growth rates, underdeveloped sectors and means of production, depletion of natural resources, obstacles to economic development as the engine of the economy, and limited access to the majority of the population. Measurements of poverty aim to pinpoint the impoverished. The metric that is most frequently employed is the headcount poverty index, which is determined by the proportion of the population that resides in households with per capita consumption below the poverty line. (ii) the poverty gap index, which measures how far the average poor person's earnings deviate from the poverty threshold; (iii) the curved poverty gap, which displays the median of the squared proportion rate squared poverty gap, which measures the severity of poverty; and (iv) the poverty gap index. According to Bello (2009), people are considered to be in absolute poverty when their income is below that required for basic survival, as opposed to low income, which is determined by other members of their community's standard of living.

Cybercrime perpetrators are young people who lack of necessities of life as a result of poverty. Nigerian fraudster Ramon Abbas known as Hushpuppi born to a taxi driver and bread seller in Lagos, Nigeria, on June 14 1982, Abass grew upon the streets, working as a beggar and gambler for much of his life, before turning to cybercrime where he amassed great wealth.

Concept of Unemployment

The International Labour Organization in their contribution has it that the unemployed are numbers of the economically active population who are without work but available for and seeking work. They also include people who have lost their jobs and those who have voluntarily left work (World Bank, 1999).

On the part of Bassey & Atan (2012), Nigerian has the potential for rapid economic growth and development, with her rich human and material resources, yet the country's economic performance has been described as being truncated, erratic, dismal, and largely unimpressed (Ajayi, 2002; lyaha & Oriakhi, 2002; Kayode, 2004; Ekpo, 2008).

Agents of Social Influence in Cybercrime in Nigeria

Oludayo (2013) argued that the unrestrained pursuit of materialism in the Nigerian society is one of the factors driving young people to devise dubious ways of acquiring wealth rather than adhering to the rules set forth by society. For instance, it is expected that a young person will move through their educational system, do the required NYSC, and then find meaningful employment. Regrettably, Nigeria's pervasive corruption further motivates young people to forgo hard work and foster an aspiration to get affluent at any cost. Therefore, it is believed that the following social elements have an impact on the rate of cybercrime in Nigeria.

Peer Influence

Young internet users may be influenced by their peers. According to reports, hackers frequently build social networks with their online friends, and to get their approval or recognition, they may demonstrate their ability to steal accounts. It may be argued that teenagers feel comfortable in their social group. They frequently desire to go on "a flight of fancy" because they live in an adventurous world, and their peers give them the supportive atmosphere they need to do so. Hence, some young people may engage in cybercrime while disregarding the repercussions only to stand out from their law-breaking classmates (Philip, 2020).

According to John (2017), peer pressure not money lures young people into cybercrime. Young people's involvement in cybercrime is attributed in large part to peer pressure and the desire for recognition. Few, if any, of those who break the law online would have done so in a traditional setting. Young criminals frequently don't prioritize monetary gain as their main goal. Perhaps more significant factors in fostering cybercrime are the sense of accomplishment one feels after completing a task and the need to prove oneself to others to enhance online reputation. Cybercrime was committed by some young individuals because they thought it was "cool." Some offenders start by using gaming cheat websites and "modding" forums before moving on to criminal hacking groups. When young people leave their homes to pursue a university education, which frequently leaves them exposed to joining gangs, Suleiman (2016) argues that association with delinquent peers can make a child more susceptible to corruption in adulthood. The majority of people who engage in cyberfraud or other crimes are gang members.

Family

In today's world, it is impossible to avoid peer social connections. The same interaction, though, is a known trigger for aberrant conduct. Parenting in Nigeria has been less effective over time as a result of the pursuit of economic objectives. While sending their children to school, parents have little choice but to grant them temporary freedom, which greatly promotes the development of youngsters who are unconstrained and who explore their surroundings without thinking about the implications for their families (Oludayo, 2013). Wards have little choice but to be guided by internet fraud.

Custom or Religion

Although Nigerian law makes online fraud a crime. The majority of online fraudsters, sometimes referred to as Yahoo Boys or Yahoo Plus Boys, seek the assistance of herbalists, clergymen, and alfas to

create charms that increase success (fetish items) to increase their chances of obtaining more victims to scam. According to Oludayo (2013), Internet browsing is combined with charms like Afose (do as I say), Oruka-Ere (charmed rings), Ijapa (tortoise), Ose Awure (success-boosting soap), and Atona (pathfinder) to make victimizing victims simple. It should be emphasized that the herbalist, pastor, or alfa who is approached is typically accompanied by followers that they preach to or influence (Oludayo, 2013).

Concept of Corruption

Umaru (2020) Nigeria has maintained its abhorrent position in the global corruption rankings. In terms of global corruption, Nigeria was placed 144th out of 176 nations in 2018 and 149th out of 180 countries in 2020, according to a poll by Transparency International.

Due to Nigeria's high level of corruption, many young people find cybercrime appealing because there is little chance of being detained or facing legal action. Moreover, some dishonest law enforcement officials continue to harass young people using the law and collaborate with offenders to secure hurried plea deals so they can profit from their crimes. For instance, the EFCC's acting chairman, Ibrahim Magu, was removed from office after being accused of egregious wrongdoing (Premium Times, 2020).

National Security

The ability to defend oneself has been described in terms of national security. National security, according to Asad, reported in Awosusi & Ogbuleke (2019), cannot be understood solely in terms of the military. National security is intricately entwined with socioeconomic, cultural, and national integration components of development and modernization. According to Okoli & Opaleke (2018), national security includes safeguarding a political entity from all threats, including military, psychological, social, economic, and technological ones. According to Felix (2017), the components of national security are political fortitude, human capital, economic foundations, technological proficiency, industrial base, access to natural resources, and military might. According to Holmes (2015), national security refers to the protection of the state as a whole. The highest kind of national security involves defending the state against external threats and preserving state secrets, and it involves using armed forces to do so. Both national defense and the safeguarding of a number of interests, such as economic and geopolitical interests, are included in the concept of national security. As a result, the working definition for this study is that national security refers to a state's provision of fundamental elements that ensure both economic prosperity and the safety of its citizens against both internal and external dangers. Threats here is in form of some attack that broad-ranging and could refer to economic attack, political attack, religious attack, or technological attack i.e., cybercrime. By extension, a direct attack on individuals and organizations (public or private) to deprive them of the capacity to enjoy economic well-being that may have otherwise been provided by the state, is an attempt to undermine national security.

Economic Development Policies and Programmes

The government has over the years created jobs, retention programs, loans, subsidies, and other initiatives to raise the standard of living in Nigeria and boost the country's economic growth. Nigerian government institutions, the World Bank, non-governmental organizations (NGOs), and even private sector donors have recently targeted young people in Nigeria (Ambrose, 2020).

The government initiated and supported Entrepreneurship Development Centres (EDCs), launched the Microfinance Policy, Regulatory and Supervisory Framework for Nigeria, and introduced the NYSC sensitization, Venture Prize Competition, and NYSC Entrepreneurship Training Programmes, among other initiatives to help empower youths and diversify the economy. It has also participated in programs such as the Youth Enterprise with Innovation in Nigeria (YouWIN!), the Youth Initiative for Sustainable Agriculture in Nigeria (YISA), the Subsidy Reinvestment and Empowerment Program (SURE-P), the Graduate Internship Scheme (GIS), Africa Youth Empowerment Nigeria (AYEN), the Youth Entrepreneur Support Program (YES-P), and the N-Power Empowerment Program.

Organizations and donors from the corporate sector have also contributed a little amount of money. Youth Empowerment and Development Initiative (YEDI), Diamond-Crest for Youth Education Foundation, Tony Elumelu Foundation for Entrepreneurship in Africa, New Era Foundation, Youth for Technology Foundation, and LEAP Africa are among them. All of this was done to increase job creation, reduce poverty, and generate revenue for both individuals and the government. Irrespective of all the above-mentioned policies and programs aimed at increasing youth employment, hence leading to economic diversification, economic growth, and development, Nigeria still faces a lot of challenges toward creating sufficient job opportunities for her unemployed youths.

Theoretical Framework

The research was guided by the following theoretical framework:

Theory of Structural Functionalist

In order to adequately provide a vivid explanation, prediction, prescription and analysis of the issue of Security challenges that pervaded Nigeria's federal arrangements right from the local levels to the federal level, Structural-functionalist Theory (SFT) was adopted by this paper. This is believed by the view that this theory will help to gain depth understanding of cybercrime in Nigeria. The adoption of this theory is justified in the ability of theory in providing a proper analysis of why cybercrime activities are yet to be curbed.

Structural functionalism as wholly explained refers to the large-scale social structures and institutions of society, their inter-relationships, and their constraining influence on actors (Ritzer, 2008). Historically, some founding fathers of sociology like Herbert Spencer, Auguste Comte and Emile Durkheim, laid the classical foundation of structural-functionalism. Talcott Parsons later redefined it to reflect his work titled “the social system” in 1951 (Scott & Marshall, 2005). From a theoretical perspective in sociology, functionalism holds a view of society as a social system that is made up of different parts, which are interdependent and interrelated (Igbo, 2013). These important parts of society, which include the family, school, government, law enforcement agencies; economy, etc. perform various functions positively toward the maintenance, stability and survival of the social system (Ravishankanr, 2019).

From the organism analogy, the functionalists equate the human society with the human or biological organism that has a structure comprising organs, systems and capillaries, which must function for the maintenance and survival of the whole organism. To understand the structure of the organism (man), the respective parts and their interconnected functions must be examined. The foregoing forms the basis of Parsons' concept of Adaptation, Goal maintenance, Integration and Latency function (AGIL). Thus, AGIL is an elaborate model of systems and sub-systems. It implies that for any society to survive, each system must meet the aforementioned four functional prerequisites namely: Adaptation (adjustment to the physical environment); Goal attainment (a means of organizing resources to achieve societal goals and obtain gratification), Integration (forms of internal coordination and ways of dealing with differences), and Latency or pattern maintenance (means of achieving comparative stability). A problem in one component might hinder the growth and existence of the other components. Although the parts make up the whole, the existence of the whole depends on the presence of the parts. Social influence, poverty, unemployment, and crime all function as necessary but inevitable components of the system, which together increase/decrease society's overall efficacy and efficiency.

Relevance of the Theory of Structural Functionalist to the Study

The theory emphasizes social order based on tacit agreements between people and state or society, views shared norms and values as the cornerstone of society and views social development as slow and orderly. The other component of the system will be impacted if one component of it is inefficient. For instance, a state's economic growth will be impacted by the political system's inefficiencies. The theory demonstrates why the ineffectiveness of the legal system and law

enforcement, as well as unemployment, family, custom, religion and poverty, are the main factors promoting cybercrime activity in Nigeria. The point of emphasis here is how social equilibrium can be achieved and maintained between and among the various elements or institutions of a social system and sub-systems in such a way that all the assigned institutions in Nigeria should rise to the task of meeting their daily functions and responsibilities in order to reduce the level of social vices (Ritzer, 2008).

Theory of Technology-Enabled Crime

The theory's core finding is that it incorporates several kinds of concepts to assist society to comprehend why crimes co-evolved with computer and telecommunications technology to become among the most complicated and challenging types of crime to prevent, investigate, and regulate. According to McQuade (1998), understanding and managing relatively complicated criminality might be challenging at first, and there is an ongoing struggle between law enforcement and the criminal element for technological superiority. Law enforcement must keep up with criminal activity to avert, regulate, dissuade, and prevent emerging types of crime. According to McQuade (2006), the technology-enabled crime theory includes:

a. crimes conducted specifically against computers and computer systems.
b. This category of criminal activity is frequently referred to as high-tech crime, computer crime, or cybercrime.
c. Using gadgets for traditional crimes or to help others do so.
d. The use of technology can make it easier to commit crimes including fraud, scams, and harassment, which presents fresh problems for long-standing offences.

The theory offers a framework for comprehending all types of criminality, particularly those that are developing as a result of advancements in computing and telecommunications technologies. The theory is relevant for comprehending current challenges provided by transnational criminal organizations, terrorist networks, and new forms of cybercrime that challenge established criminal justice systems and security precautions for preventing and managing crime. The theory is important to this study because it sheds light on the new tools and methods used by cybercriminals - a transition from basic crimes performed with simple tools to complex crimes committed with sophisticated instruments. Also, it aids in comprehending novel instances of social abuse, criminal activity, and other forms of deviance brought on by cutting-edge technological use.

Relevance of Technology-Enabled Crime to the Study

The theory offered a framework for comprehending all types of criminal behaviour, particularly those that are developing in response to advancements in computing and telecommunications technology. The theory is relevant for comprehending current challenges posed by international criminal networks, developing forms of cybercrime, and terrorism networks that challenge conventional techniques of criminal justice and security measures for preventing and managing crime.

The theory is important to our study because it sheds light on how cybercriminals are adopting new tools and tactics, which represents a change from basic crimes to complicated crimes using complex tools. Also, it aids in comprehending novel instances of social abuse, criminal activity, and other forms of deviance brought on by cutting-edge technological use.

Conclusion and Recommendations

Youth unemployment has continued despite efforts by Nigeria's successive administrations to address it through the implementation of targeted programs and policies that are meant to increase employment and combat poverty. The main causes of cybercrime among young people include poverty, unemployment, unfairness, and the inability of socialization agents to educate the public about the negative impacts of cybercrime, which are harmful to both individual and societal development. One of the main ways that cybercrime threatens society is by undermining the importance that society places on working hard to get money. According to the structural function theory, the effectiveness of one

component of the political system will have an impact on how well the other components of the system work.

Hence, new behaviours frequently lead to the destruction of moral principles and acceptable social norms. This is hardly surprising given that riches and success are socially desired in Nigeria; nevertheless, many youths are prevented from achieving success through legal channels, which encourages them to turn to cybercrime. Cybercrime also has an impact on people's financial situations, which inevitably has an impact on their physical and mental health. To effectively engage the energies of the young people in growing the economy and curb the involvement of youths in cybercrime.

The majority of the scholars also concurred that youth unemployment in Nigeria has a significant influence in encouraging cybercrime. The writings of Umaru (2020), who maintained that a high unemployment rate has socioeconomic, political, and psychological repercussions, support this. This dynamic promotes the growth of urban urchins and street kids (also known as "area boys") who are raised in a society that values criminal activity. Young people without jobs have free time and easy access to the internet, which they use to commit cybercrimes.

It was shown that teenagers' involvement in cybercrime was a direct outcome of their poverty. For instance, inequitable access to necessities of life is a major factor ill Nigerian cybercrime operations. According to Olubukola (2017), while poverty can be defined in terms of income, many people view it to be multidimensional and based on markers like (I) low income, (ii) poor levels of education and health, (iii) vulnerability to health or income loss, natural disaster, crime and violence, and education curtailment and (iv) stridency and powerlessness (such as feeling discriminated against or having few opportunities for revenue generation).

The following are recommended as strategies to address the undesirable crisis that has been engendered by the malaise. Adolescents should be empowered through numerous programs aimed at eradicating poverty. As the government works to create various programs to eradicate poverty, meritocracy must be a process of empowerment rather than favouritism if it is to work. The Nigerian National Youth Policy should also be completely executed to guarantee the youth a bright future. To give young people access to social and educational resources as well as basic education, healthcare, and jobs, long-term planning should be implemented. The government should work with UBE and NUC to inform students and young people about the benefits and drawbacks of using the Internet. by revising the curriculum and adapting it to match the problems with cybercrime. To raise knowledge of the many types of cybercrime, deliberate efforts must be made.

References

Adagba, O. S. (2012). Evaluation of The Performance of the Code of Conduct Bureau (CCB) and Code of Conduct Tribunal (CCT) In Combating Corruption in the Nigerian Public Service. Retrieved from Ahmadu Bello University Database.

Adekemi, O. (2016). Comparative Perspectives on Cybercrime Legislation in Nigeria and the UK - A Case for Revisiting the "Hacking" Offences Under the Nigerian Cybercrime Act 2015. *European Journal of Law and Technology.* vol 7, No 3.

Adewale, N., (2020). Panic as Fraudsters Hack FCMB Database, Steal Customers' N900 Million. Retrieved from https://businesslive.ng/

Ambrose, O., Augustine, J. M., & Michael, O., (2020,). Youth Empowerment and Entrepreneurship in Nigeria: Implication for Economic Diversification. DOI: 10.1177/2158244020982996

Awosusi, O. E. & Ogbuleke L. E. (2019). "Critical Thinking in Information Technology and Management for National Security in Nigeria." *Asian Journal OfApplied Science and Technology* 41–52.

Ayofe, A. N. & Oluwaseyifunmitan, O., (2009). Approach to Solving Cybercrime and Cybersecurity. *International Journal of Computer Science and Information Security*. Vol. 3, No. 1.

Bello, A. T., (2017). Anatomy of Cybercrime in Nigeria; The Legal Chronicle. Retrieved from Https://papers.ssrn.com/sol3/papers.ccm?abstract_id=3055743

Bello, R. A., Toyebi, G. O. A, Balogun, I. O., Akanbi, S. B. (2009). Poverty Alleviation Programmes and Economic Development in Nigeria: A Comparative Assessment of Asaand Ilorin West Local Govt. Areas of Kwara State, Nigeria. *International Multi-Disciplinary Journal*, Ethiopia Vol. 3 (4), July 2009 ISSN 1994-9057.

Bolaji, O., Olatayo, O., Odiase P. O., & Adebimpe E., (2016): Cybercrimes in Nigeria: Analysis, Detection, And Prevention. *FUOYE Journal of Engineering and Technology*, Volume 1, Issue 1.

CALED (2020). What Is Economic Development? Retrieved from Https://Caled.Org

Chiara M., Evelyn M., & Celestine O. O., (2017). Inequality in Nigeria; Exploring The Drivers. Retrieved from https://www.oxfam.org

Cohen L. E. & Felson M., (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, Vol.44 (2):588-605.

Council of Europe (N.D). Cybercrime Policies/Strategies. Retrieved from https://www.coe.int/

Creswell, J. W., (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. Sage Publications, Inc.

Edward, O. U. & Charles, O. O., (2017). Social Structure and the Production of Young Cyber Criminals in Nigeria. *International Journal of Social Sciences, Humanities, and Education*, Vol 1 (2), ISSN 2521-0041.

Erhabor, I. M., (2008). Cybercrime and the Youths (PGDE Thesis), Department of Education, Ambrose Alli University, Ekpoma, Nigeria, p.37. Retrieved from academicjournals.org.

European Commission (N.D.). Cybercrime. Retrieved From https://Ec.Europa.Eu.

Ewepu, G., (2016). Nigeria Loses N127bn Annually To Cybercrime -NSA. Retrieved from http://www.wanguardngr.com

Felix, E. E., (2017). Curtailing Cybercrime InNigeria: Applicable Laws And Derivable Sources. Retrieved From https://www.researchgate.net/publication/336243066.

Felix, E., (N. D). Cybercrime Prosecutors and Non-Retroactivity of the Nigerian Cybercrimes Act 2015: Implication for the Administration of Cybercrime Justice. *Revista Acadêmica Escola Superior Do MinistérioPúblicoDo Ceará*.

Frank, I., (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. (IJCRSEE) *International Journal of Cognitive Research in Science, Engineering, and Education* Vol. 1, No.1, 2013. Retrieved From https://www.researchgate.net/.

Giddens, A., (2001). *Sociology.* Uk: Blackwell Publishers Pp.306-501.

Grabosky, P. N., (2001). Virtual Criminality: Old Wine in New Bottles. *Social and Legal Studies* 10 (2):243-249.

Hamid J., Al-Nemrat A., & Amin H. (2014). Cybercrime Classification and Characteristics. doi:10.1016/B978-0-12-800743-3.00012-8

Hassan, A. B., Lass F. D., & Makinde, J. (2012).Cybercrime in Nigeria: Causes, Effects and The Way Out, *ARPN Journal of Science and Technology*, Vol. 2(7), 626-631.

Holmes, K R, "What is National Security?" (2015) 10

Ibikunle, F., & Eweniyi O., (2013). Approach to Cybersecurity Issues in Nigeria: Challenges and Solutions. Department of Electrical &Information Engineering, Covenant University, Nigeria. (IJCRSEE) *International Journal of Cognitive Research in Science, Engineering, and Education.* Vol. 1, No.1.

Ibrahim, S. (2016). Causes of Socioeconomic Cybercrime in Nigeria (Parents' Perspectives). The Centre for Doctoral Training in Cyber Security, The Information Security Group Royal Holloway University of London TW20 0EX Surrey, UK. *SSRN Electronic Journal*. doi:10.2139/ssrn.3240469

Ijaiya, G. T., Bello, R. A., Arosanyin, G. T., Oyeyemi, G. M., Raheem, U. A., & Yakubu, A. T., (2015). Poverty in the Urban Informal Sector of Kwara State, Nigeria. *Ilorin Journal of Economic Policy.* Vol. 2: 16-29, 2015.

James, O., Enyinnaya, D. C., & Fidelis, O., (2016). The Nigerian Cybercrime Act 2015 and Its Implications for Financial Institutions and Service Providers. Retrieved from https://www.financierworldwide.com

John, L., (2017). Peer Pressure, Not Money, Lures Youngsters into Cybercrime – Report. Retrieved from https://www.theregister.com

Kaspersky, (N. D). Tips On How to Protect Yourself Against Cybercrime. Retrieved from https://www.kaspersky.com/

Kemi, B., (2017). Nigeria's Cybercrime Act Needs Review – Senate Committee. Retrieved from https://www.premiumtimesng.com

Kunle, S., (2020). Ibrahim Magu was Suspended as EFCC Chairman. Retrieved from https://www.premiumtimesng.com

Lakshmi, P., & Ishwarya, M., (2015). Cybercrime: Prevention & Detection. *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. Vol. 4(3).

Lastowka, F. G., & Hunter, D., (2004). *Virtual Crimes*. New York Law School Law Rev. 49:293-316. Retrieved from https://academicjournals.org/

Laura, A., (N. D). Cybercrime and National Security: The Role of the Penal and Procedural Law. Law and Security in Nigeria Vol.(7) pp:197-232. Retrieved from https://nials-nigeria.org.

Lawpadi, (2015). 10 Things to Know about Nigeria's Cybercrime Act 2015. Retrieved from https://lawpadi.com/.

Longe, O. B., & Chiemeke, S. C. (2008). Cybercrime and Criminality in Nigeria – What Roles are Internet Access Points Playing? *JITI Journal of Information Technology Impact*, Vol. 9, No. 3, pp. 155-172. Retrieved from https://www.researchgate.net/

Maitanmi, O., Ogunlere S., Ayinde S., & Ayinde S., (2013). Impact of Cybercrimes on Nigerian Economy. *The International Journal of Engineering and Science*(IJES)Vol (2) Issue (4) pp:45-51. Retrieved from https://www.theijes.com/.

Mamoun, A., & Roderic, G., (2017). An Analysis of the Nature of Spam as Cybercrime. Doi: 10.1007/978-3-319-32824-9_13.

Marcus, A., (2018). Cyber-Terrorism under Nigerian Law: A New Form of Threat or an Old Threat in a New Skin. Retrieved from https://ssrn.com/abstract=3286617.

Mcquade, S. (2006). *Understanding and Managing Cybercrime,* Boston: Allyn &Bacon.

Mcquade, S., (1998). Towards a Theory of Technology-Enabled Crime. Unpublished Manuscript. George Mason University, Fairfax, Virginia.

Michael, A., Boniface., A. & Olumide, A. (2014). Mitigating Cybercrime and Online Social Networks Threats in Nigeria, Proceedings of the World Congress on Engineering and Computer Science.*Adu Michael Kz*, Vol. Vol. I WCECS 2014, 22–24.

Morse, J. M., (1994). Designing Funded Qualitative Research: In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 220–235). Sage Publications, Inc.

Mshana, J. A., (N.D). A Cybercrime-An Empirical Study of Its Impact in Society- A Case Study of Tanzania. Institute of Judicial Administration Lushoto, Box 20 Lushoto. Retrieved from https://www.ajol.info/.

Msigwa, R. & Kipesha, E. F. (2013). Determinants of Youth Unemployment in Developing Countries. Evidence from Tanzania. *Journal of Economics and Sustainable Development*, Vol. 4, No.14.

National Bureau of Statistics, Statista (2019). 2019 Poverty and Inequality In Nigeria: Executive Summary. Retrieved from https://www.statista.com/

National Bureau of Statistics, Statista (2021). The Unemployment Rate in Nigeria in the Selected Quarter between the 1st Quarter of 2015 and the 4th Quarter of 2020. Retrieved from https://www.statista.com/

NBS (2019). 2019 Poverty and Inequality in Nigeria: Executive Summary, By NBS 2019 (Abuja: Proshare, 2019).

Nigeria Communications Week (2020). How N900m Disappeared from MTN, Multichoice Bank Accounts- FCMB Staff. Retrieved from https://www.nigeriacommunicationsweek.com.ng/

Nigerian Communication Commission (2016). Final Report on Effects of Cyber Crime on Foreign Direct Investment and National Development. Retrieved from https://www.ncc.gov.gg/.

Nigerian Communication Commission (2019). Understanding the Concept of Cyber Security. Policy Competition & Economic Analysis Department. Retrieved from https://www.ncc.gov.gg/

Nimi, P., (2021). Nigerian Entrepreneur Obinwanne Okeke Jailed for 10 Years in $11m Email Scam. Retrieved from https://edition.cnn.com.

Nneoma, B., (2019). Buhari Warns Nigerians Against Cybercrime, 'We Will Take Firm and Decisive Action'. Retrieved from https://www.icirnigeria.org

Odumesi, J. O (2006). Combating the Menace of Cybercrime: The Nigerian Approach. [Project] Department of Sociology, University of Abuja, Nigeria p. 45.

Odumesi, J. O., (2014). A Socio-Technological Analysis of Cybercrime and Cybersecurity in Nigeria. *International Journal of Sociology and Anthropology*. doi: 10.5897/IJSA2013.0510

Okeshola, F. B. & Adeta, A. K, (2013).The Nature, Causes and Consequences of Cybercrime in Tertiary Institutions in Zaria-Kaduna State, Nigeria, *American International Journal of Contemporary Research*, Vol. 3(9), 98-114.

Okoli, A. C. & Idom, A. M., (2018). "The Internet and National Security in Nigeria: A Threat-Import Discourse" 6:1 Covenant University. *Journal of Politics &International Affairs* 20–29.

Okoli, A. C. & Okpaleke, F., (2014). "Cattle Rustling and Dialectics of Security in Northern Nigeria" 2:3. *International Journal of Liberal Arts and Social Science* 109–117.

Olubukola, S. A., (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science* Vol. 13, No. 4, 2017, pp. 19-29 doi:10.3968/939.

Oludayo, T., (2013). A Spiritual Dimension to Cybercrime in Nigeria: The 'Yahoo Plus' Phenomenon. *Human Affairs* 23, 689–705, 2013 doi: 10.2478/S13374-013-0158-9

Osahenvemwen, A., & Ogbeide, K. O., (2014). The Role of the Internet and Effects on Nigerians. *International Journal of Engineering Innovation &Research*. Volume 3, Issue 4, ISSN: 2277 – 5668

Osayemwenre, B. O., (2018). An Appraisal of the Activities of Economic and Financial Crime Commission (EFCC) on the Administration of Criminal Justice in Nigeria. Acta Universitatis Danubius. *Relations Internationales*, Vol.11, No 2 (2018).

Pereware A. T., (2016). Efforts in Combating Cyber Crime and Criminality in Nigeria. Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol. 6, No.3, 2016.

Philip N., (2020). *Nature, Causes and Consequences of Cybercrime in Nigeria. Sociological Insights on the Contemporary Social Problems in Nigeria*. (pp.60-80) Publisher: Federal University of Kashare Printing Press, Gombe, Gombe State, Nigeria.

Phishing.Org (N. D.) What is Phishing? Retrieved from https://www.phishing.org/.

Proshare (2020). Cybercrime in Nigeria: Causes and Effects. Retrieved from https://www.proshareng.com/.

Ruth, O., (2021). Nigeria Unemployment Rate Rises to 33%, Second Highest on Global List. Retrieved from https://www.bloomberg.com/.

Study.Com (N.D).Agents of Socialization: Family, Schools, Peers and Media. Retrieved from https://study.com

Techopedia (2020). Cyberspace. Retrieved from https://www.techopedia.com.

Thomas, D., & Loader, B., (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. *RoutledgeLondonJ. Soc. Policy*30(1):300.

Uche, M., & Eman D., (2015). The Cyberspace: Redefining A New World. Centre ForCyberspace Studies, Nasarawa State University, Keffi, Nasarawa State, Nigeria. Doi:10.9790/0661-17361724

Ufuoma, V. A., & Ohwomeregwa, O. B., (2020). Appraising the Laws Governing the Control of Cybercrime in Nigeria. *Journal of Law and Criminal Justice*. Vol. 8, No. 1, pp. 30-49

Umaru, I. (2020). The Impact of Cybercrime on the Nigerian Economy and Banking System. Nigeria Deposit Insurance Corporation. Retrieved from https://ndic.gov.ng/

United Nations (N. D). Ending Poverty. Retrieved from https://www.un.org/

Wada, F., & Odulaja, G. O., (2014), Electronic Banking and Cybercrime in Nigeria - A Theoretical Policy Perspective on Causation. *Afr J Comp &ICT*, Vol.4(3), No. Issue 2.

Yakubu, M. A., (2017). Cyber Security Issues in Nigeria and Challenges. doi:10.23956 /Ijarcsse/V6I12/01204

Yar, M., (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *Eur. J. Criminol*. 2(4):407-427.