Journal of Contemporary Sociological Issues, Volume 1, Issue 2 (2021), pp. 86-109
doi: 10.19184/csi.v1i2.24188
ISSN 2723-3456 E-ISSN 2775-2895

Poverty, Cybercrime and National Security in Nigeria

Akinyetun Tope Shola
akinyetuntope@gmail.com

Abstract

The number of people living in poverty in Nigeria continues to grow at an exponential rate, making Nigeria the poverty capital of the world. As a result, cybercrime has become a haven for youths. The festering of cybercrime increases the chances of cyberterrorism and proliferates radicalization and hate speech – all of which pose a danger to national security in Nigeria. This study adopts an analytic approach to explore the interplay between poverty, cybercrime, and national security in Nigeria. The findings reveal that poverty is a major driver of cybercrime in Nigeria, and cybercrime poses a serious threat to national security. It shows that, with the prevalence of poverty, deprivation, and inequality, many Nigerian youth turn to crime for creating Nigeria as their desired. Cybercrime undermines national security by exposing individuals to violence, cyberespionage, cyberstalking, and manipulation. The study, recommends that decisive policies targeted at reducing poverty should be developed in Nigeria and that youths should be educated on the dangers of cybercrime and its incapacitating effect on national security. Moreover, cybersecurity should be prioritized by the Cyber Advisory Council. Meanwhile, cybercriminals must be dealt with under the full force of the law, establishing justice and serving as a deterrent to perpetrators who intend to commit crimes.

Keywords: Cybercrime, National security, Poverty, Scam, Unemployment

HOW TO CITE:
Shola, Akinyetun Tope. "*Poverty, Cybercrime and National Security in Nigeria*" (2021) 1:2 ***Contemporary Sociological Issues*** 86-109.

Submitted :May 4, 2021
Revised :June 14, 2021
Accepted :July 25, 2021
Publish : August 31, 2021

I. INTRODUCTION

The rise in the use of technology has disrupted channels of communication between countries. Citizens can now interact freely, conduct businesses, and engage in transborder trade. As of 2020, 58 percent (i.e. 4.5 billion people) of the world's total population (7.8 billion people) are connected to the internet, while social media users represent 49 percent (i.e. 3.8 billion people) of the world's total population.[1] Indeed, the world has become a global community with increased interconnectedness, permeating every sphere of human endeavors.[2] On the one hand, the rise in technology use has the potential to improve communication, facilitate technological advancements, engender paradigm shifts in information production, distribution, and control. On the other hand, it has also produced a phenomenal increase in the incidence of criminal activities, endorsed illegal business, and entrenched cyberterrorism and cybercrime.[3] Reportedly, the United States, Russia, and Hong Kong have the highest rates of cybercrime in the world. Cybercrime in Hong Kong rose by 70 percent in 2013, with financial losses totaling US$118 million, nearly four times as much as 2012. Meanwhile, in the United Kingdom, an estimated £27 billion (US$43 billion) is lost to cybercrime annually.[4]

Nigeria is reportedly one of the countries of the world from where cybercrime originates.[5] Although, the most common type of cybercrime in Nigeria is "advanced fee fraud 419" (also known as yahoo-yahoo), there are several other types such as hacking, phishing, spamming, identity theft, piracy, credit card fraud (ATM), and scamming.[6]A prominent factor that has contributed to the proliferation of cybercrime in Nigeria is pervasive unemployment and poverty. Despite being branded the giant of Africa, Nigeria has a developing economy that ranks low in all socioeconomic indicators including health, income, life expectancy, education, employment, and criminal investigations[7]The unemployment rate in Nigeria is 23.1%, of which youth unemployment constitutes 55.4%. At the national level, 40.1 percent (i.e. 82.9 million) of Nigerians are considered living in poverty. Moreover, 4 out of every 10 persons in Nigeria have expenditures per capita below N137, 430 (i.e. $355) per year.[8]

If left unchecked, cybercrime can place an indelible dent in a country's national image. The prevalence of cybercrime in Nigeria has not only undermined the country's efforts to maintain national security, but has also contributed to negative perceptions

[1] *Digital 2020: Global digital overview*, by Simon Kemp (2020).

[2] Alao David, Osah Goodnews & Eteete Michael, "Unabated cyber terrorism and human security in Nigeria." (2019) 15:11 Asian Social Science 105–115.

[3] John Olayemi Odumesi, "A socio-technological analysis of cybercrime and cybersecurity in Nigeria" (2014) 6:3 International Journal of Sociology and Anthropology 116–125.

[4] Red24, "Cybercrime top 10 affected countries", (2015a), online: <https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+affected+countries+-2015.pdf>.

[5] Red24, "Cybercrime Top 10 countries where attacks originate", (2015b), online: <https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf>.

[6] Sam Ogunlere et al, "Impact of cybercrime on the Nigerian economy" (2013) 2:4 The International Journal of Engineering and Sciences 45–51.

[7] Olukayode Olabanji & Ese Urhie, "Insecurity and socio-economic development in Nigeria" (2014) 5:1 Journal of Sustainable Development Studies 14–20.

[8] *2019 poverty and inequality in Nigeria: Executive summary*, by NBS 2019 (Abuja: Proshare, 2019).

and erroneous beliefs that Nigeria is a fraudulent country. As such, Nigeria is treated with suspicion in virtually all endeavors of life, including education, business, relationship, and traveling by nations across the globe as well as their citizens.[9]Indeed, "legitimate interactions of all forms originating in, or concerned with Nigeria and across cyberspace are now characterized with increasing disbelief".[10]

Limited studies have attempted to establish the nexus between poverty and cybercrime in Nigeria,[11]while few others have also tried to point out the effect of cybercrime on national security in Nigeria.[12]These studies have failed to establish a link between poverty, cybercrime, and national security in Nigeria. As such, the present study adopts a qualitative approach to explore the causal relationship between poverty and cybercrime in Nigeria and its implications for national security.

II. THEORETICAL UNDERPINNING

The concept of poverty is best understood in relation to the environment, society, individual, or group people belong to. Poverty results in deprivation).[13] Further, Townsend (1979) claims that:

> "The term of the concept of relative deprivation is understood objectively rather than subjectively. Individuals, families, and groups in the population can be said to be in poverty when they lack the resources to obtain the types of diet, participate in the activities, and have the living conditions and amenities that are customary, or at least widely encouraged or approved, in the society to which they belong"[14]

Contrary to Townsend's proposition of the objectivity of deprivation, Rummel[15] claims that poverty is subjective because the definition of what passes as deprivation or lack is not absolute, but shifts according to society, period, and person. Rummel[16] argues that individuals use their present and expected positions as a basis of comparison against needs or supposed achievement. It is the difference between the perceived and the expected that counts as deprivation; relative deprivation when assessed in comparison with others. The central argument here is that poverty is perceived differently, engenders deprivation, and exists in relative terms – hence the term 'relative deprivation'. For example, although needs such as food, healthcare, clothing, education,

[9] Al Chukwuma Okoli & Okpaleke Francis, "Cattle rustling and dialectics of security in northern Nigeria" (2014) 2:3 International Journal of Liberal Arts and Social Science 109–117.

[10] Oluwafemi Osho & Agada D Onoja, "National Cyber Security Policy And Strategy Of Nigeria: A Qualitative Analysis" (2015).

[11] Adesina, 2017; Badmus, 2018; Epron, 2019

[12] Alao et al., 2019, Odumesi, 2014; Okoli & Idom, 2018

[13] Peter Townsend, *Poverty in the United Kingdom: A survey of household resources and standards of living* (Harmodsworth: Penguin Books Ltd, 1979).

[14] *Ibid.*

[15] Rudolph Rummel, *"Frustration, deprivation, aggression, and conflict helix." In: Understanding conflict and war* (Beverly Hills, California: Sage Publications, 1977).

[16] *Ibid.*

and shelter are universal, how they are met varies across societies. Therefore, the deprivation of any (or a combination) of these needs is understood relatively.

Literature on relative deprivation is well presented by Ted Gurr's "Why Men Rebel" (1970).[17] The notion of relative deprivation has been used to measure inequality, fairness, social justice, grievance, social hostility, or aggression. According to Gurr, relative deprivation "is defined as actors' perception of discrepancy between their value expectations and their value capabilities." It is the gap between that "to which people believe they are rightfully entitled" and that which "they think they are capable of getting and keeping".[18] Value *expectations* are the goods, services, and general resources to which people believe they are rightfully entitled; value *capabilities* are the goods and conditions people think they are capable of attaining, if afforded the right opportunity. Therefore, relative deprivation is not just based on a person's (or group of people's) needs, but on the conditions a person thinks they deserve or ought to have.[19]

For Uzoh[20], relative deprivation presumes that people who share the sentiment of being deprived often end up taking collective action. That is, individuals (or groups) who are deprived of essential services, critical infrastructure, and life-easing goods needed for survival, are more inclined to organize collectively to defend or improve their conditions. Gurr hypothesizes that the potential for collective response varies depending on the amount and range of deprivation among group members. Given this, the study turns to Relative Deprivation (RD) theory, arguing that the perceived discrepancy between what people think they deserve, and what they believe they can get; or the disparity between their aspirations and achievements, leads to a collection of action to change the narrative.

According to Akinyetun[21], socioeconomic deprivation leads to multidimensional poverty, inequity, injustice, and unemployment. This exacerbates existing tensions among marginalized groups, who can be triggered to seek alternative although by illegal ways.. This perceived economic, political, and social deprivation is a precursor to violence, terrorism, extremism, insurgency, and crime. Crime has become a haven in the context of general neglect, the misappropriation of the commonwealth by the political class, and the starvation and suffering of the people. This study argues that this has become a basis for [self] recruitment to cybercrime. These recruits are mainly illiterate, school drop-outs, jobless, ignorant, and disadvantaged youth. In short, the relative deprivation and marginalization perceived in the country have made cybercrime attractive to, and common among Nigerian youth.

[17] Ted Robert Gurr, *Why Men Rebel* (Princeton: Center of International Studies, Princeto University, 1970).
[18] *Ibid*.
[19] Rudolph Rummel, *supra* note 15.
[20] Bonaventure Chigozie Uzoh, "Poverty–conflict nexus: The Nigerian experience" (2016) 3:10 The International Journal of Social Sciences and Humanities Invention 2832–2838.
[21] Tope Shola Akinyetun, "A theoretical assessment of Boko Haram insurgency in Nigeria from relative deprivation and frustration-aggression perspectives" (2020) 1:2 African Journal of Terrorism and Insurgency Research 89–109.

For Nnam, Agboti & Otu[22], "the meteoric rise in unemployment, poverty, social exclusion and weak or dysfunctional social structures (both formal and informal) have exacerbated the crime problem in Nigeria." Agboti & Nnam[23]claim that many Nigerians are excluded and deprived of essential services; they are habitually neglected. "When people are relatively deprived of essential goods and services (social exclusion), frustration and depression will invariably ensue and consequently lead to the acting out of their discontentment and aggression through all means, including crime." This view is rooted in Gurr's presumption that deprivation leads to frustration, and "if frustrations are sufficiently prolonged or sharply felt, aggression is quite likely, if not certain, to occur"[24]

Poverty leads to deprivation which, in turn, drives Nigerian youth to pursue alternative means to improve their living condition, namely through cybercrime. This was aptly captured by Rummel:[25]

> "[a] relatively deprived person may believe that the gap between rightful wants and capabilities is due to his laziness. He then may determine to live a better, more socially useful life, or to try to improve his capabilities… A frustrated person may regress; he may withdraw from human interaction associated with the frustration, absorb it into a higher goal, or try to cope with it." (1977:4)

From Rummel's submission, a deprived and frustrated person may decide to improve his capabilities or try to cope with the deprivation How this person intends to improve or cope with this situation is not clarified, though the study argues that they may turn to cybercrime. This view is also shared by Agboti & Nnam who claim that "people who are socially excluded may take to crime and delinquency as an expression of displeasure and dissatisfaction with a hostile political regime".[26] Although this theory has been criticized for being applied to violent civil conflict, and a potential trigger for aggression and collective violence, the theory is relevant in attributing the exponential rise in youth involvement in cybercrime to the high level of poverty, inequality, and deprivation in Nigeria (see tables 1 and 2).

Table 1. Multidimensional Poverty Index: developing countries

	Multidimensional Poverty Index	Population in dimensional poverty	Population

[22] Uchenna Nnam, Agboti Iheanacho, & M Otu, "Inadequate motivation as a reason for police officers' ineffectiveness in policing contemporary Nigeria" (2013) 15:2 South-South Journal of Culture and Development 67–86.

[23] Agboti Iheanacho & Nnam Uchenna, "An assessment of the relationship between crime and social exclusion in Nigeria" (2015) 8:1 International Journal of Research in Arts and Social Sciences 157–164.

[24] Ted Robert Gurr, *supra* note 17.

[25] Rudolph Rummel, *supra* note 15.

[26] Iheanacho & Nnam Uchenna, *supra* note 23.

	Index	Inequality among the poor	Population in severe multidimensional poverty	vulnerable to multidimensional poverty
Country	**Value**	**Value**	**(%)**	**(%)**
China	0.016	0.005	0.3	17.1
South Africa	0.025	0.005	0.9	12.2
Ghana	0.138	0.016	10.4	22.0
Kenya	0.178	0.014	13.3	34.9
Tanzania	0.273	0.016	25.9	24.2
Nigeria	0.291	0.029	32.3	16.8
Uganda	0.269	0.017	24.1	24.9

Source: Extracted from United Nations Development Programme Multidimensional Poverty Index Report 2019

Table 2. Multidimensional Poverty Index: developing countries contd.

	Contribution of deprivation in dimension to overall multidimensional poverty			**Population living below the income poverty line (%)**	
	Health	**Education**	**Standard of living**	**National poverty line**	**PPP $1.90 a day**
Country	**2007-2018**			**2007-2017**	
China	35.2	39.2	25.5	3.1	0.7
South Africa	39.5	13.1	47.4	55.5	18.9
Ghana	22.3	30.4	47.2	23.4	13.3
Kenya	24.9	14.6	60.5	36.1	36.8
Tanzania	21.1	22.9	56.0	28.2	49.1
Nigeria	27.0	32.2	40.8	46.0	53.5
Uganda	22.4	22.5	55.1	21.4	41.7

Source: Extracted from the United Nations Development Programme (2020) Multidimensional Poverty Index Report 2019

III. CONCEPTUAL FRAMEWORK

A. Poverty

Poverty is a complex concept with a multitude of meanings, while its definitions are variable, it can be understood as a chronic and debilitating condition that results from multiple adverse synergistic risk factors that affect the mind, body, and soul.[27] While some see poverty as strictly an economic state, others consider it a condition of political vulnerability, others still view poverty as a measure of social class.[28] According to Haughton & Khandler[29], poverty is a pronounced deprivation of well-being. A 'poor'

[27] Eric Jensen, *Teaching with poverty in mind* (Virginia: ASCD, 2009).

[28] Rawyat Deonandan, "Defining poverty: A summary of competing models" (2019) 2:1 Journal of Social and Political Sciences 17–21.

[29] *UNDP 1994. Human development report 1994* (New York: United Nations: UNDP, 1994).

individual does not enjoy the opportunities and choices of human development that afford the potentiality of a long, healthy, and self-accomplished life.

To be free from poverty is to enjoy the privileges of education, expect a reasonably comfortable standard of life, self-respect, dignity to participate in the community, and to be able to live in freedom.[30] As observed by the United Nations[31], poverty connotes a denial of choices and opportunities and constitutes a violation of human dignity. Poverty implies the lack of a basic capacity to participate effectively in society. This study conceptualises poverty as a state of deprivation whereby access to basic institutions that ensure well-being are denied and individuals face increased susceptibility to indices of negative human development. Living in a state of poverty is characterized by inadequate access to food, healthcare, employment, and education. Poverty describes a state of perpetual vulnerability to the outbreak of communicable diseases, insecurity, violence, social exclusion, and crime. From this, we can see how pervasive poverty can trigger and escalate cybercrime in Nigeria.

Table 3. Forms of Poverty

SN	Form	Narrative
1	*Income or consumption*	Lack of monetary resources to meet needs.
2	*Absolute* poverty	Poverty below a set line of what is required to access minimum survival needs.
3	Shelter poverty, food poverty, asset poverty, time-poverty or health poverty	Lack of respective good.
4	Situational poverty	Generally caused by a crisis or loss and is often temporary. Events causing situational poverty include environmental disasters, divorce, or severe health problems.
5	Generational poverty	This occurs in families where at least two generations have been born into poverty. Families living in this type of poverty are not equipped with the tools to move out of their situations.
6	Relative poverty	Refers to the economic status of a family whose income is insufficient to meet its society's average standard of living.
7	Urban poverty	Occurs in metropolitan areas with populations of at least 50,000 people. The urban poor deal with a complex aggregate of chronic and acute stressors (including crowding, violence, and noise) and are dependent on, often inadequate, large-city services.
8	Rural poverty	Occurs in nonmetropolitan areas with populations below 50,000. In rural areas, there are more single-guardian households, and families often have less access to services, support for disabilities, and quality education opportunities.
9	*Multidimensional* poverty	Recognizes the multiple ways people can be deprived.
10	*Child poverty*	Refers to the deprivation of the material, spiritual and emotional resources children need to survive, develop and

[30] J Haughton & SR Khandker, *Handbook on poverty and inequality* (Washington DC: World Bank, 2009).

[31] United Nations, *The real wealth of nations: Pathways to human development* (New York: Palgrave Macmillan, 2010).

		thrive, and enjoy their rights, and achieve their full potential.
11	The *transiently poor*	People who move in and out of poverty.
12	The *chronically poor*	People who experience poverty for prolonged periods of time, even their whole lives.
13	*Vulnerability to poverty*	The probability or risk of experiencing poverty in the future.

Source: Adapted from Jensen (2009) and Rohwerder (2016)

B. Cybercrime

'Cybercrime' is defined as the use of computers and the internet to defraud individuals, groups of individuals, or organizations, ranging from identity and credit card theft to money laundering by terrorists, and organized crime syndicates.[32] Adesina[33] defines cybercrime as crimes committed on the internet with a computer as either a tool or a beset victim. It encompasses all illicit activities committed by one or more people, referred to as internet fraudsters, hackers, scammers, cyber citizens, or 419ers, who use the internet through the medium of networked computers, telephones, and other information and communications technologies (ICT). Odinma as cited in Makeri[34] describes cybercrime as a criminal activity involving information technology infrastructure, including unauthorized access, illegal interception, data interference, systems identity theft, and electronic fraud.

Cybercrime may be committed by technical means of data to, from, or within a computer network. It is aimed at interfering with the functioning of a computer system by inputting, transmitting, damaging, or altering computer data. 'Cybercrimes' are a set of criminal offenses that have been committed, or made possible, by the use of computer technologies, including traditional crime that has been so shaped by the use of a computer that it requires an understanding of computers by law enforcement agents to solve.[35] Cybercrime is the crime perpetrated through the communication process on computer devices with the aid of the internet and computer applications to extort victims of their hard-earned money or property.[36] This study, therefore, defines cybercrime as a crime involving the use of computers and the internet to either extort money or information from unsuspecting victims or to infect a computer network to steal a victim's identity.

[32] Jack Jackson & Jack Jackson, "Cybercrime and the challenges of socio-economic development in Nigeria" (2016) 14:2 JORIND 42–49.

[33] Adesina Olubukola Stella, "Cybercrime and poverty in Nigeria" (2017) 13:4 Canadian Social Science 19–29.

[34] Yakubu Ajiji Makeri, "Makeri, Yakubu Ajiji. 2017. 'Cybersecurity issues in Nigeria and challenges.' International Journal of Advanced Research in Computer Science and Software Engineering 7(4): 315-321" (2017) 7:4 International Journal of Advanced Research in Computer Science and Software Engineering 315–321.

[35] Chioma Chigozie-Okwum, Michael Daniel, & Ugboaja Samuel, "Computer forensics investigation: Implications for improved cybersecurity in Nigeria" (2017) 6:1 International Journal of Science and Technology 59–73.

[36] Taiwo Oluwadare & Igbekoyi Kayode, "Prevalence and consequences of cybercrime perpetrated by students in public tertiary institutions in Ekiti state" (2019) 2:1 International Journal of Arts, Languages and Business Studies 211–224.

Table 4. Forms of Cybercrime

SN	Form	Narrative
1	Hacking	Breaking into a person's computer to compromise information. This is often perpetuated from a remote location and takes advantage of loopholes in the victim's computer program. Hackers can also monitor what the victim does on the computer and can import files such as passwords, credit card information, company data, business plans, etc.
2	Cyber-theft	The use of a computer to steal electronic information falls under this category. Herein, hackers break into the system of banks and transfer money to a third-party account. Cyber-theft is one of the most common forms of cybercrime as it promises a large sum of money for experienced cyber-criminals. Cybercriminals access a victim's banking information to siphon money or buy expensive items in the victim's name.
3	Cyberstalking	This refers to the subjection of an individual to harassment over the internet. It often involves sending life-threatening messages to the victim.
4	Software, viruses, and worms	Cybercriminals also create and spread malicious, internet-based software known as viruses and worms to disrupt a victim's computer network and gain access to sensitive information or to cause damage to the system. Viruses and worms are capable of damaging systems and are often attached to other programs or documents through which it enters the computer.
5	*Cyberterrorism*	This is a large-scale disruption of computer networks through viruses to spread fear and panic or to destroy computer networks for political or ideological reasons.
6	*Cyber espionage*	This refers to the illegal use of a computer to steal state secrets, spy on another government, or gain information about a government's clandestine operation.
7	Child soliciting and abuse	Cybercriminals are known to solicit for and abuse minors in chat rooms for child pornography.
8	Intellectual theft	This occurs when a person violates copyrights or downloads unlicensed intellectual properties such as movies, music, games, and software on the internet. Disturbingly, some websites encourage software piracy.
9	Phishing, website cloning, and spamming	Cybercriminals are known to spam emails by sending mass emails to promote and advertise fictitious products and websites. In a bid to promote these businesses or products, these criminals may clone a well-known website to deceive their victims who often end up inputting their credit card details and other personal information which criminals later use to commit credit card fraud. Moreover, cybercriminals are also in the habit of posing as a known dignitary or celebrity to lure their victims into business transactions. This is a very common form of cybercrime in Nigeria.
10	Business Email Compromise [BEC] and romance fraud	BEC, another common cybercrime in Nigeria, is the act of sending emails from a spoofed or compromised account to the victim company's financial institution requesting a wire transfer. Once the transfer is sent, the payment details are intercepted by criminals and changed. These fraud operations are often driven by syndicates based in Nigeria, which may target a U.S.-based business and then move stolen funds to Mexico, Ireland, or China.

		Nigerian cybercriminals are also known to pretend to be the opposite gender of their victim in a bid to facilitate romance and gain the trust of the victim before attacking.

***Source*:** African Cyber Security (2019); Chigozie et al. (2017); Makeri (2017)

C. National Security

National security has been used to describe the capacity for self-defense. However, Asad as cited in Awosusi & Ogbuleke[37] argues that national security cannot be understood in exclusively military terms. Socio-economic and cultural aspects of development and modernization, and national integration are all deeply intwined in national security. Okoli & Opaleke[38] assert that national security encompasses the protection of a political entity from any form of threat, whether political, social, economic, military, psychological, or technological. Aladenusi[39] opines that national security comprises a mixture of political resilience, human resources, economic structures, technological capability, industrial base, availability of natural resources, and military prowess.

According to Holmes[40], national security refers to the protection of the state as a whole. Protecting the state from attack is the highest order of national security. It involves the use of armed forces to protect the state from external dangers and guard state secrets. National security encompasses both national defense and the protection of a series of interests including economic and geopolitical interests. From this, the working definition of this study is: national security refers to a states' provision of basic conditions that guarantee economic well-being as well as human and state security from both internal and external threats. 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.

IV. THE EXTENT OF CYBERCRIME IN NIGERIA

According to Shiloh & Fassassi[41], hundreds of millions of cyberattacks take place in Africa every year; banks and offices are usually, and increasingly, targeted by hackers. In these attacks South Africa, Kenya, and Nigeria tend to pay the highest prices. Indeed, cybercrime costs the world economy $500 billion annually, more than the GDP of

[37] Oladotun Emmanuel Awosusi & Ogbuleke Loveday Enyinnaya, "Critical thinking in information technology and management for national security in Nigeria" (2019) 3:3 Asian Journal of Applied Science and Technology 41–52.

[38] Okoli & Okpaleke Francis, *supra* note 9.

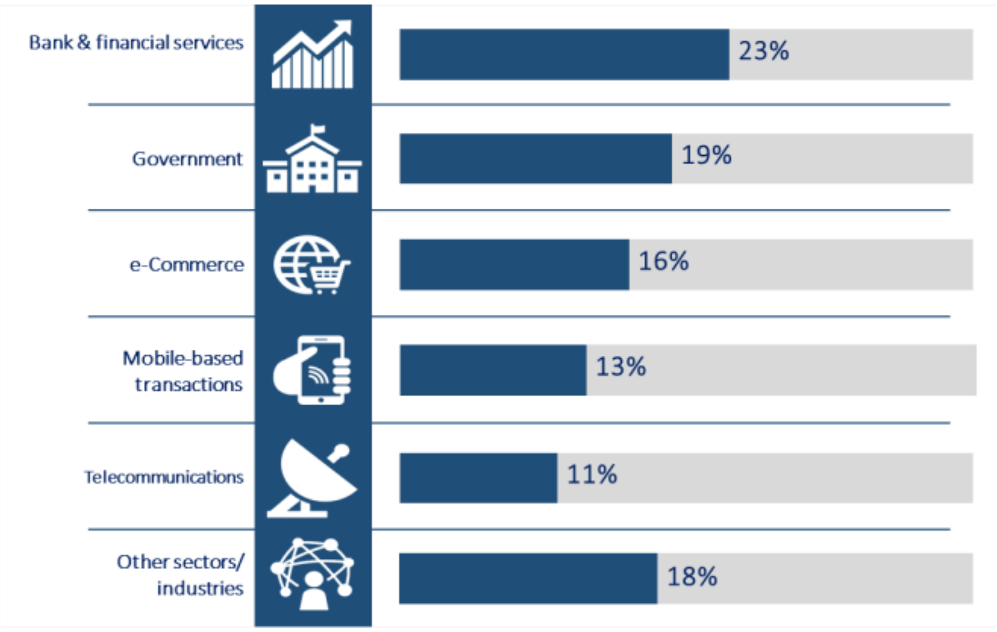
[39] Tope Aladenusi, *Solving national security challenges with information technology* (2014).

[40] Kim R Holmes, "What Is National Security?" (2015) 10.

[41] Amzath Fassassi & Claude Akoussan, "Cybercrime in Africa: Facts and figures", online: <https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/>.

Africa's largest economy, Nigeria. Shiloh & Fassassi[42] assert that cybercrime costs the Nigerian economy a total of $500 million per annum while Signe & Signe (2018) put the figure at $649 million in 2017, followed by Kenya with an annual loss of $210 million. Signe & Signe[43] also stress that, in Nigeria, and indeed all over Africa, financial institutions, the government, and industries are the three most affected industries.

Fig. 1 - Cybercrime cost in Africa by industry



Source: Signe & Signe (2016)

Africa lost a total of $3.5 billion to cybercrime in 2017 alone. A further review of this indicates that in comparison to other countries in Africa, Nigeria suffers the highest cost of cybercrime despite being home to the highest number of certified professionals. This is followed by Kenya, Tanzania, and Uganda (see Table 5). Ajala[44] posits that Nigeria loses about N127 billion, 0.8 percent of the country's GDP to cybercrime annually. Meanwhile, the Financial Derivatives Company [FDC] (2020) reports that the estimated annual financial loss in Nigeria relating to cybercrime was N250 billion ($649 million) in 2017 and N288 billion ($800 million) in 2018.

Table 5 - Cost of cybercrime: Nigeria in comparison to other countries in Africa

[42] *Ibid.*

[43] Landry Signe & Signe Kevin, "Global cybercrimes and weak cybersecurity threaten businesses in Africa", (2018), online: <https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/>.

[44] Samuel Akindele Ajala, "Fight against cybercrime: Nigeria ranked 57th globally", (27 July 2019), online: <https://www.premiumtimesng.com/news/top-news/343442-fight-against-cybercrime-nigeria-ranked-57th-globally.html>.

	Population (2017 Est.)	GDP (2017) in USD	Penetration % Population (2017)	Estimated cost of cybercrime (2017)	Estimated No. of Certified Professionals
Africa	**1,300,000,000**	**$3.3T**	**35%**	**$3.5B**	**10,000**
Nigeria	195,875,237	$405B	50%	$649M	1800
Kenya	50,950,879	$70.5B	85%	$210M	1600
Tanzania	59,091,392	$47B	39%	$99M	300
Uganda	44,270,563	$24B	43%	$67M	350
Ghana	29,463,643	$43B	34%	$54M	500
Namibia	2,587,801	$11B	31%	*	75
Botswana	2,333,201	$15.6B	40%	*	60
Lesotho	2,263,010	$2.3B	28%	*	30
Mauritius	1,268,315	$12.2B	63%	*	125

Source: Extracted from African Security Report (2019).

Nigeria is among the countries that engage in unlicensed software installation. In 2009, the rate of unlicensed software installation in Nigeria was 83% with a commercial value of $156 million. This fell to 82% in 2011 with an increased value of $251 million. This continued to drop for the years 2013 and 2015, 81% with a commercial value of $287 million and 80% with a commercial value of $287 million respectively. This is the second highest in Africa, after South Africa.[45]

According to Scamwatch[46], in Australia alone a total of $104,522 has been lost to 'Nigerian Scams'. 'Nigerian scam,' as used here, refers to a scheme whereby someone overseas offers a potential victim a share in a large sum of money or a payment on the condition that the victim helps the perpetrator transfer money out of their country. Although these scams are now used all over the world, their origin in Nigeria has led them to be dubbed 'Nigerian 419,' which refers to a section of Nigeria's Criminal Code that outlaws the practice.

Scamwatch further reports that Nigerian scams are implemented through several methods including via email, social networking, text message, the internet, mobile applications, telephone, fax, personally, and post. Of these methods, email delivery is the most common. The report also claims that these scams target people irrespective of age, despite the fact that the elderly make up the majority of their victims, male targets far outweight their female counterparts although theNigerian scam does not appear to be bound to any particular location.

[45] The Software Alliance, "Seizing opportunity through license compliance: BSA global software survey", *Washington: BSA* (2016), online: <https://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf#page=5>.

[46] "Nigerian scams stats for 2020", *Scamwatch* (2020), online: <https://www.scamwatch.gov.au/scam-statistics?scamid=6&date=2020>.

A. Case Study: Raymond Igbalode Abass (Hushpuppi)

Born to a taxi driver and bread seller in Lagos, Nigeria, on June 14 1982, Abass grew up on the streets, working as a beggar and gambler for much of his life, before turning to cybercrime where he amassed great wealth.[47] Abass moved to Malaysia, working in fashion, before relocating to the United Arab Emirates [UAE]. Despite claiming to be an estate developer, Abass is known for flaunting some of the most valuable cars in the world, expensive clothing, wristwatches, shoes, etc. on his social media handles which are not consistent with his self-proclaimed profession.[48]

Abass was arrested by the Dubai police on June 10, 2020, alongside 12 other accomplices in connection with multiple fraud charges amounting to $35million. He was reportedly involved in the dispatch of letters from email addresses almost identical to those of legitimate companies, prompting customers to divert payments to themselves.[49] He and Olalekan Jacob Ponle (Woodberry) were accused of committing additional crimes outside the UAE, including hacking, money laundering, banking fraud, cyber-fraud, criminal impersonation, and identity theft. The Dubai CID claimed incriminating documents that detailed planned frauds worth a total of $435 million were found. They also seized $40.9 million in cash, 21 laptop computers, 12 luxury cars valued at $6.8 million, 47 Smartphones, five hard disks, and 15 memory sticks, containing 119,580 fraud files and the addresses of 1,926,400 victims.[50]

V. POVERTY, CYBERCRIME AND NATIONAL SECURITY IN NIGERIA: AN INTERPLAY

Before the transformational permeation of digital technology in Nigeria, financial fraudsters, popularly known as '419ers,' already operated in the city of Lagos. These groups were mainly comprised of a mix of educated and illiterate adult men and women, who specialized in using fax machines to defraud unsuspecting Nigerians and foreigners. The BBC corroborates this in its 2019 report which states that the first surge of Nigerian 419 scammers were mostly uneducated criminals, while the next wave comprised of young, educated men who were frustrated by the lack of formal jobs in an economy ruined by a protracted military interregnum and years of economic

[47] Naijalebrity, "Hushpuppi biography: Arrested, age, real name, income, controversy, shoes, cars, house net worth", (2020), online: <https://naijalebrity.com/top-of-the/hushpuppi/hushpuppi-biography-age-real-name-cars-house-arrested-shoes?content>.

[48]Daniel Semeniworima, "Hushpuppi arrested: Nigerian, Raymond Igbalode or Ramon Olorunwa Abbas wey FBI wan sentence for fraud dey MCC Chicago, Federal Bureau of Prisons BOP in Chicago, Illinois USA", *BBC* (2020), online: <https://www.bbc.com/pidgin/tori-53300260>.

[49] "Saharareporters 2020. 'Why we arrested Hushpuppi —Dubai police.'", *Saharareporters* (2020), online: <http://saharareporters.com/2020/06/18/why-we-arrested-hushpuppi-E2%80%94dubai-police>.

[50] William Ukpe, "Hushpuppi extradited to the United States", (2020), online: <https://nairametrics.com/2020/07/02/hushpuppi-extradited-to-the-united-states/#:~:text=Hushpuppi%20and%20Woodberry%20were%20arrested,operation%20%E2%80%9C%20Fox%20Hunt%202%E2%80%9D.&text=The%20suspects%20are%20accused%20of,banking%20fraud%20and%20identity%20theft.>.

mismanagement.[51] This group of educated men were taken aback by the wealth and esteem of the uneducated scammers and decided to join them, viewing their activities as a means of employment and route out of poverty.

In the context of widespread unemployment and poverty, further complicated by deeply entrenched political corruption, these cybercriminals have become somewhat of a beacon of hope for Nigerian youth. Many Nigerians admire these young scammers, marveling at the ingenuity and audacity that enables them to swipe, with ease, millions of dollars from American neuroscientists, British CEOs, and German scholars.[52] As Ezea[53] notes, in the early 1990s, the group of scammers in Nigeria were influential people in society, commanding respect from their ostentatious lifestyle. The views of both Ezea and the BBC lend credence to the crux of this paper: that the proliferation of cybercrime in Nigeria is an outcome of widespread poverty and has continually undermined the government's efforts to protect national security. The Nigerian government has been unable to fulfil its primary duty to protect the economic interests of Nigerians from both internal and external threats.

There are also concerns that Nigerian scammers have hampered Nigeria's international reputation. The business chances of genuine, young entrepreneurs are increasingly strained as countries apply caution in granting visas to Nigerians.[54] Signe & Signe[55] note that cybercrime decimates the reputation of a country, creating a hostile business environment for small and medium-sized enterprises (SMEs) and start-ups. This environment also discourages foreign economic investment. This is troublesome considering that after the arrest of Abass (case study), six Nigerians were placed on the FBI's most-wanted list, alongside 73 others from different countries. The six Nigerians – Alex Ogunshakin, Richard Uzuh, Abiola Kayode, Micheal Olorunyomi, Nnamdi Benson, and Felix Okpoh – were accused of perpetrating Business Email Compromise and romance scams totalling $6.3m in U.S. losses.[56] What's more, individuals are not spared from the fangs of cybercrime which has a domino effect on their financial resources, personal confidential information, and intellectual property. The costs are far-reaching and often target vulnerable, elderly populations. For instance, in 2018, in the US, roughly 62,000 people aged 60 or over reported losses totaling over $649 million.

As Scamwatch stresses, the majority of the victims of Nigerian scams are senior citizens. Reporting for Nigeria Deposit Insurance Corporation [NDIC], Umaru (2019) not only states that poverty is a tenable cause for cybercrime but that cybercrime also tarnishes a country's image, and deters tourists and potential investors from visiting

[51]"Letter from Africa: Why Nigeria's internet scammers are 'role models'", *BBC* (2019), online: <https://www.bbc.com/news/world-africa-49759392>.

[52] *Ibid*.

[53] S Ezea, *Ezea, S. (2017). The prevalence of internet fraud among Nigerian youths. Nigeria: The Guardian Saturday Magazine* (Nigeria: The Guardian Saturday Magazine, 2017).

[54] note 51.

[55] Signe & Signe Kevin, *supra* note 43.

[56] Eniola Akinkuotu, ""$6.3m fraud: Six Nigerians placed on the FBI's most-wanted list.", online: <https://punchng.com/6-3m-fraud-six-nigerians-placed-on-fbi-most-wanted-list/>.

and investing in the country. This has grim consequences for the nation's macroeconomic stability on one hand, and financial inclusion on the other. This is due to the fear of being a victim of a cyberattack. Umaru's submission is at the heart of this study, which is hinged on the notion that the national interest of a state, in terms of both economic welfare and well-being is greatly hampered by cybercrime. Cybercrime remains one of the critical drivers of national embarrassment for Nigeria, contributing to the reduced confidence placed in a country's financial system (Umaru, 2019). The fear of cybercrime has made some persons avoid the use of information and communication technologies (ICT) which can cause adverse effects on the welfare of both the citizenry and (potential) investors.[57]

Engaging in social interactions of any kind with foreigners over the internet has become a problematic for Nigerians who are faced with the onerous task of proving that you are not a potential scammer. That is, if you are even afforded the respect of clarification. Honest Nigerians have lost their confidence in the country due to the slow progress of cybersecurity. This loss of confidence may also affect the country's developmental progress as foreign investments face challenges integrating into the economy. This relegates the nation to the status of an economic pariah. Meanwhile, cybercrime continues to threaten the lives of Nigerians. According to Ogunseye[58], The Boko Haram sect hacked the servers of the Department of State Security on August 30 2013, leaking the details of over 60 officials, including their addresses and the names of family members. This posed a very real threat to the lives of the officials, their family members, and of course, strained national security.

Beyond the rhetoric, Nigerians have lost confidence in the banking sector as a result of cybercrime. Umaru[59] notes that cybercrime has led to an increase in the operating cost of businesses due to huge expenses incurred through the purchase of security software applications to reduce the rate of cyberattacks. As noted earlier (figure 1), the banking sector has been worst hit by cybercrime in Africa. The contribution of cybercrime to the total fraud committed in Nigeria has consistently risen. Between 2011 and 2016, cybercrime has been responsible for an average of 40% of the total fraud committed in the banking sector.

Table 6 - Contribution of Cybercrime to Total Fraud Loss in the Nigerian Banking Industry (2011-2016)

Year	Cybercrime losses (ATM & Internet) (N billion)	The growth rate of cyber-crime losses (%) year-on-year	Total Fraud Loss (N billion)	Contribution Of Cyber Crimes To Total Fraud (%)

[57] Ibrahim Umaru, "The impact of cybercrime on the Nigerian economy and banking system. Nigeria Deposit Insurance Corporation", (2019), online: <https://ndic.gov.ng/wp-content/uploads/2020/03/NDIC-Quarterly-Q1-and-Q2-2019-Article-The-Impact-of-Cybercrime-on-The-Nigerian-Economy-and-Banking-System-.pdf>.

[58] T Ogunseye, *Ogunseye, T. "Boko Haram: Intelligence operatives investigate Nigerians in the UK." The Punch 5 (2012).* (The Punch 5, 2012).

[59] Ibrahim Umaru, *supra* note 57.

2011	0.115	-	4.071	2.82
2012	0.794	590.4	4.516	17.58
2013	2.268	185.6	5.757	39.40
2014	4.438	95.6	6.193	71.66
2015	1.361	-69.3	3.173	42.89
2016	1.058	-22.2	2.4459	43.26

Source: NDIC Annual Report (2011-2016), extracted from Umaru (2019)

Due to the pervasive reach of poverty, many start-ups and small and medium-sized enterprises cannot afford cybersecurity. Schjolberg[60] asserts that poor countries are usually at the mercy of cybercriminals. Security measures in developing countries are less rigorous than those in other parts of the world. This has made them attractive targets. In May 2016, the national bank of Bangladesh fell victim to a cyberattack and was robbed. The same thing happened to banks in Ecuador, the Philippines, and Vietnam in 2015 and 2016. African Cyber Security reports that most business outfits in Africa perceive cybersecurity as a highly technical and expensive affair.[61] They struggle to determine the appropriate level of security and budgeting for security initiatives. It is also observed that most organizations in Africa operate below the poverty line, making it difficult for them to effectively protect themselves against losses to cyber attackers.

Of course, most businesses, especially SMEs, struggle to establish basic cybersecurity structures. Over 95% of African organizations in both the private and public sectors operate either on or below the security poverty line. SMEs are faced with several challenges, including the prohibitive cost of Cybersecurity solutions, services, limited budgets, and lack of skilled personnel. With these challenges, it has not been possible for many companies to adopt effective Cybersecurity frameworks, leaving them exposed and vulnerable to attacks.[62] From this, it is deducible that poverty not only provides impetus to cybercrime, but also makes it difficult for businesses to protect themselves against it, serving as another stimulus for its incursion.

More specifically, Ibrahim & Dabugat[63] note that a major implication of cybercrime for national security in Nigeria is communal and sectarian violence. They affirm that social media is being used to spread hate speech and divisive content that create or exacerbate tension between different groups in the country. For example, social media has played a major role in framing the prevailing farmer-herder conflict as an ethnoreligious crusade. Jacobson[64] asserts that, in addition to using cyberspace to incite violence, cybercriminals are starting to commit acts of terrorism via computer networks. Cyberterrorism, cyberespionage, insurgency financing, and recruitment are

[60] Stein Schjolberg & Solange Ghernaoti-Helie, *A global treaty on cybersecurity and cybercrime* (Norway: AiTOslo, 2011).

[61] Jibrin Ibrahim & Dabugat Kop'ep, *Rural banditry and hate speech in northern Nigeria: Fertile ground for the construction of dangerous narratives in Nigeria*, in mohammed kuna and ibrahim ibrahim (ed). rural banditry and conflict in northern nigerian ed (Abuja: Centre for Democracy and Development CDD, 2016).

[62] *2019 global threat report: Adversary tradecraft and the importance of speed.*, by African Cyber Security (2019).

[63] Ibrahim & Dabugat Kop'ep, *supra* note 61.

[64] Michael Jacobson, "Terrorist financing on the Internet" (2009) 2:6 CTC Sentinel 17–20.

gradually becoming an internet norm. Indeed, cyberspace is now being used to solicit funds, increase membership to terrorist organizations, drive ideological indoctrination, and promote radicalization. Ogunseye[65] claims that the Boko Haram insurgency group in Nigeria has begun developing a cyber presence.

Moreover, Okoli & Idom[66] submit that Nigeria's security is constantly threatened by spies and hackers who seek to steal the identity of high profile Nigerians to stalk, harass, and manipulate victims into obtaining their personal information and defrauding them. This has far-reaching implications for their safety; in some cases people have been defrauded and even abducted through hacked social media accounts. Furthermore, the websites of the Independent National Electoral Commission (INEC) and the Lagos State Government were reportedly hacked and defaced in 2015, indicating that even government establishments are not safe from cybercrime.

VI. GOVERNMENT RESPONSE AND SOLUTION TO CYBERCRIME IN NIGERIA

A cursory review of the trend analysis of cybercrime in Nigeria reveals that it is deeply entrenched and requires government attention. Omodunbi, Olaniyan & Esan[67] claim that cybercrime in Nigeria has a long history and generally takes several forms including BVN scams, banking fraud, sale fraud and forgery, data and airtime theft, software piracy, Nigerian prince scam, charity funds, and social hi-jacking. As a result, the Nigerian government has promulgated several laws to address cybercrime in Nigeria. The major legal framework for combating cybercrime in Nigeria is the Cybercrime Act, 2015, though several other pieces of legislation preceeded this. According to Ufuoma & Ohwomeregwa[68], before the Cybercrime Act of 2015, the relevant laws in operation in Nigeria were: the Economic and Financial Crimes Commission (Establishment) Act, 2004; the Advanced Fee Fraud and Other Related Offences Act, 2006; the National Identity Management Commission Act, 2007; Money Laundering (Prohibition) Act, 2011 as amended in 2013; the Nigerian Evidence Act; The Criminal Code Act; The Penal Code Act; the Cybersecurity Act of 2011; and the Terrorism (Prevention) Act. As Ufuoma & Ohwomeregwa[69] argue, the aforementioned legislation were insufficient to regulate the elaborate activities that constitute cybercrime and lacked effective enforcement mechanisms.

The Cybercrime Act, 2015 was the first cybercrime legislation enacted by the National Assembly of the Federal Republic of Nigeria for the prohibition, prevention, and prosecution of cybercrimes and other related issues. Its objectives are:

[65] T. Ogunseye, *supra* note 58.

[66] Al Chukwuma Okoli & Idom Augustine Mogom, "The internet and national security in Nigeria: A threat-import discourse" (2018) 6:1 Covenant University Journal of Politics & International Affairs 20–29.

[67] Bolaji Omodunbi et al, "Cybercrimes in Nigeria: Analysis, detection, and prevention" (2016) 1:1 FUOYE Journal of Engineering and Technology 37–42.

[68] Awhefeafa Ufuoma & Ohwomeregwa Ogechi, "Appraising the laws governing the control of cybercrime in Nigeria" (2020) 8:1 Journal of Law and Criminal Justice 30–49.

[69] *Ibid*.

(a) to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria;
(b) to ensure the protection of critical national information infrastructure; and
(c) to promote cybersecurity and the protection of computer systems and networks, electronic communications, data, computer programs, intellectual property, and privacy rights.

As contained in Part II of the Act, The President may, on the recommendation of the National Security Adviser, designate certain computer systems, networks, and information infrastructures vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure. This implies that the Act recognizes computer infrastructure as a vital component of national security and as a prerequisite to ensuring the economic welfare of Nigerians.

According to Part III of the Act, the offense of cybercrime in Nigeria includes offenses against critical national information infrastructure; unlawful access to a computer; unlawful interception of communications; unauthorized modification of computer programs or data; system interference; misuse of devices; computer-related forgery; computer-related fraud; identity theft and impersonation; child pornography and related offenses; cyberstalking; cybersquatting; cyberterrorism; racist and xenophobic offenses; attempt, conspiracy, aiding, and abetting; and corporate liability. The penalty for these offenses ranges from imprisonment to death sentence and/or a fine of 5,000,000 ($12,904) to 25,000,000 ($64,523) depending on the offense.

Since the enactment of the Cybercrime Act, little progress has been made in the fight against cybercrime in Nigeria. Although the Act provides for the establishment of a Cybercrime Advisory Council to advise on "measures to prevent and combat computer-related offenses, cybercrimes, threats to national cyberspace and other cybersecurity-related issues"[70], the Act is bereft of specific cybersecurity measures to be taken in combating cybercrime. To be sure, the spate of cybercrime has not abated. As such, this study now turns to assess the future of cybersecurity.

Nigeria ranks 57 out of 175 countries in the global campaign against cybercrime globally on the Global Cybersecurity Index (GCI).[71] Nigeria's commitment to the fight against cybercrime is ranked 'medium,' alongside South Africa, Uganda, Tunisia, Pakistan, Mexico, UAE, Kuwait, Iran, Greece, and 45 others. This is against countries like Kenya, Egypt, the USA, United Kingdom, Korea, Japan, and France whose commitment level is considered 'high.' As such, it is clear that Nigeria's government has far more work to do to enhance their cybersecurity.

[70] Federal Government of Nigeria, *Cybercrime Act* (2015).
[71] Samuel Akindele Ajala, *supra* note 44.

Ghernaouti-Helie[72] avers the pertinence inherent in developing a cybersecurity culture that cannot be overruled. Cybersecurity promises to increase the level of understanding of members of the cybersecurity chain dealing with essential social, economic, and legal issues related to information security and contributes to helping countries prepare for challenges related to the uses and misuses of ICT. Schjolerb & Ghernaouti-Helie think that capacity-building and human resource development are needed to sustain an effective cybersecurity culture. Capacity-building refers to the creation of an enabling environment with appropriate policy frameworks. Human resource development is the process of equipping individuals with the appropriate understanding, skills, and access to information, knowledge, and training, enabling effective performance.

Nigeria must improve its capacity building and human capital development to lay the groundwork for a more effective cybersecurity system government and other stakeholders need to be more focused on Sensitization and cybersecurity education. Cybersecurity should be treated as an integral part of the schooling system and should be present throughout the various levels of education (Technical College, College of Education, Polytechnic and University) in all relevant fields (political sciences, economics, business, engineering, social, and legal fields.) As noted earlier, education is a critical factor in building human capital. Education reinforces competitiveness, employment, and social integration. As such Schjolerb & Ghernaouti-Helie argue that education should be considered an essential component in enhancing confidence and security in the use of ICT and cybersecurity.

IV. CONCLUSION

From the preceding analysis, this study concludes that poverty is a major driver of cybercrime in Nigeria. With the prevalence of multidimensional poverty, deprivation, and inequality, unguided Nigerian youth are forced to turn to crime as a means of bridging the gap between their reality and the Nigeria of their dreams. As such, proper attention must be paid to human capital development to ensure youth have reasonable access to sustainable employment opportunities, reducing their susceptibility to recruitment for cybercrime. Decisive policies targeted at reducing widespread unemployment and poverty should be prioritized by the government to reduce the level of poverty and inequality in the country.

There is an urgent need to sensitize youth to the dangers of cybercrime and its incapacitating effect on national security in Nigeria. Further, cybercrime's effect on the country's image, consequent restricted business opportunities, and social interaction should also be emphasized.

Cybersecurity should be taken seriously by the Cyber Advisory Council and offenders of cybercrime should be dealt with appropriately, serving as a deterrent to potential offenders. Moreover, cybersecurity should be integrated into Nigerian

[72] Schjolberg & Solange Ghernaoti-Helie, *supra* note 60.

education systems through an interdisciplinary course to facilitate capacity building and promote human capital development.

Finally, the Nigerian government should work in conjunction with the Nigerian Police to establish 'Anti-Scam Reporting Channels' across its thirty-six states. With this, Nigerians can promptly report suspected cybercriminals. At the same time, a Cyber Forensics Department should be created to analyze and track of cyber activities and investigate any suspected acts of cybercrime.

ACKNOWLEDGMENT

None

COMPETING INTERESTS

None

REFERENCES

Eric Jensen, Teaching with poverty in mind (Virginia: ASCD, 2009).

Haughton, J & SR Khandker, Handbook on poverty and inequality (Washington DC: World Bank, 2009).

Ibrahim, Jibrin & Dabugat Kop'ep, Rural banditry and hate speech in northern Nigeria: Fertile ground for the construction of dangerous narratives in Nigeria, in mohammed kuna and ibrahim ibrahim (ed). rural banditry and conflict in northern nigerian ed (Abuja: Centre for Democracy and Development CDD, 2016).

Peter Townsend, Poverty in the United Kingdom: A survey of household resources and standards of living (Harmodsworth: Penguin Books Ltd, 1979).

Rudolph Rummel, "Frustration, deprivation, aggression, and conflict helix." In: Understanding conflict and war (Beverly Hills, California: Sage Publications, 1977).

S Ezea, Ezea, S. (2017). The prevalence of internet fraud among Nigerian youths. Nigeria: The Guardian Saturday Magazine (Nigeria: The Guardian Saturday Magazine, 2017).

Schjolberg, Stein & Solange Ghernaoti-Helie, A global treaty on cybersecurity and cybercrime (Norway: AiTOslo, 2011).

T Ogunseye, Ogunseye, T. "Boko Haram: Intelligence operatives investigate Nigerians in the UK." The Punch 5 (2012). (The Punch 5, 2012).

Ted Robert Gurr, Why Men Rebel (Princeton: Center of International Studies, Princeto University, 1970).

United Nations, The real wealth of nations: Pathways to human development (New York: Palgrave Macmillan, 2010).

Awosusi, Oladotun Emmanuel & Ogbuleke Loveday Enyinnaya, "Critical thinking in information technology and management for national security in Nigeria" (2019) 3:3 Asian Journal of Applied Science and Technology 41–52.

Bonaventure Chigozie Uzoh, "Poverty–conflict nexus: The Nigerian experience" (2016) 3:10 The International Journal of Social Sciences and Humanities Invention 2832–2838.

Chioma Chigozie-Okwum, Michael Daniel, & Ugboaja Samuel, "Computer forensics investigation: Implications for improved cybersecurity in Nigeria" (2017) 6:1 International Journal of Science and Technology 59–73.

Daniel Semeniworima, "Hushpuppi arrested: Nigerian, Raymond Igbalode or Ramon Olorunwa Abbas wey FBI wan sentence for fraud dey MCC Chicago, Federal Bureau of Prisons BOP in Chicago, Illinois USA", BBC (2020), online: ‹https://www.bbc.com/pidgin/tori-53300260›.

David, Alao, Osah Goodnews & Eteete Michael, "Unabated cyber terrorism and human security in Nigeria." (2019) 15:11 Asian Social Science 105–115.

Eniola Akinkuotu, ""$6.3m fraud: Six Nigerians placed on the FBI's most-wanted list.", online: ‹https://punchng.com/6-3m-fraud-six-nigerians-placed-on-fbi-most-wanted-list/›.

Fassassi, Amzath & Claude Akoussan, "Cybercrime in Africa: Facts and figures", online: ‹https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/›.

Holmes, Kim R, "What Is National Security?" (2015) 10.

Ibrahim Umaru, "The impact of cybercrime on the Nigerian economy and banking system. Nigeria Deposit Insurance Corporation", (2019), online: ‹https://ndic.gov.ng/wp-content/uploads/2020/03/NDIC-Quarterly-Q1-and-Q2-2019-Article-The-Impact-of-Cybercrime-on-The-Nigerian-Economy-and-Banking-System-.pdf›.

Iheanacho, Agboti & Nnam Uchenna, "An assessment of the relationship between crime and social exclusion in Nigeria" (2015) 8:1 International Journal of Research in Arts and Social Sciences 157–164.

Jackson, Jack & Jack Jackson, "Cybercrime and the challenges of socio-economic development in Nigeria" (2016) 14:2 JORIND 42–49.

John Olayemi Odumesi, "A socio-technological analysis of cybercrime and cybersecurity in Nigeria" (2014) 6:3 International Journal of Sociology and Anthropology 116–125.

Michael Jacobson, "Terrorist financing on the Internet" (2009) 2:6 CTC Sentinel 17–20.

Nnam, Uchenna, Agboti Iheanacho, & M Otu, "Inadequate motivation as a reason for police officers' ineffectiveness in policing contemporary Nigeria" (2013) 15:2 South-South Journal of Culture and Development 67–86.

Okoli, Al Chukwuma & Idom Augustine Mogom, "The internet and national security in Nigeria: A threat-import discourse" (2018) 6:1 Covenant University Journal of Politics & International Affairs 20–29.

Okoli, Al Chukwuma & Okpaleke Francis, "Cattle rustling and dialectics of security in northern Nigeria" (2014) 2:3 International Journal of Liberal Arts and Social Science 109–117.

Olabanji, Olukayode & Ese Urhie, "Insecurity and socio-economic development in Nigeria" (2014) 5:1 Journal of Sustainable Development Studies 14–20.

Olubukola Stella, Adesina, "Cybercrime and poverty in Nigeria" (2017) 13:4 Canadian Social Science 19–29.

Oluwadare, Taiwo & Igbekoyi Kayode, "Prevalence and consequences of cybercrime perpetrated by students in public tertiary institutions in Ekiti state" (2019) 2:1 International Journal of Arts, Languages and Business Studies 211–224.

Omodunbi, Bolaji et al, "Cybercrimes in Nigeria: Analysis, detection, and prevention" (2016) 1:1 FUOYE Journal of Engineering and Technology 37–42.

Osho, Oluwafemi & Agada D Onoja, "National Cyber Security Policy And Strategy Of Nigeria: A Qualitative Analysis" (2015).

Rawyat Deonandan, "Defining poverty: A summary of competing models" (2019) 2:1 Journal of Social and Political Sciences 17–21.

Red24, "Cybercrime top 10 affected countries", (2015a), online: <https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+affected+countries+-2015.pdf>.

———, "Cybercrime Top 10 countries where attacks originate", (2015b), online: <https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf>.

Sam Ogunlere et al, "Impact of cybercrime on the Nigerian economy" (2013) 2:4 The International Journal of Engineering and Sciences 45–51.

Samuel Akindele Ajala, "Fight against cybercrime: Nigeria ranked 57th globally", (27 July 2019), online: <https://www.premiumtimesng.com/news/top-news/343442-fight-against-cybercrime-nigeria-ranked-57th-globally.html>.

The Software Alliance, "Seizing opportunity through license compliance: BSA global software survey", Washington: BSA (2016), online: <https://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf#page=5>.

Tope Shola Akinyetun, "A theoretical assessment of Boko Haram insurgency in Nigeria from relative deprivation and frustration-aggression perspectives" (2020) 1:2 African Journal of Terrorism and Insurgency Research 89–109.

Ufuoma, Awhefeafa & Ohwomeregwa Ogechi, "Appraising the laws governing the control of cybercrime in Nigeria" (2020) 8:1 Journal of Law and Criminal Justice 30–49.

William Ukpe, "Hushpuppi extradited to the United States", (2020), online: <https://nairametrics.com/2020/07/02/hushpuppi-extradited-to-the-united-states/#:~:text=Hushpuppi%20and%20Woodberry%20were%20arrested,operation%20%E2%80%9C%20Fox%20Hunt%202%E2%80%9D.&text=The%20suspects%20are%20accused%20of,banking%20fraud%20and%20identity%20theft.>.

Yakubu Ajiji Makeri, "Makeri, Yakubu Ajiji. 2017. 'Cybersecurity issues in Nigeria and challenges.' International Journal of Advanced Research in Computer Science and Software Engineering 7(4): 315-321" (2017) 7:4 International Journal of Advanced Research in Computer Science and Software Engineering 315–321.

"Letter from Africa: Why Nigeria's internet scammers are 'role models'", BBC (2019), online: <https://www.bbc.com/news/world-africa-49759392>.

"Nigerian scams stats for 2020", Scamwatch (2020), online: <https://www.scamwatch.gov.au/scam-statistics?scamid=6&date=2020>.

"Saharareporters 2020. 'Why we arrested Hushpuppi —Dubai police.'", Saharareporters (2020), online: <http://saharareporters.com/2020/06/18/why-we-arrested-hushpuppi-E2%80%94dubai-police>.

African Cyber Security, 2019 global threat report: Adversary tradecraft and the importance of speed., by African Cyber Security (2019).

Federal Government of Nigeria, Cybercrime Act (2015).

Naijalebrity, "Hushpuppi biography: Arrested, age, real name, income, controversy, shoes, cars, house net worth", (2020), online: <https://naijalebrity.com/top-of-the/hushpuppi/hushpuppi-biography-age-real-name-cars-house-arrested-shoes?content>.

NBS 2019, 2019 poverty and inequality in Nigeria: Executive summary, by NBS 2019 (Abuja: Proshare, 2019).

Signe, Landry & Signe Kevin, "Global cybercrimes and weak cybersecurity threaten businesses in Africa", (2018), online: <https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/>.

Simon Kemp, Digital 2020: Global digital overview, by Simon Kemp (2020).

Tope Aladenusi, Solving national security challenges with information technology (2014).

UNDP 1994. Human development report 1994 (New York: United Nations: UNDP, 1994).