

# WAR AGAINST CYBERCRIME: ASSESSING THE ROLE OF NIGERIAN GOVERNMENTS IN THE PROMOTION OF CYBERCRIME AMONG NIGERIAN YOUTHS, 2000 – 2020

Dr. Uchime, Victoria Ozioma  
Department of History & International Studies,  
Chukwuemeka Odumegwu Ojukwu University, Igbariam  
[ozioauchime@gmail.com](mailto:ozioauchime@gmail.com)

Dr. Molokwu, Ubaka Cosmas  
Department of History and International Studies,  
University of Nigeria, Nsukka.  
[cosmas.molokwu@unn.edu.ng](mailto:cosmas.molokwu@unn.edu.ng)

&

Ewa, Okoro Onu  
Department of History and International Studies,  
University of Nigeria, Nsukka. [okoro.ewa@unn.edu.ng](mailto:okoro.ewa@unn.edu.ng).

## Abstract

Cybercrime among Nigerian youths has rapidly been on the increase in recent times, plunging Nigeria into about #127 billion losses annually among other human and material losses. Arguably, this has been largely attributed to such factors as increasing youth unemployment, population increase, poverty, peer group influence, access to the internet, and mobile and computer technological improvement, among others. The Nigerian governments on their part have also adopted various measures including jobs creation, social intervention programmes, the introduction of Bank Verification Number (BVN), the establishment of the Nigerian Electronic Fraud Forum (NeFF), Nigerian Interbank Settlement System (NIBSS), Nigerian Deposit Monetary Banks (NDMB), Economic and Financial Crimes Commission (EFCC), Cybercrime Act, 2015, Independent Corrupt Practices and other Related Offences Commission (ICPC), among other measures towards curbing the surge of the menace of cybercrime; yet, the situation seems not abating. This paper, therefore, examines how Nigerian governments have contributed to the promotion of cybercrime among Nigerian youths. The paper adopts a qualitative research method, it utilizes secondary data. The paper employs a historical and analytical approach in the interpretation of its data. Findings reveal that the proliferation of cybercrime among Nigerian youths during the period under investigation is largely consequent upon the failure of the government to timely engage the youths in productive and gainful employment and poor implementation of the enacted anti-cybercrime policies in Nigeria.

**Keywords:** Cybercrime, Cybercrime Control, Nigerian Youths, Nigerian Government.

## Introduction

The war against cybercrime in Nigeria, especially by the government, has been raging on since the dawn of the 21st century, prompted essentially by the obvious harsh consequences the cybercriminals have inflicted on individuals, corporate organizations, government institutions, the economy, and imagine of the country, among others. What constitutes Cybercrime in Nigeria has been variously defined by scholars. The term, cybercrime, was coined by Peter Cassidy, Secretary General of the anti-phishing working group to distinguish computer programmes (and coordinated, interlocking sets of programmes) that are designed specifically to animate financial crimes from other kinds of malevolent packages (Shehu 2014:169). For

Nwosu (2018:3) cybercrime connotes criminal activities done using computers and the internet. He maintains that what constitutes cybercrime includes:

...anything from downloading illegal music files to stealing money from online bank accounts, scams, and all forms of obtaining money and valuables by making a false representation; non-monetary offenses such as creating and distributing viruses on other computers, posting confidential private or business information on the internet, identify theft, cyber threat, cyber-attacks, and cyber espionage (2018:3).

Similarly, according to Halder and Jaishanker cited in (Nwosu, 2018:169), cybercrimes are offenses committed against individuals or groups of individuals with a criminal intention to deliberately damage the reputation of the victim, or cause physical, mental harm, or financial loss to the victim directly or indirectly, by the help of modern telecommunication networks such as internet and smartphones. In tracing the origin of the word, 'cybercrime', Olivia (2022:18) argues that the term derives its definition from the word 'cyber' which has its origin in 'cybernetics' and refers to the science of communication that deals with the study of automatic control systems as well as mechanical and electrical communication systems. For McQuade (2006:134) Cybercrime is the employment of electronic devices or computers via information systems to facilitate illegal activities.

While the definitions above may largely reveal the meanings, channels, and motives of cybercrime across the world, Nigeria inclusive, it is pertinent to note that what mainly constitutes cybercrime among Nigerian youths includes: Spamming - an act of sending unsolicited messages to many users promoting products or services for dubious motives; Phishing - a high-tech identity theft that steals personal data and identity from unsuspecting consumers, legitimate businesses, and financial institutions; Cyber-stalking - the use of the Internet or other electronic communication devices to track a person's online activity to gather information that could be used to extort money from the victims by threats of exposing the information to the public; Fake copy-cat websites - the setting up by criminals of impersonator websites that take advantage of ignorant customers to hoodwink them; Cyber-squatting - an act of registering a name in bad faith, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark, and others (Nwosu, 2018:4-5).

Cybercrime, since the year 2000, has caused Nigeria and foreign investors in the country huge financial, reputational, and material loss. For instance, between 2000 to the first quarter of 2013, Nigerian banks lost #159 billion, and another #44 billion between January to September 2014 (Ude, March 31st, 2015: 63). For Nigerian consumers, in 2012 alone, a total of 13.5 billion dollars was lost to cybercriminals in the country (Clarke, 2004: 55). In 2018, commercial banks in Nigeria lost over NGN 15 billion (\$39 million) to cybercrime and electronic fraud and thereafter, its increasing rate has been recorded to the sum of NGN1.9 billion every year (Mohammed, Mohammed & Solanke, 2019: 59). Nigeria's apex bank, Central Bank of

Nigeria (CBN), in 2019, also confirmed that transaction values at #6.5 trillion were stolen by hackers (cyber criminals) on commercial banks in Nigeria (Mohammed, Mohammed & Solanke, 2019: 60). Foreign investors in Nigeria have also had their unfortunate share of cybercrime activities which has discouraged others from further investment in the country. Nigeria's image is also at stake consequent upon the activities of cybercriminals. It has created a bad image for the country and its nationals among the Committee of Nations (Jackson & Robert, 2016: 5).

The foregoing necessitated Nigeria's resolve to wage war against cybercrime in the country. Consequently, the Nigerian government created a central agency to implement crime laws, began regulation of cybercafés, enacted cyber laws and instituted a partnership with Microsoft (Jackson & Robert, 2016: 36). Specifically, in 2001, the Federal Government of Nigeria established the National Information Technology Development Agency (NITDA) and in 2007, enacted the National Information Technology Development Act (2007), Economic and Financial Crimes Commission (2002), Economic and Financial Crimes Commission Act, 2004; Nigerian Communication Agency (NCC, 2003); Nigerian Cybercrime Working Group (NCWG); Advance Fee Fraud Related Offences Act, 2006; Evidence Act, 2011; Cybercrime (Prohibition, Prevention, etc) Act, 2015 and many others towards regulating the cyberspace, cybercrime and ensuring conducive financial atmosphere in the country.

Despite the efforts of the Nigerian government to curb cybercrime in the country, Nigeria has continued to experience an unimaginable upsurge in cybercrime rate, especially, among the youth. Although scholars, economic and political analysts, and commentators have advanced certain factors as regards the causes and consequences of cybercrime in Nigeria; and efforts of the government towards tackling the menace, yet, adequate attention has not been extended to investigating government roles in the promotion of cybercrime among Nigerian youths which, this paper argues is largely responsible for the proliferation of cybercrime in the country.

### **Overview of Causes of Cybercrime among Nigerian Youths**

Nigerian youths' increasing involvement in cybercrime in recent times has been attributed to several different factors by scholars. Nwosu (2018) identifies the harsh economic climate and recession as one of the driving forces pushing Nigerian youths into cybercrime. According to him, "The harsh economic climate in the country which eventually led to the present recession forced many of the youth in Nigeria into embracing cybercrime as a means of livelihood." Oluwu cited in (Bello, 2018:40) attributed it to the high unemployment rate among African countries and argues that cybercrime may probably continue unabated until when the issue of unemployment is comprehensively addressed. Despite abundant human and natural resources at Nigeria's disposal, it appears surprising that chronic youth unemployment is evident

in the country (Adebayo, 2013:350). For Adebayo, the above largely explains why about 4.5 million youths enter the labour market every year without any hope of getting employment for life sustenance. This situation creates an avenue for a “devil's workshop” out of the youths.

Table 1: Youth Unemployment Rate in Nigeria, 2000 - 2020

Year Youth unemployment rate

2020	53.40%
2019	17.69%
2018	15.8%
2017	13.91%
2016	12.48%
2015	7.81%
2014	8.41%
2013	9.84%
2012	9.68%
2011	9.56%
2010	9.58%
2009	9.49%
2008	8.97%
2007	9.02%
2006	9.21%
2005	9.43%
2004	9.48%
2003	9.57%
2002	9.49%
2001	9.51%
2000	9.54%

Source: Aaron O’Neill, [statista.com/statistics](https://www.statista.com/statistics).

The acute shortage of legitimate employment opportunities in Nigeria seems to be a major factor that pushes the youths into various forms of crime, including cybercrime, as they cannot afford to idle away their lives in abject poverty even when qualified for various employment opportunities. Poverty is another major factor that pushes Nigerian youth involvement in cybercrime. The poverty level across the country is so high that a 2007 UNDP survey on poverty and extreme deprivation of 108 countries ranked Nigeria at the 80th position, giving it a Human Poverty Index of 37.3 among the lowest for the entire continent (Bello, 2018:40). Poverty ratio in Nigeria as at 2017 indicates that about one third of Nigerians (35%) live in

extreme poverty while about 54% are relatively poor; which means more than half of the Nigerian population lives on less than a dollar a day (Adebayo, 2013:357). In 2018, another study by Jolaosho (1996:31) revealed that about 50% of Nigerians live in extreme poverty. As of the year, 2020, Nigeria's poverty index rose exponentially leading to Nigeria being nicknamed the poverty capital of the world.

Besides issues of unemployment and poverty, failed leadership has also been identified as another important factor that contributed to the proliferation of cybercrime among many Nigerian youth. According to Akande and Shadare (2020:33) “failed leadership, unemployment, and poverty are the major factors driving yahoo-yahoo in Nigeria.” Contrary to the argument in support of youth unemployment, poverty, and failed leadership as key factors driving the majority of Nigerian youths into cybercrime, Muktar Bello (2018:155) argues strongly that the major cause of cybercrime in Nigeria is the irrepressible desire for ill-gotten wealth.

His argument suggests that some cybercriminals were neither jobless nor poor in the first instance but joined cybercrime out of greed for more wealth. Similarly, cyber victimization has been argued to be a result of abuse of individual frailties such as greed, gullibility, and the uncontrollable desire for getting rich syndrome and not crimes that are inevitably influenced by social factors such as poverty and unemployment (Adesulu 2017). Furthermore, cybercrime occurs not because of a lack of a decent means of livelihood but a lack of contentment and a desperate longing for quick money through illegal means (Jacinta, 2017).

Scholars have also attributed cybercrime activities among many Nigerian youths to the Internet Revolution. Thinking in this direction, Devine is of the view that what propelled cybercrime in Nigeria to such a huge booming industry was the dawn of the internet. In the same view, Folashade and Abimbola (2013:76) suggest that the surge could be linked to the increasing availability of broadband connections consequent upon the introduction of mobile telecommunications and reduction in subscription fees. They argue that integration of the internet into every aspect of our socio-economic lives ranging from electronic banking, electronic commerce, and electronic education to electronic governance has resulted in new forms of cybercrimes as computer technology grew to a stage where data began to move from one computer to another over networks and eventually other forms of online communication outside regular computers. Numerous factors have been advanced on why the majority of Nigerian youths’ venture into cybercrime. However, having examined the major ones, it is pertinent, on the other hand, to investigate the Nigerian government's efforts, over the years, towards preventing its increasing rate in the country.

### **War against Cybercrime: Nigerian Government Efforts**

The Nigerian government, during the period under review, adopted a series of measures, including the enactment of anti-cybercrime laws and the establishment of law enforcement agencies targeted at regulating cyberspace activities, prevention of cybercrime, and arrest and prosecution of cybercrime law offenders. To

this end, the Nigerian government, in 2004 established the Nigerian Cybercrime Working Group (NCWG) for the sole purpose of developing appropriate legal and institutional frameworks. The NCWG is an inter-agency consisting of the most relevant law enforcement, security, intelligence, ICT agencies of government and major private organizations in the ICT sector. Some of these agencies include the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF), National Security Advisor (NSA), Nigerian Communication Agency (NCC), Internet Service Providers' Association of Nigeria (ISPAN), Nigeria Computer Society (NCS), Department of State Services (DSS), National Intelligence Agency (NIA), Nigeria Internet Group (NIG), National Information Technology Development Agency (NITDA) and individual citizens representing public interest.

Specifically, NCWG was established to engage in public enlightenment programmes, build institutional consensus amongst existing agencies, provide technical assistance to the National Assembly on cybercrime and the drafting of the Cybercrime Act, create the framework for a cybercrime agency that will eventually emerge to take charge in tackling cybercrime in Nigeria, collaborate with global cybercrime enforcement agencies in the USA, UK, and other countries who are at the forefront of fighting cybercrime (Bello, 2018:47).

Following the recommendation of NCWG, the National Assembly passed legislation establishing the Economic and Financial Crimes Commission (Establishment) Act, 2004. By this Act, EFCC was legally empowered to serve as Nigeria's designated Financial Intelligence Unit (NFIU) charged with the responsibility of preventing, investigating, prosecuting, and penalizing financial and economic crimes such as illegal oil bunkering, terrorism, capital market fraud, cybercrime, Advance Fee Fraud (419), banking fraud and economic governance fraud (Obuah, 2010:56). According to the EFCC Act, 2004, section 6b, part 2, the commission, is also obligated, among other functions to, 'investigate money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, and contract scam.

In 2006, in an attempt to strengthen the war against cybercrime in Nigeria, another legislation of the National Assembly established the Advance Fee Fraud and Other Related Offences Act, 2006. The Act criminalizes certain cyber and other related crimes as contained in section 1, subsections 1, 2, and 3 which states:

1. Notwithstanding anything contained in any enactment or law, any person who by any false pretence, and with intent to defraud;
  - a. Obtains from any other person, in Nigeria or any other country for himself or any other person;

- b. Induces any other person, in Nigeria or in any other country, to deliver to any person; or
  - c. Obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretense, commits an offence under this Act.
2. A person who by false pretence, and to defraud induces any other person, in Nigeria or any other country, to confer a benefit on him or any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act.
  3. A person who commits an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not more than 20 years and not less than seven years without the option of a fine (Nwosu, 2018:16).

Additionally, in 2015, a seemingly more proactive, effective, and specific law was passed to nib in the bud the proliferation of cybercrime and its adverse consequences in the country and that was the Cybercrime Act, 2015. The objectives of the Act as provided in Section 1 thereof include:

To provide an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; ensure the protection of critical national information infrastructure; and promote cyber security and the protection of computer systems and networks, electronic communications, data, and computer programs, as well as intellectual property and privacy rights (Nwosu, 2018:17).

Specifically, the Act prescribes:

1. A death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that results in the death of an individual.
2. That hacker, if found guilty of unlawfully accessing a computer system or network, is liable to a fine of up to N10 million or a term of imprisonment of 5 years. The same punishment goes for Internet fraudsters who perpetrate their acts either by sending electronic messages or accessing and using data stored on computer systems.
3. Punishment for identity theft which is imprisonment for a term of not less than 3 years or a fine of not less than N7 Million or both.
4. Punishment for child pornography is imprisonment for a term of 10 years or a fine of not less than N20 Million or both as the circumstances warrant.
5. Punishment for cyber-stalking and cyber-bullying for 1-10 years and/ or a fine of N2-N25 Million or both, as the case may be.

6. Punishment for cyber-squatting upon conviction with a minimum of 2 years imprisonment or a fine of not less than N5 Million or both (Nwosu, 2018:14).

Besides the foregoing legislative and policy approaches adopted by the Federal Government of Nigeria to curb cybercrime, certain agencies were also empowered to enforce their compliance and punishment of the defaulters. Some of these agencies that have played diverse roles in achieving a cybercrime-free Nigeria include the Nigeria Police Force (NPF), Nigerian Communication Agency (NCC), Internet Service Providers' Association of Nigeria (ISPAN), Nigeria Computer Society (NCS), Department of State Services (DSS), National Intelligence Agency (NIA), Nigeria Internet Group (NIG), National Information Technology Development Agency (NITDA), among others.

Evidence suggests that the above government efforts have yielded some level of success in tackling the upsurge of cybercrime across Nigeria. For instance, between 2003 and 2007, the Nigerian government through the EFCC, stopped cybercrime transactions worth £300 million, €200 million, and \$500 million respectively (Ribadu, 2007). A considerable number of youths have also been arrested, prosecuted, convicted, and punished appropriately over several cybercrime and other related activities. Consequently, while some of these criminals have lost their lives, others were confined in jails across the country.

Despite the above efforts of the Nigerian government to control and eradicate cybercrime and its effects on the people and economy of Nigeria, the trend seems to have continued to thrive among the youths.

### **Nigerian Government and Promotion of Cybercrime among the Youths**

Although the Nigerian government has expended so much human, material, and financial resources on fighting cybercrime in the country during the period of this investigation, the menace seems unabated. Individuals, institutions, corporate organizations, and even foreign investors have continued to lose huge amounts of money and other valuables to cybercriminals. Surprisingly, it appears that it is the government itself that is waging the war against cybercrime that has equally been promoting its increase among the Nigerian youths through her failure to create certain socio-economic and political conditions that could make cybercrime difficult to thrive. Ironically, this has occurred through the same measures she had attempted to control and prevent as well as punishment for the perpetrators. As a result, the menace has become widespread (Maitanmi, 2013:49), to the extent that every nine seconds, a Nigerian commits a crime on the internet (Saulawa, & Abubakar, 2014). Again, because of the prevalence, according to the Internet Crime Complaint Centre, a partnership between the Federal Bureau of Investigation (FBI) and America's National White Collar Crime Centre, Nigeria has been ranked third among the list of top ten sources of cybercrime globally (Maitanmi, 2013:49). In the African region, Nigeria has also been ranked first as the target and origin of malicious cyber activities (Jackson & Robert, 2016:45).



The Nigerian government, while fighting cybercrime, seems to have indirectly contributed to its proliferation among the youths through its reluctance to create sufficient employment opportunities for the rapidly increasing number of unemployed persons. This disinclination has increased the unemployment rate in Nigeria. For instance, between 2000 and 2009, the rate rose exponentially to 142%. According to National Bureau of Statistics (2010) the growth rate was 13.1% in 2000, 13.6% in 2001, 12.6% in 2002, 14.8% in 2003, 13.4% in 2004, 11.9% in 2005, 13.7% in 2006, 14.6% in 2007, 14.9% in 2008, and 19.4% in 2009. As of March 2009, unemployed persons within the age bracket of 15 and 24 were 41.6% while those between 25 and 44 years were 17% (National Bureau of Statistics, 2010). It is important to note that a greater number of unemployed persons in these age brackets are youths. Although the unemployment rate, generally, has been on the increase across Nigeria annually that of the youths in particular has been the worst. For instance, by the fourth quarter of 2018, while the unemployment rate across Nigeria stood at 23.1%, that of the youths alone was above 47% (Nwosu, 2018:36). Similarly, in 2020, the general unemployment rate in Nigeria was 33.3% whereas youth unemployment rate was 53.40% (National Bureau of Statistics, 2020).

Even though it is not the exclusive responsibility of the Nigerian government to employ all her citizens; she owes her citizens, especially, the youths the statutory responsibility for their gainful and productive engagement as well as the creation of conducive environments for businesses to flourish. On the other hand, while every capable person anywhere in the world is expected to consider self-employment or even job creation for others to assuage the impact of joblessness, certain militating factors beyond their control seem to either discourage these prospective entrepreneurs or severely hinder the progress of those who have started already. The figures above, to a large extent, reveal the Nigerian government's negligence to her primary responsibilities of not just job creation, but failure to avail the people of such opportunities and conditions necessary for any legitimate and gainful engagement to thrive. The inability of the Nigerian government to proactively and timely create employment opportunities and enabling socio-economic and political atmosphere for the youths has indirectly promoted the proliferation of cybercrime among this class of persons in the country.

The relatively adverse socio-economic and political conditions, insecurity, and inadequate financial and material support from the government to the few existing manufacturing companies in Nigeria have further exacerbated the unemployment issue, especially among the youths, and this has grossly encouraged them to find solace in cybercrime. For example, as reported by the United Nations Development Programme (UNDP) survey, in 2009, due to a lack of government-supportive financial and policy measures, more than 837 factories collapsed and closed shops while about half of the remaining operating firms were classified as ailing (Okafor, 2011:362). Aggregating the data of the collapsed factories, the survey reveals that:

...in 2009, a total number of 176 firms became terminally ill and collapsed in the Northern area, comprising the Kano and Kaduna manufacturing axis. In the southeast area, which comprises Anambra, Enugu, Imo, and Abia states, a total number of 178 companies closed shops during the period, while in the South-south area, which comprises Rivers, Cross River and Akwa Ibom states, 46 companies shut down operations before December 2009; the Southwest area, which comprises Oyo, Ogun, Osun, Ondo, Ekiti, Kogi, and Kwara states, lost 225 companies during the year; Lagos area covering Ikeja, Apapa, Ikorodu, and other industrial divisions in the state followed closely with 214 manufacturing firms closing before the end of 2009 (Maiyak, 2010:38).

It appears that corruption has also made worse the foregoing socio-economic reality in Nigeria. Corruption among Nigeria's political leaders, civil servants, public workers, and others seems to have made it extremely difficult for the unemployed youths to have access to employment opportunities except for the few that could submit to their tainted whims and caprices. Corruption in Nigeria is regrettably overwhelming to the extent that the country was reported to have scored 25% and ranked 149 in the list of countries surveyed by the Corruption Perception Index in 2020.

As noted earlier, although the Nigerian government, through a legislative mechanism, had made and enforced certain anti-cybercrime laws in an attempt to control and prevent the upsurge of cybercrime in the country, the same government, through the enactment of weak laws, poor enforcement of those laws and deficit supply of enforcement personnel, has encouraged the proliferation of cybercrime among many of the Nigerian youths. In other words, as Nwosu (2018:43) observes, cybercrime and its perpetrators in Nigeria and other developing countries are succeeding because laws against cybercrimes are usually weak while the enforcement agencies are either not enough or incompetent. Thus, even with legislation on cybercrimes, the provisions of the existing laws are not comprehensively strict enough to daunt cybercriminals from their criminal acts. Faulting the Criminal Code, of 2006 in this regard, Nwosu (2018:12) further argues that, the maximum punishment of seven years and a minimum of three years prescribed by the Criminal Code is, to say the least, inadequate as it does not reflect the reality of the situation given the gravity of the offence of cybercrime and the enormity of property involved in most instances, and as a result could not serve as a deterrent to offenders.

Even though the cybercrime law enforcement agencies have contributed a reasonable quota in fighting cybercrime in Nigeria, their low staff strength has also been found responsible for its promotion among many youths. A case in point is the Nigerian Police Force, a principal law enforcement agency in Nigeria, with a staff strength of about 371,800 (Bello, 2018:17). Not only that their limited staff strength makes it difficult for effective and efficient policing of lawbreakers, they have also served as accomplices and informants to the cybercriminals (Bello, 2018:17). However, rather than blame the police officer collaborators for their corrupt attitude, Akande and Shadare (2020:39) observed that public opinion tends

to blame the Nigerian government. Their opinion suggests that these official partners in crime's attitudes are a sequence of corruption that begins with the government that refused to remunerate them satisfactorily thereby leaving them hungry and desperate; compelling them to turn to Yahoo Boy hunters for their daily bread. The limited resources, skills, and motivation problems that are rampant within the force have also been blamed on the Nigerian government due to its inability to fund the agency adequately to achieve all tasks before it.

Again, a closer examination of the various acts that criminalize cybercrime and fraud in Nigeria reveals the existence of some areas of ambiguities in terms of definitions and limits of the law enforcement agencies in the discharge of their responsibilities as well as their points of cooperation. This lack of uniformity among the various legislations has created more confusion in the legal system especially with particular reference to punishment as they all have different prescriptions for violation of each of the laws. Besides, in most instances, there have been serious misunderstandings as to which agency or institution has the authority to investigate and prosecute cybercrime law offenders. Consequently, there have been rivalry and conflict between and among officers of the Nigerian Police, Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices and Related Offences Commission (ICPC), and others (Nwosu, 2018:13). Moreover, even within agencies engaged in the investigation of cybercrime in Nigeria, there appears to be lack of cooperation among the investigative, legal and forensic departments in conducting a thorough and evidence-based investigation. These factors, among others, have made investigating cybercrime cumbersome. The continuous increase in the number of youths engaging in cybercrimes daily and the dearth of their proportionate arrest, prosecution, conviction, and punishment by the judiciary and law enforcement bodies largely shows the extent of the government's insufficient efforts in tackling activities of cybercriminals through legislation and law enforcement personnel. Another means through which the Nigerian government appears to have contributed to the promotion of cybercrime among the youths has been its lackadaisical attitude to ensuring adequate, functional, effective, and efficient cyber security measures in Nigeria's cyberspace. Cyber security in Nigeria is so porous that many of the Nigerian youths find it easy to successfully manipulate the system for their nefarious activities. The frequency this happens is quite regular that a South Africa-based Institute of Digital Communications (IDC), a market research and forecasting firm had remarked that, 'in Nigeria, organizations are busy adopting information technologies without commensurate investment in information security.

## **Conclusion**

The study examines how the actions and inactions of the government promote and sustain cybercrime among Nigerian youth. It argues that even though the Nigerian government has expended so much human, material, and financial resources on fighting cybercrime in the country during the period under review, the

menace seems unabated as Individuals, institutions, corporate organizations, and even foreign investors have continued to lose huge amounts of money and other valuables to cybercriminals. One major way the government has contributed to the menace of cybercrime in Nigeria is through its failure to create socio-economic and political conditions that would make cybercrime difficult to thrive. Similarly, the inability of the Nigerian government to proactively and timely create employment opportunities and enable a socio-economic and political atmosphere for the youths has indirectly promoted the proliferation of cybercrime among this class of persons in the country. Sadly, the relatively adverse socio-economic and political conditions, insecurity, and inadequate financial and material support from the government to the few existing manufacturing companies in Nigeria have further exacerbated the unemployment issue, especially among the youths, and this has grossly encouraged them to find solace in cybercrime. It appears that corruption has also made worse the foregoing socio-economic reality in Nigeria. Corruption among Nigeria's political leaders, civil servants, public workers, and others seems to have made it extremely difficult for the unemployed youths to have access to employment opportunities except for the few that could submit to their tainted whims and caprices. Although the Nigerian government, through a legislative mechanism, had made and enforced certain anti-cybercrime laws in an attempt to control and prevent the upsurge of cybercrime in the country; these laws and their enforcement are, however, weak; the agencies of government established to fight against cybercrimes in the country are constrained by several factors which militates against their effectiveness. Sadly, some members of these agencies are accomplices to the very crimes they were meant to fight. Until these issues are addressed, the fight against cybercrime and cybercriminals will rather remain elusive

## References

- Adebayo, A. A. (2013). Youths' unemployment and crime in Nigeria: A nexus and implications for national development. *International Journal of Sociology and Anthropology*, 5(8), pp350-357
- Akanle, O. & Shadare, B. R. (2020). Why has it been so difficult to counteract cybercrime in Nigeria? Evidence from an ethnological study. *International Journal of Cyber Criminology*, 14(1), pp.27-43
- Adesulu, D. (2017). Greed, cause of cybercrime. *Vanguard News*, Retrieved 20/3/2022, <https://www.vanguardngr.com/2017/06/greed-cause-cybercrime-don/>
- Ajayi, E. F. G. (2016). Challenges to enforcement of cybercrimes laws and policy. *Journal of Internet and Information Systems*, 6 (1), pp.1-12
- Clarke, R. V. (2004). Technology, criminology and crime science. *European Journal on Criminal Policy and Research*, 10, pp.55-63
- Devine, J. "History of 419 Fraud. file:///c:/Users/jegede/documents/thehistoryof419internetfraud.htm . Internet Ezine Articles
- Economic and Financial Crimes Commission (EFCC). (2015). *Red Alert on Scams*. Abuja: Sidwell Productions.

- Folashade, B. O. & Abimbola, K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), pp.98-114
- Jackson T. C. B. & Robert, W. Ene (2016). Cybercrime and the challenges of socio-economic development in Nigeria. *JORIND*14(2), pp42-48
- Institute of Digital Communications. (August, 2013). *Newsletter*:
- Jolaosho, A. (1996). Some popular perceptions of poverty in Nigeria. UNDP Human Development Report on Nigeria.
- Jacinta, O. J. (2017). 'The rapid growth of internet fraud in Nigeria, causes, effect and solution', <https://innertempleoou.wordpress.com/2017/03/07/the-rapid-growth-of-internet-fraud-in-nigeria-cause-effect-and-solution-by-nweke-oluchi-jacinta/> Accessed 20/3/2022.
- McQuade, S. C. (2006). *Understanding and Managing Cybercrime*. Allyn and Bacon.
- Mohammed, K. Mohammed, Y. & Solanke, A. (2019). Cybercrime and digital forensics: Bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria. *International Journal of Cyber Security Intelligence and Cybercrime*, 2(1), pp.56-63
- Mukhtar Bello. (2018). Investigating cybercriminals in Nigeria: A comparative study (Unpublished Ph.D. Thesis) Salford Business School College of Business and Law University of Salford, UK.
- Musari, A. (March 19, 2009). Youth and the national youth employment action plan, Abuja. *Guardian Newspapers*.
- Maitanmi, O. *et al*, (2013). Impact of cybercrimes on Nigerian economy. *The International Journal of Engineering & Science (IJES)*, 2(4), pp.45-51
- Maiyak, U. (26 July, 2010). Implications of the U.S. energy independence policy to Nigeria: A Revised Edition, *Guardian Newspaper*
- Nwosu, U. W. (2018). Cybercrime and Nigeria's receding economy: The role of the legal system," in *Public Policy, National Security and Economic Development*. Advance International Publisher.
- National Bureau of Statistics. (2010). *Statistical News Labour Force Statistics* No. 476. Abuja: The NBS Publication
- National Bureau of Statistics. (2020). Labour Force Statistics: Unemployment and Underemployment Report, Abridged under COVID 19, Q2, 2020, [https://www.nigerianstat.gov.ng/pdfuploads/Q2\\_2020\\_Unemployment\\_Report.pdf](https://www.nigerianstat.gov.ng/pdfuploads/Q2_2020_Unemployment_Report.pdf)
- Olivia, O. E. (2022). Examining the effect of the elevated rate of cybercrime on the growth and sustainable development of Nigeria's economy. *Nnamdi Azikiwe University, Awka Journal of Commercial and Property Law*, 9(1), pp.32-43
- Okafor, E. E. (2011). Youth unemployment and implication for stability of democracy in Nigeria. *Journal of Sustainable Development Africa*, 13(1), pp.358-373
- Obuah, E. (2010). Combatting corruption in Nigeria: The Nigerian Economic and Financial Crimes Commission (EFCC). *African Studies Quarterly*, 12(1), pp.17-44
- Ribadu, V. (9th – 12th July, 2007). Cybercrime and commercial fraud: A Nigerian perspective. A Paper Presented at the Modern Law for Global Commerce, Vienna
- Saulawa, M. A. & Abubakar, M. K. (2014). Cybercrime in Nigeria: An overview of Cybercrime Act 2013. *Journal of Law, Policy and Globalization*, 34, pp.23-33

Shehu, A. Y. (2014). Emerging issues in cyber-crime: causes, implications and effects for the legal profession. *Online Journal of Social Sciences Research*, 3(7), pp.169-180

Ude, N. (March 31st, 2015). Financial institutions and the challenges of cybercrime, *The Guardian Newspaper*.