



CONTEMPORARY ISSUES IN SOCIOLOGY AND SOCIAL WORK

AN AFRICANIST PERSPECTIVE

Edited by

Ali A. Abdullahi, Ph.D. & Emmanuel M. Ajala, Ph.D.

CONTENTS

<i>Acknowledgements</i>	viii
<i>Foreword</i>	ix
<i>Notes on Contributors</i>	xii

SECTION I

CORE SOCIOLOGY

1. Foundation of Sociology <i>Ali A. Abdullahi & Moshood Issah</i>	I
2. Contemporary Sociological Theories: An Africanist View <i>Olayinka Akanle & Okewumi O. Ewajesu</i>	27
3. Sociology of Social Problems: An Introduction <i>Jimoh Amzat & Ahmed A. Magaji</i>	45
4. Contemporary Issues in Gender Studies <i>Oluwatobi J. Alabi</i>	61
5. The Sociology of Formal Organisations <i>Bashir Bello</i>	80
6. Foundation of Development Sociology <i>Olayinka Akanle & Gbenga Adejare</i>	98
7. Scope and Trends in Urban Sociology <i>Usman Abubakar & Okoro P. Mmahi</i>	116
8. Basic Discourse in Rural Sociology <i>Saheed A. Lawal</i>	139
9. Crime, Deviance and Social Control <i>Abdullahi K. Ibrahim & Monsurat Isiaka</i>	153

10.	Cybercrime and Criminality <i>Abdullahi K. Ibrahim</i>	177
11.	Issues in Medical Sociology <i>Olufunke O. Adegoke. & Victor I. Kolo</i>	199
12.	Discourses in Social Epidemiology <i>Kamorudeen Adegboyega</i>	220
13.	Social Epidemiology of Mental Illness <i>Kabiru K. Salami</i>	237
14.	Basic Issues in Comparative Health Care Systems <i>Jimoh Amzat & Victor I. Kolo</i>	257
15.	Issues in Social Gerontology <i>Kafayat Mahmoud</i>	278
16.	The Nexus between Politics and Sociology <i>Luqman Saka & Rafiu A. Bakare</i>	296
17.	Social Differentiation, Social Inequality and Social Stratification <i>Abdul-Ganiy Olatunji</i>	314
18.	Industrial Sociology in Africa <i>Akeem A. Akinwale</i>	334
19.	Afrocentric Social Thought: Rethinking Sociology in Africa <i>Issah Moshood & Ali A. Abdullahi</i>	353

SECTION II

CORE SOCIAL WORK

20.	Foundation of Social Work <i>Mohammed S. Yusuf, Abdussalam Abdulhmeed & Daniel D. Oladeinde</i>	375
-----	--	-----

21.	The Fundamentals of School Social Work <i>Angela I. Ogbu</i>	398
22.	Social Security Systems: The Concept, Typology and Classifications <i>Fariudeen O. Liadi</i>	413
23.	Forensic Psychology: Theory and Application <i>Rotimi Oguntayo & Helen O. Osinowo</i>	432
24.	Industrial Social Work: An Introduction <i>Emmanuel M. Ajala</i>	452
25.	The Dynamics of Human Social Functioning <i>Isaiah M. Ojedokun</i>	469
26.	Social Workers and the Military <i>Daniel D. Oladeinde & Johnson T. Oyeleke</i>	486
27.	Social Workers and Mental Health <i>Karamat A. Kelani</i>	503
28.	Community Organisation and Rural Development <i>Abdullateef Raji & Ibrahim O. Adeshina</i>	523
29.	Social Workers and Community Development <i>Abdussalam Abdulhameed</i>	541
30.	Social Workers and Child Protective Services <i>Abdulganiyu H. Mohammed, & Olufemi A. Fawole</i>	555
31.	Social Workers in the Hospital Settings <i>Abdul-Lateef B. Adeoti</i>	571
32.	The Concept Of Human Sexuality: Implications For Social Work <i>Isaiah M. Ojedokun</i>	587
33.	Social Workers in Global Terrorism <i>Bolanle Oriola</i>	607

SECTION III

SOCIOLOGY AND SOCIAL WORK

34.	The Domains of Sociology and Social Work <i>Mohammed S. Yusuf</i>	620
35.	Research Methods in Social Work and Sociology <i>Emmanuel M. Ajala</i>	641
36.	Statistical Reasoning in Sociology and Social Work <i>Anthony I. Ajayi</i>	665
37.	Psychology of Adolescence <i>Abiola O. Popoola & Babatunde O. Popoola</i>	678
38.	Socio-Cultural Context of Disease and Illness <i>Joseph S. Owoseni</i>	692
39.	Social Workers and Rural Development <i>Musediq O. Lawal & Sunday Akor</i>	704
	Index	721

CHAPTER TEN

CYBERCRIME AND CRIMINALITY

Abdullahi K. Ibrahim

Criminology is an interesting area of specialisation that is interested in understanding the dynamics of crime and criminality in human society. It investigates, largely, the social factors that propel crime and criminality with a view to finding solutions. Meanwhile, Criminology has always been housed in the Department of Sociology, not only in Nigeria but across the world. This is because it has always been seen as a variant or strand of Sociology. In recent times, however, some universities, especially in Nigeria, are beginning to mount Criminology as a distinct department, sometimes independent of the Department of Sociology. A good example is the University of Ilorin, Nigeria, which carved out the Department of Criminology and Security Studies from the Department of Sociology. Nevertheless, Criminology and Security Studies can still not survive without inputs from Sociology.

Cybercrime and criminality are emerging areas of interest in Criminology. This is because, lately, information, communication and technology (ICT) has become a vast growing aspect of civilisation. The Internet, especially, is an aspect of information technology that enables us to communicate with one another globally, irrespective of the country and the continent, within a short time (Clough, 2010). Modern technology and the Internet have unified many countries of the world (Zero Tolerance, 2006). The digital technology has become an open channel through which information and resources can be tapped and transferred throughout the world (Nzeako, 1999). However, one of the demerits of the unlimited access to the Internet is the issue of cybercrime and criminality. In Africa and indeed the world, the positive impacts of the Internet on socio-economic development have been hampered, as the Internet has become an avenue for criminal activities. The obscure identity of the Internet crime perpetrators has been attributed to the high level of cybercrimes in a country like Nigeria (Hasan, Rahman, Abdillahi & Omar, 2015; Matanmi, Ogunlere, Ayinde & Adekunle, 2013).

In recent times, cybercrime and criminality in Africa have attracted the attention of policy makers, law enforcement agencies and researchers, hence, efforts are being geared towards combating cyber criminality. Nigeria is a good example of a

country in Africa that is taking the fight against cybercrimes very seriously, perhaps because it ranks high in global ranking. A number of laws have been promulgated to fight against cybercrimes. Among these are:

- The National Drug Law Enforcement Agency (NDLEA) Act No. 48 of 1989 which was to confront the menace of money laundering in compliance with the Vienna Convention;
- The Failed Bank (Recovery of Debt and Financial Malpractice in Banks) Act No. 18 of 1994 which was promulgated to check the cases of money laundering and insider abuses by bank officials in the country (CBN, 2003);
- The Money Laundering Act of 1995; the Advanced Fee fraud (419) Act of 1995; and the comprehensive amendments of the Banks and Other Financial Institutions Act (BOFIA) and the Central Bank of Nigeria Act of 2002.
- The Anti-Corruption Act of 1999, which established the Independent and Corrupt Practices and Other Related Offenses Commission (ICPC) (Ezeoha, 2006) and
- The Economic and Financial Crime Commission (EFCC).

However, as at the time the EFCC and the ICPC laws were enacted, most of their activities did not cover cybercrime. However, the good thing is that in recent times, most of these institutions are beginning to expand their scope to equally capture cyber criminality in Nigeria. Aside from the EFCC and ICPC, the Nigeria Police Force is equally a playing pivotal role in curbing cybercrimes in Nigeria. However, despite the efforts against cybercrime and criminality, they have continued unabated in Nigeria. In this chapter, contemporary issues around cybercrime and criminality, including why people engage in cybercrime are discussed.

CONCEPTUAL CLARIFICATION

In this section, some concepts that are important to this chapter are clarified. These concepts include cybercriminals, computer virus and cybercrime.

Cybercrime

Cybercrime is a worldwide problem. It is not peculiar to any particular region or nation. It is a global social phenomenon which has raised global concern. These types of crimes are crimes perpetrated using the social networks and computers (Oumarou, 2007; Plot, 2010; Shinder, 2002). They are also crimes or offences committed against people with the intention of influencing physical or mental

harm using technology. Such crimes may threaten a nation's security and its financial health (Akogwu, 2012). Another way to describe cybercrime is to view it as a criminal act committed mostly via the cyberspace, which has a physical component and is simply facilitated through the use of Internet-based tools (Saul, 2007). Innovations in technology opened up the opportunity for these types of crime (Oumarou, 2007). According to Obiri-Yeboah (2015, p. 20), cybercrimes are:

offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice boards and groups) and mobile phones.

- **Cybercriminal**

Who is a cybercriminal? In simple language, anyone who engages in cyber criminality with the intent to defraud is a cybercriminal. In other words, cybercriminals are individuals or groups who perpetrate cybercrime and are usually called either computer hackers, pranksters or crackers (Nykodym, Taylor & Vilela, 2005; Chawki, 2009; Boateng, Longe, Mbarika, Avevor & Isabalija, 2010). Smith, Grabosky & Urbas (2004) describe cybercriminals as those criminals who operate on the cyberspace. Ludwig and Noah (2017) see a cybercriminal as a person who tampers with the internet or network in order to defraud. To Tade (2013, p. 689), cybercriminals are "those who explore the internet and pervert it for criminal opportunities". Most of the cybercriminals in any part of the world are usually young people and the majority of them can be found in tertiary institutions. Onifade & Mohammed (2000, p. 25) have categorised cybercriminals into: (i) Serious Minded; and (ii) Pranksters.

Onifade & Mohammed (2000) opined that a serious minded computer criminal on the one hand is very curious; he tends to be relatively honest, working in a trustworthy position; bright, highly motivated, most often, male, between 18 and 30 years of age and would not cause any physical harm to another human being; they usually have a purpose other than showing off. Pranksters, on the other hand, are usually computer hackers. A hacker is a dedicated person who enjoys learning the intricate details of computer systems and dedicates many computer hours to it. He deploys computer virus as a tool in crippling computers protected by passwords. Some experts refer to hackers as crackers. Nykodym et al., (2005) describe a cracker as a person who enjoys breaking computer codes either in cyberspace or breaking into computers illegally; he/she is very good at

computer programming. The most common hacking pathway is accessing and trapping signals in cyberspace. Using the right kind of equipment, the hacker generally, traps signals in space by decrypting the encrypted codes of data (Chawki, 2009). According to Onifade & Mohammed (2000) the hackers can be further subdivided into external and internal hackers. An external hacker gains access to the target computer from a remote computer located outside the target computer. The most common tools used in this case are the internet and satellites link. An external hacker is usually an employee, a contractor or a consultant employed by a firm.

- **Computer Virus**

Onifade & Mohammed (2000, p. 56) define computer virus as “a small programme that impairs or simply destroys a computer's ability to function properly”. Virus or viruses are often programmed to spread themselves via the Internet. Cybercriminals may employ strategies such as masquerading in the form of games and pictures and using tricky subject lines mainly to incite the computer user to run them. The result is that the computer begins to malfunction. More often than not, hackers make use of viruses to create holes in a computer network's security system. These holes are then used to access the network. It should be stressed that computer viruses often affect computer network.

CYBER CRIMES IN AFRICA

Although cybercrime is not peculiar to Africa, it is one of the regions mostly affected by this type of crime. According to a report from the Institute of Security Studies in 2014, the number of targeted cyber attacks in Africa had increased by 42% from the previous years (Mark, 2018). The reports further revealed that hundreds of millions of cyber attacks take place every year in Africa, where South Africa, Nigeria and Kenya are heavily affected (Mark, 2018). According to a report from the Shadow Market (2012), not less than twelve countries in Africa have had their IT infrastructure infected. They include Libya (98%), Zimbabwe (92%), Algeria (84%), Cameroon (83%), Nigeria (82%), Ivory Coast (81%), Kenya (78%), Senegal (78%), Tunisia (74%), Morocco (66%) and Mauritius (57%). Essentially, in Africa, cybercriminals are called different names. For instance, they are called *yahoo yahoo* boys in Nigeria (Tade & Aliyu, 2011). In Ghana, they are called *Sakawa* (Coosom, 2009 cited in Obiri-Yeboah, 2015) and in Cameroon, they are called *Faymania* (Oumarou, 2007). While the Internet has contributed immensely to the development of Africa and has impacted positively on every sphere of life, the educational, banking and e-

commerce sectors have had their share of the effect of cybercrimes. Specifically, in Nigeria, cybercrime has become one of the main avenues for pilfering, hacking and business espionage. Ewepu (2016) noted that in 2016, Nigeria was one of the highly ranked countries in cyber-attack vulnerabilities in Africa.

Obiri-Yeboah (2015) has observed that cybercrime and the indiscriminate use of the Internet have become a hiding place for criminals who have moved from the streets to an electronic platform. Similarly, Asokhia (2010) asserted that cybercrime is a replica of advance-fee-fraud which became popular in the early 1990s in Nigeria. The crime has advanced to what is commonly known as "YAHOO PLUS" (Tade & Aliyu, 2011). Alemika (2007) noted that in Nigeria today, cybercrime is deeply rooted in the society, and seems to have been accepted by the same society. Most modern songs, modern dresses, dance steps and other activities in the society are tailored towards giving the 'yahoo-yahoo' a platform to continue to succeed (Alemika 2007). It is a common belief today that most young boys and girls are being called *yahoo* or *yahoo-plus* because a sizeable number of them are young people and they adopt different strategies in using the Internet to commit different types of crime; they are mostly students in Nigerian tertiary institutions (Olaide & Adewole 2004). For Okeshola & Adeta (2013), cybercriminals are mostly young people, usually, males within the age range of 18 and 30 years and are mostly out of school youth. A study by Youth against Cybercrimes and Fraud in Nigeria (2008) shows that majority of youths are involved in these nefarious activities in most cities in Nigeria. Those interviewed by this organisation attributed their involvement to poverty or to the belief that all Nigerians are corrupt. Perpetrators of this act live with each other, move together, drive in the same car and attend the same parties. Adeniran (2008) submitted that there is a sort of synergy between them and this relationship, like every other group, must be governed by certain rules, folkways and norms. Government had made several attempts to mitigate the scourge of cybercrime in Nigeria but all efforts proved futile owing to the fact that the identities of the perpetrators remain unknown (Oludayo, 2011; Adeniran, 2011). Table 1 ranks Nigeria in global cybercrimes. According to the table, up until 2013, Nigeria was ranked first in Africa in cyber-criminality. Also according to the table, Nigeria was among the first ten in global ranking between 2002 and 2014. Table 2 showcases cases of cybercrimes filed and prosecuted in Nigeria. From the table, between 2010 and 2014, out of the 740 cases reported, 196 convictions were recorded with, 544 pending cases.

Table 1: Nigeria's ranking in Global Cybercrime (2002-2014)

YEAR	GLOBAL RANKING	AFRICA RANKING
2002	Second (2 nd)	First (1 st)
2003	Third (3 rd)	First (1 st)
2004	Third (3 rd)	First (1 st)
2005	Second(2 nd)	First (1 st)
2006	Third (3 rd)	First (1 st)
2007	Third (3 rd)	First (1 st)
2008	Third (3 rd)	First (1 st)
2009	Third (3 rd)	First (1 st)
2010	Third (3 rd)	First (1 st)
2011	Not ranked among top ten	-
2012	Twenty fifth(25 th)	First (1 st)
2013	Third (3 rd)	First (1 st)
2014	Twenty fourth	Second(2 nd)

Source: Adapted from Oyenuga (2015, p. 10)

Table 2: Cybercrime cases filed, convictions and pending cases between 2010 – 2014

Year	Number of cases filed in court	Number of convictions recorded	Pending cases
2010	151	17	134
2011	200	38	162
2012	187	49	138
2013	96	33	63
2014	106	59	47
Total	740	196	544

Source: Cybercrime Report 2014 (Unpublished report)

IMPACT OF CYBERCRIMES AND CRIMINALITY

Some have focused on the positive impacts of cybercrimes and criminality and argue that cybercrime has taken many families out of poverty, brought prestige to the young millionaires, created job for some unemployed youths and beefed up the activities of the security agents in most endemic countries. However, when juxtaposed with the disservice cybercriminals have done to Nigeria, the

aforementioned benefits become so infinitesimal. With specific focus on Nigeria, the most common impacts of cyber-crimes are the following:

- **Soiled National Image**

Hansell (2007) submits that cybercrimes may threaten the financial health and national security of the affected countries. Salifu (2008) added that it can widen the digital divide, disrupt information infrastructure and affect consumer confidence in online transactions. A high incidence of cybercrimes might make some foreign investors lose interest in the country. Some potential investors may be scared and discouraged to get involved in online transactions. For example, some online companies have reportedly employed software that can red-flag or automatically reject online orders from Nigeria because of the rate of cyber fraud in the country (Hansen, 2002/2003). At international airports, immigration officers normally take their time to scrutinise Nigerians, waste their time and pelt them with embarrassing questions, the moment they reveal their identities.

- **Stifled Economic Development**

Online piracy and other cybercrimes have rendered a country like Nigeria's cyber space too risky for buying and selling. Nigeria loses more than 11 billion naira to software piracy every year (Ayatokun, 2006). The rate at which spam messages increases in Nigeria has become a big concern to Nigeria and the world at large because it overcrowds the Internet bandwidth and reduces its speed of operation. For instance, most organisations including government parastatals, cannot conduct online recruitments efficiently. Coupled with the issue of cyber-crimophobia that the international market has developed for Nigeria, we may continue to be limited to doing business, the crude way (manually).

- **Colossal Loss of Resources**

In 2008 alone, one trillion naira was lost to computer crime generally (Orunsolu et al., 2017). Similarly, in May 2011, Sony's play station came under attack and lost up to \$171 million (Voigt, 2011). Even businesses suffer great losses, both tangible and intangible, when attacked by hackers. In the U.S, victims of credit-card theft may be liable for the initial \$50 of fraudulent charges, but financial institutions bear the brunt (Goodman, 2002/2003). Many organisational victims of industrial or economic espionage have also lost sensitive information.

- **Undermined National Sovereignty**

Cybercrime has the tendency to undermine national sovereignty. By lending its weight to trans-border and other organised crimes, cybercrimes have undermined the sovereignty of Nigeria (Siegel, 2007). Several police and military systems across the globe including the so-called super powers have been

humbled by hackers. For instance in 2000, Ikenna Ifeih, a 20 year old Nigerian was convicted for hacking into the U.S Army's and NASA'S computers among other private targets (Ogunsaya, 2006; Bashir, 2011). The worst is that most of the attacks go undetected. According to Goodman (2002/2003), out of 38,000 attacks perpetrated against the U.S Department of Defense, between 1992 and 1995, only 4% of the successful attacks were detected. The Cable Network News (CNN) has reported an increase in the asymmetric attacks in which a small group of hackers does disproportionate damage to governments and large companies. Typical examples are those painful revelations by Wikileaks that punctured U.S's foreign policy. Often, spies do give away state secrets or security information for peanuts (Voigt, 2011).

TYOLOGY OF CYBERCRIMES

It is imperative to briefly discuss some of the typologies of cybercrimes. Cybercrimes are usually categorised into different forms. Brenner (2010) categorised cybercrimes into target cybercrimes, tool cybercrimes and computer incidental crimes. According to Brenner, target cybercrime mainly focuses on the computer as a target; tool cybercrime uses computer as a tool for perpetrating evil while incidental cybercrime allows the computer to play a role in the crime. A broader cybercrime classification has been provided by Dashora (2011). This is discussed below:

- **Cybercrimes against Persons**

When one uses the computer to harass and intimidate persons, it is called cybercrime against persons. A good example is e-mail phishing, which may include the distribution, posting and dissemination of offensive and unsolicited materials such as pornography and indecent exposure of persons. This form of cybercrime constitutes one of the most important cybercrimes known today. It adversely affects youths as it can leave psychological scars and injuries on the younger generation, if not controlled. A victim of cyber bullying may commit suicide to escape the embarrassment of watching a video of himself or herself in a homosexual display, which might have been sent online by some bullies in school (Kawalski, Cappelli & Moore, 2008).

- **Cybercrimes against Property**

This type of cybercrime usually involves crime against property. The destruction involves destruction of property such as computer vandalism and the transmission of harmful programmes such as viruses are examples of this type of crime. The hackers usually engage in cracking security codes in order to steal cash or destroy vital documents. They often engage in cracking to gain access to

e-commerce, funds, point cards and e-marketing product sites of computer systems among others (Dashora, 2011).

- **Cybercrimes against Government**

Government could also be a victim of cybercrime. A good example is cyber-terrorism. Technological development has shown that individuals or groups may use the cyberspace to terrorise the government and the citizens of the country. Through the Internet, this crime became manifested when individuals or groups forcefully infiltrated a government or military website to expose some secret documents in order to indict the government or expose some of their hidden activities or agendas to the world (Dashora, 2011). For instance, a hacker made a name for himself in 2014 when he took on six Senegalese government sites (Jean & Amzath, 2016). Also, there was another hacker named Anons who in 2015, attacked the sites of the State Information Technology Agency (ADIE) and the Ministry of Livestock and Animal Production in Senegal (Jean & Amzath, 2016).

- **Fraud - Identity Theft**

This is one of the most common cybercrimes in Africa. In this type of cybercrime, the personal information of a person is used by another person to procure certain benefits such as credit and goods. This involves a situation when someone gains access to another person's personal information and uses it for his own benefit. It also includes an occurrence such as stealing online banking account login and password to get access to an Automated Teller Machine (ATM). In Nigeria, for example, criminals usually adopt different kinds of strategies such as designing a web page and requesting unsuspecting individuals to fill in their personal information such as account and pin numbers and use these to commit crime (Parker, 1983). Unsuspecting unemployed graduates could also be victims of this type of criminality.

- **Password Sniffing**

Sniffers are in the business of monitoring all network traffic. A sniffer is a programme or a device that monitors and transmits information through a computer network. More often than not, cybercriminals often install a sniffer on their computer networks in order to monitor the personal information of their victims (Obiri-Yeboah, 2015). As noted by Dashora (2011), password sniffers are special kind of programmes that are receptive to the first 128 or more bytes from each computer network connections being monitored. When a computer network user is required to type his/her password after he/she must have put in his/her username, the sniffers may collect all the information of that user (Kowalski et al., 2008; Matanmi et al., 2013).

- **Cyber Stalking**

Cyber stalking involves the use of the Internet to harass another person. In most cases, it is used to commit sexual harassment as well as showing anger against people the perpetrators feel have wronged them. Individuals who leave their personal information on the Internet are more vulnerable to cyber stalking. The information they leave on the Internet can be used by the cyber stalker to follow them and observe or monitor their activities on the Internet (Justin, 2010). Cyber stalkers may use foul language against their victims, using their race/ethnic group, gender, religion as well as their countries of origin as the basis for casting aspersions on them. They often send such foul language and aspersions to their victims through online groups; they also send hate or derogatory e-mail messages (Obiri-Yeboah, 2015).

- **Yahoo Attack**

As noted earlier, 'yahoo' is a popular term commonly used in Nigeria to describe internet fraudsters. They are also called 419ers because the law against the offender has been enshrined in section 419 of the Nigerian criminal code. Yahoo attacks can be achieved through the use of e-mail addresses that might have been retrieved from the access points of the Internet through the use of the harvesting application of the e-mail addresses. The extractor can be used as a tool that can automatically retrieve e-mail addresses from web pages. This is not new among Nigerian Internet fraudsters. These online fraudsters may impersonate another person or pretend to be someone else in order to defraud (Tade & Aliyu, 2011; Tade, 2013).

- **Drug Trafficking Deals**

This is another type of cybercrime. It is an illegal activity involving deals such as cultivating, manufacturing, distributing and selling substances which are prohibited by drug prohibition laws. Drug traffickers use the Internet to sell their products through different Internet technologies such as encrypted e-mails. It is argued that selling drugs on the Internet has been on the rise as a result of lack of a one-on-one communication between the sellers and buyers. According to Oludayo (2011), these virtual trades between the sellers and buyers allow both buyers and sellers to trade comfortably.

- **Bank Verification Number (BVN) Scams**

The Bank Verification Number (BVN) was introduced by the Central Bank of Nigeria (CBN) in order to safeguard financial transactions, especially in commercial banks. The essence of the BVN is to reduce or eliminate fraudulent financial transactions (Orunsolu, Sodiya, Akinwale, Olajuwon, Alaran, Bamgboye & Afolabi, 2017)). However, the implementation of the use of the BVN has given the fraudsters the opportunity to extort money and to carry out other fraudulent

activities (Alao, 2016). Some fraudsters may fraudulently claim to know the simplest ways of registering for the BVN, thereby demanding the bank details of their victims (Ebem, Onyeagba & Ugwuonah, 2017). Some of them threaten their victims (Esoimeme, 2015). Some may claim to be working for their victims' banks. The main target is to get access to their victims' money. They usually send unauthorised text messages to victims and also make phone calls asking for the personal information and bank details of their victims (Omodunbi, Odiase, Olaniyan & Esan, 2016). In addition, phishing sites may be created to acquire such information for dubious activities on bank accounts (Alao, 2016).

FACTORS FUELLING CYBERCRIMES IN AFRICA

A number of factors has contributed to and sustained the high incidence and prevalence of cyber-criminality in Africa. This section is devoted to discussing some of these factors. The most discussed factors are the high rate of unemployment, increased urbanisation, the quest for quick money or greed, the negative role models and peer influence. These are discussed within the context of relevant theories of crime and criminality.

- **High Rate of Unemployment**

Some literature have linked unemployment with cybercrimes (Zenou, 2000; Oumarou, 2007; Anah, Funmi, & Makinde, 2012). According to a UN report cited in Borode (2011), over one billion people are unemployed globally, with most of them in Africa. Ajaegbu (2012) noted that those between 14 and 50 years of age are the worst hit by unemployment and its consequences. According to Sodipo (2014), the rate of unemployment increased from 21% in 2010 to more than 23% in 2011. In the first quarter of 2015, the rate of unemployment increased by 9.9% (Chukumezie & Osakpa, 2015). Based on a report cited in Shuaibu *et al.*, (2018), the number of the underemployed in the labour force increased by 392, 390 or 2.61%, resulting in an increase in the underemployment rate to 19.3% in Q2 of 2016 from 19.1% in Q1 of 2016. This clearly reveals that a lot of youths are not employed; many are also underemployed.

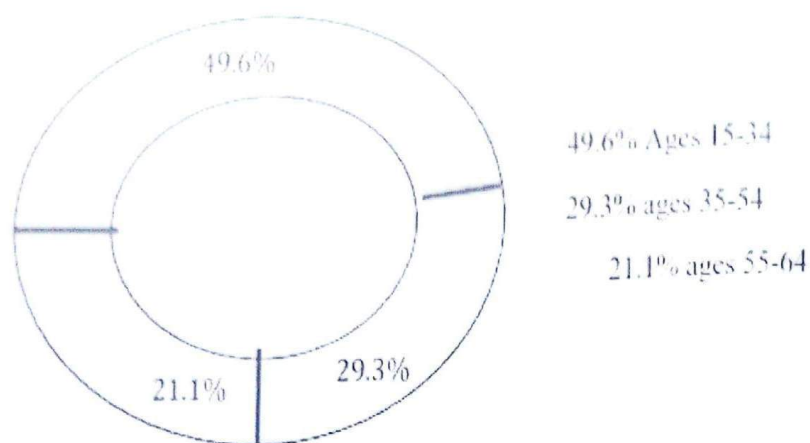


Figure 1: Unemployment Situations in Nigeria

Source: Shuaibu et al., (2018, p.60)

Okeshola & Adeta (2013), Sodipo (2014), Chukumezie & Osakpa (2015) and Shuaibu, Jogana & Mukhtar (2018) have, therefore, posited that the main driver of cyber-criminality in Africa and indeed Nigeria is unemployment. A Yoruba adage says “Owo to dile lesuyalo” (meaning “An idle mind is the devil’s workshop”). As such, most of our youths will use their time and knowledge as a platform for criminal activities in order to improve their livelihood and make ends meet. This tallies with the argument of the Relative Deprivation Theory (RDT).

The RDT was developed by Gurr (1970). According to this theory, individuals are more likely to commit crimes when situations in the society are unfair to them. In other words, poverty, unemployment and inequality are the main correlates of crime. According to Obi (2008, p. 7), “the high expectations of the people that democracy would reverse decades of poverty, corruption and underdevelopment have hardly been met by the new democrats”. Based on this theory, those who are unemployed see themselves as being deprived OF employment opportunities in the country. In reaction to their perceived deprivation, they are more likely to engage in cybercrimes.

- **Increased Urbanisation**

The influx of people from villages to urban centres has been considered as one of the major determinants of the increasing rate of cybercrimes in Africa in general and in Nigeria in particular. Urban growth is associated with the expansion of urban centres as a result of the positive migratory behaviours among rural dwellers. The expansion of urban centres produces increasing number of youths

who are unemployed. While they are jobless in urban centres, some youths take the path of cybercriminality as a means of survival. These people are mostly referred to as 'Yahoo Boys' (Meke, 2012). Literature has reported a connection between urbanisation and crime (Wirth, 1938; Clinard, 1942; Johnson, 1992; Oumarou, 2007; Meke, 2012). One of the oldest publications by Wirth (1938), had reported that urbanisation is one of the causal factors of crime. Also, Wirth (1964) stated that certain urban characteristics such as size, density, heterogeneity and impersonality may produce a kind of lifestyle that generates crimes. According to him, "the close living together and working together of individuals who have no sentimental and emotional ties foster a spirit of competition, aggrandisement, and mutual exploitation. Formal controls are instituted to counteract irresponsibility and potential disorder" (Wirth, 1964, p. 74). In the same vein, Clinard (1942, p. 203) stressed that crime is more likely to concentrate in a densely populated area than in a sparsely populated area. He attributed this to urban characteristics such as mobility, differential association, limited participation in community organisations, organised crime cultures and impersonal relations (Ajaz, 2016).

Long ago, Shaw & McKay (1942) used the concentric model to explain the process of social disorganisation that leads to concentrations of crime in some parts of the urban centres. These authors emphasised some characteristics of urban areas that cause high crime rates. These are poverty, residential mobility, ethnic heterogeneity, over population, housing problems and weak social relations. These characteristics which occur in urban centres are indicative of social disorganisation. After a further deterioration of the centres, many offenders are more likely to settle there. Burgess (1967) further expanded the idea of the SDT. As noted by Burgess, a city can be ecologically divided into concentric zones with varying crime rates. Based on the theory, crime is more likely to be very high in the transitional zones surrounding business centres. To Sampson and Groves (1989), crimes may be consequences of socio-economic deterioration in urban centres.

- **Quest for Wealth or Greed**

Many young people get involved in cybercrimes because they want to get rich quickly, regardless of whether the means are legitimate or not (Zenou, 2000; Lipsey & Chrystal, 2007). One of the theories that best explains this phenomenon is the Queer Ladder of Social Mobility Theory developed by a sociologist, Daniel Bell (1953). Bell originally used this theory to explain the entry of Italian American criminals into organised crime. Bell (1953) observed that

most Italian immigrants in America lacked access to political ladders to move up in the American society. Consequently, they decided to device their illicit ladders to achieve wealth or rise to the highest social status in the American society. Based on this theory, those who are excluded from reaching their expected goals through political ladders discover illicit means of becoming wealthy. They find few illicit routes to wealth. They may also use illicit paths to achieving their goals. This theory can be used to explain the increasing prevalence of cybercrimes in our contemporary society.

Another theory that can be used to explain the quest for wealth among cybercriminals is the Social Strain Theory developed by an American sociologist, Robert K. Merton (1968). According to the theory, social structures may push people to commit cybercrimes. For instance, society values success and wealth, but it does not give equal opportunities to every citizen to achieve success and wealth. The theory stipulates that opportunities are blocked for some people in the society despite their efforts in achieving goals or becoming wealthy (Boundless, 2015; Halder & Aishankar, 2011). Consequently, these people turn to illicit means of getting rich or wealthy (Choi, 2008; Lovet, 2009). According to Dambassau (2011), in Nigeria, wealth is not only glorified; it is worshipped. In Nigeria, nobody will ask how a pauper suddenly becomes wealthy. As noted by Dambasau (2005), the only thing they would say is that he has made it. This means that society no longer care about how money is made. This could explain why most unemployed youths turn to *Yahoo-Yahoo* in order to get rich, since the society will not ask how they made their money.

- **Negative Role Models/Peer Influence**

Some studies have linked negative role models with the cause and sustenance of cybercrimes (Holt, Bossler & May, 2012; Tade, 2013; Babatunde & Olanrewaju, 2015). Tade (2013) found peer influence as one of the major factors influencing cybercrimes in southwestern Nigeria. Similarly, Babatunde & Olanrewaju (2015) reported that the peer factor is significantly related to the prevalence of cybercrimes in their study among university undergraduates in southwestern Nigeria. The influence of negative role models on cybercrimes is in line with the Differential Association Theory developed by Edwin Sutherland. According to Sutherland (1973), criminal behaviour is learned through association with experienced criminals. Thus, cybercrimes require a lot of knowledge, motivation and experiences to start. Therefore, it requires a lot of learning from experienced cybercriminals. It is from the experienced cybercriminals that the techniques for perpetuating the crimes and the motivation required for engaging in and sustaining the act are learned (Holt et al., 2012; Tade, 2013).

CONCLUSION

This chapter has discussed cybercrime and criminality as an emerging form of crime in Africa. The chapter examines the incidence, prevalence and causes of cybercrimes in Africa. It explains the various types and dimensions of cyber-criminality, both within Africa and globally. It is important to mention that cyber criminals will always keep pace with any technological advancement. It is, therefore, important that students and experts in the fields of sociology, criminology and social work familiarise themselves with these emerging forms of crimes with a view to understanding them and getting equipped with skills to help both the victims, the perpetrators, and by and large the society as a whole.

REFERENCES

- Adaramola, Z. (2011). *Nigeria to launch two satellites into orbit in July*. Daily Trust, Friday, June 24. Pp.11.
- Adeka, M.I., Anoh, K.O., Ngala, M.J., Shepherd, S.J., Ibrahim, E.M., Elfergani, I.T., & Abd-Alhameed, R. A. (2017). *Africa: cyber-security and its mutual impacts with computerisation, miniaturisation and location-based authentication*. European Alliance for Innovation, University of Bradford. Retrieved on the 11th January, 2019 from <https://core.ac.uk/download/pdf/153514956.pdf>.
- Adeniran, A. (2011). Cafe culture and heresy of yahooboyism in Nigeria. In: K. Jaishankar (ed.), *Cyber criminology: Exploring internet crimes and criminal behaviour*. Boca Raton, FL, USA: CRC Press. Pp: 3-12.
- Adeniran, A.I. (2008). The internet and emergence of yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology*, 2(2): 368—381.
- Ajaegbu, O.O. (2012). Rising youth unemployment and violent crime in Nigeria. *American Journal of Social Issues and Humanities*, 2(5): 315-321.
- Akogwu, S. (2012). *An assessment of the level of awareness of cybercrime among internet users in Kaduna State*. Bachelor of Science Project submitted to Department of Sociology, Ahmadu Bello University, Zaria.
- Alao, A.A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research*, 4: 1-19.
- Alemika, E.O. (2007). *Police reform in Africa: Issues and challenges*. IDASA, Police reform in post-conflict African countries conference. Pretoria, South Africa. Pp. 12-15.
- Amara, N., Zhiqui, H., & Ali, A. (2017). *Cloud computing security threats and attacks with their mitigation techniques*. Paper presented at the 2017

- International conference on cyber-enabled distributed computing and knowledge discovery (CyberC), 12-14 October (Pp. 244-251).
- Ani, L. (2011). Cyber crime and national security: The role of the penal and procedural law. *Law and Security in Nigeria*, pp. 197-232.
- Arase, S.E., & Obaedo, A. (2007). Hi-tech (Computer and cyber) crimes. In S.E. Arase & Iwuofor (eds.), *Policing Nigeria in the 21st century*. Ibadan: Spectrum Books E. pp: 299-307.
- Asokhia, M.O. (2010). Enhancing national development and growth through combating cybercrime/Internet fraud: a comparative approach. *Journal of Social Sciences*, 23(1), 13-19.
- Ayantokun, O. (2006). *Fighting cybercrime in Nigeria*. Retrieved on the 17th July, 2018 from www.tribune.com/ng/08062016/infosys2.html.
- Babatunde, M.M., & Olanrewaju, M.K. (2015). Peer pressure, parental socioeconomic status, and cybercrime habit among University undergraduates in Southwestern Nigeria. *International Journal of Technology in Teaching & Learning*, 11(1): 50-59.
- Bashir, M. (2011). NSA: Cyber terrorism days are numbered. Daily Trust. Friday June 24, 2011. Pp: 3.
- Bell, D. (1953). Crime as an American way of life. In: M.E. Wolfgang, L. Savitz., & N. Johnston (eds), *The sociology of crime and delinquency* (2nd edition), New York: Wiley.
- Boateng, R., Longe, O.B., Mbarika, V., Avevor, I., & Isabalija, S.R. (2010). Cyber crime and criminality in Ghana: Its forms and implications. Proceeding of the Americas Conference on information system retrieved on the 16th June, 2017 from
- Borode, M. (2011). Higher education and poverty reduction among youths in the sub-Saharan Africa. *European Journal of Educational Studies*, 3(1): 149-155.
- Brenner, S.W. (2010). *Cybercrime: Criminal threats from cyberspace*. An imprint of ABC-CLIO, LLC, Santa Barbara, CA. retrived on the 17th of July, 2019 from http://law.suffolk.edu/highlights/stuorgs/jhtl/book_reviews/2010_2011/Anna%20Cometa%20-%20Cybercrime.pdf
- Burgess, E.W., & Bogue, D.J. (eds.) (1967). *Urban sociology*. Chicago: University of Chicago.
- Central Bank of Nigeria (2003). *CBN annual report and statement of accounts for the year ended 31st December*. Abuja, CBN.
- Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of information, Law and Technology*, 1(1): 1-20.
- Choi, K.S. (2008). Computer crime victimisation and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1): 45-61.

- Chukwumezie, F.U., & Osapka, D.U. (2015). Entrepreneurship opportunities and Nigerian graduates' unemployment in south-east and south-south geopolitical zones. *African Educational Research Journal*, 3 (3): 2354-2160.
- Clinard, M.B. (1942). The process of urbanisation and criminal behaviour. *American Journal of Sociology*, 48 (2): 202-21.
- Clough, J. (2010). *Principles of cybercrime*. Cambridge: Cambridge University Press.
- Dambazau, A.B. (2011). *Criminology and criminal justice*. Ibadan: Spectrum Books Limited.
- Dashora, K. (2011). Cybercrime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1): 240-259.
- Ebem, D.U., Onyeagba, J.C., & Ugwuonah, G.E. (2017). Internet banking: Identity theft and solutions-The Nigerian perspective. *The Journal of Internet Banking and Commerce*, 22(2): 1-15.
- Esoimeme, E. (2015). A critical analysis of the bank verification number project introduced by the Central Bank of Nigeria. Available at SSRN 2544934.
- Ewepu, G. (2016). Nigeria loses N127bn annually to cyber-crime — NSA. Retrieved 23rd of April, 2018 from [at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/](http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/)
- Ezeoha, A.E. (2006). Regulating internet banking in Nigeria, problem and challenges. *Journal of Internet Banking and Commerce*, 11(1), 56-78.
- Goodman, M. (2002/2003). Making computer crime count. In J.L. Victor & J. Naughton, (eds.) *Criminal justice*. Connecticut: McGraw Hill/Dushkin.
- Grabosky, P. (2010). 9 types of cybercrime. Retrieved on the 17th July, 2018 from www.hku.hk/cybercrime.htm
- Gurr, T.R. (1970). *Why men rebel*. Princeton (NJ): Princeton University.
- Gyongyi, A., & Hector, G. (2005). *Web spam taxonomy*. Proceedings of the first internal on the web (AIRWeb), 2005 in the 14th international world wide web conference (www2005) May 10,(Tue)-14(Sat), 2005, Nippon Convention center (makuharimesse) chiba, Japan (PDF). New York, NY:ACM Press. I-SBNI-59593-046-9.
- Haag, R. (2002). *Computing concepts*. New York: McGraw-Hill.
- Halder, D., & Aishankar, K. (2012). *Cybercrime and the victimization of women: laws, rights and regulations*. Hershey, PA: Information Science Reference.
- Hansell, S. (2007). *Social network launches worldwide spam campaign*. New York: New York Times.

- Hansen, B. (2003/2004). Cybercrime: Should penalties be tougher? In J.L. Victor & J. Naughton, (eds.), *Criminal justice*. USA: McGraw Hill and Dushkin. Pp: 19-27.
- Hasan, M.S., Rahman, R.A., Abdillah, S.F.H.B.T., & Omar, N. (2015). Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, 11(4): 395.
- Hassan, A., Lass, F.D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *Journal of Science and Technology*, 2(7): 626-631.
- Holt, T.J., Bossler, A.M., & May, D.C. (2012). Low self-control, deviant peer associations, and juvenile cyber deviance. *American Journal of Criminal Justice*, 37(3): 378-395.
- Jean S., & Amzath, F. (2016). *Cybercrime in Africa: Facts and figures*. Retrieved on the 19th of June, 2018 from <https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html>.
- Johnson, E.A. (1995). *Urbanisation and crime*. New York: Cambridge University Press.
- Kasperky, E. (2008). *The cybercrime arm race*. Massachusetts, MA: Kaspersky Laboratory Incorporation.
- Lovet, G. (2009). *Fighting cybercrime: Technical, juridical and ethical challenges*. Virus Bulletin Conference September, 2009. Retrieved 122th June, 2017 from <https://www.scribd.com/document/238750730/Fighting-Cybercrime-Technical-Juridical-and-Ethical-Challenges>
- Ludwig, M., & Noah, D. (2017). *The giant black book of computer viruses*. Washnigton DC: American Eagle Books.
- Matanmi, O., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Impact of cybercrimes on Nigerian economy. *The International Journal of Engineering and Science*, 2(4): 45-51.
- Malik, A.A. (2016). Urbanisation and crime: A relational analysis. *J. Human. & Soc. Sci.*, 21: 68-69.
- Mark, S. (2018). *Known unknowns: The threat of cybercrime in Africa*. Institute for Security Studies. Retrieved on the 19th June, 2018 from <https://issafrica.org/iss-today/known-unknowns-the-threat-of-cybercrime-in-africa>.
- Mbasekei, M.O. (2008). *Cybercrimes: effects on youth development*. A paper presented at Clean Foundations' Youth against Crimes Quarterly Interactive Forum in Bola Ige Millennium Secondary School Ajegunle, Lagos 1st Sept. 2008. Retrieved 14th June, 2011 from <http://i.genuis.org/member/profile.php/id/1138/post1007>

- McAfee North America Criminology Report (2007). *Organised crime and the internet*. California: McAfee incorporation.
- Meke, E.S.N. (2012). Urbanisation and cyber crime in Nigeria: Causes and consequences. *European Journal of Computer Science and Information Technology*, 3(9): 1-11.
- Merton, R.K. (1968). *Social theory and social structure* (1968 enlarged Ed.). New York: Free Press.
- Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Review*, 21(5): 408-414.
- Nzeako, A. (1999). *Internet and rural development: prospects and challenges*. A paper presented at the Internet Society in Nigeria Chapter International Conference.
- Obi, C.I. (2008). *No choice, but democracy: Prising the People out of Politics in Africa?* Department of Peace and Conflict Research, Uppsala University; Nordiska Afrikainstitutet.
- Obiekwe, O.T. (2006). *The impact of pornography on Nigeria youths in Gwagwalada area Council of Abuja*. B.Sc Project submitted to Department of Sociology University of Abuja, Abuja).
- ObiriYeboah, N.L. (2015). *An Investigation of Youth in Cybercrime in the Ayawaso East Constituency of Greater Accra* (Doctoral dissertation, University of Ghana).
- Oji, C. (2011). *Scan: Police rescue Saudi Bizman from kidnappers*. The Daily Sun, Thursday October 20th 2011. Retrieved on the 21st October 2011 from www.sunnewsonline.com.
- Okeshola, F.B., & Adeta, A.K. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research*, 3(9): 98-114.
- Olaide, A., & Adewole, R. (2004). Cybercrime embarrassing for victims. Retrieved on the 12th September 2014 from <http://www.heraldsun.com.au>.
- Oludayo, T., & Ibrahim, A. (2011). Social organisation of internet fraud among university
- Olusesi, M. (2008). *Cybercrime in Nigeria: A sociological analysis*. Retrieved on the 14th June, 2011 from <http://profgave.blogspot.com>
- Omodunbi, B.A., Odiase, P.O., Olaniyan, O.M., & Esan, A.O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *Journal of Engineering and Technology*, 1(1): 37-42.
- Onifade, A., & Mohammed, M. (2000). *Money laundering and cybercrime*. Zaria: Hasha Ventures Publishers.

- Orunsolu, A.A., Sodiya, A.S., Akinwale, A.T., Olajuwon, B.I., Alaran, M.A., Bamgboye, O.O., & Afolabi, O.A. (2017). An empirical evaluation of security tips in phishing prevention: A case study of Nigerian banks. *International Journal of Electronics and Information Engineering*, 6(1): 25-39.
- Oumarou, M. (2007). Brainstorming advanced fee fraud: 'Faymania'– the Camerounian experience. *Current Trends in Advance Fee Fraud in West Africa*, 33-34.
- Oyenuga, A.S. (2015). *Youth and cybercrime culture in Lagos state, Nigeria*. Unpublished Ph.D. Post-Field Seminar, Department of Sociology, University of Ibadan.
- Pack, W., & Jewel, D. (2014). *The Nigerian cyber threat. Barometre Report 486*. Retrieved August 19th, 2015 from www.digitaljewels.net/index.php/index.php/resource-center/djlnews/129-the-2014-nigerian-cyber-threat-barometer
- Parker, D. (1983). *Fighting computer crimes*. U.S.Charles Scribner's Sons.
- Plot, J. (2010). *Top five computer crimes and how to protect yourself from them*. Publication of Justin plot.
- Rittinghouse, J.W., & Ransome, J.F. (2005). *IM: Instant messaging security*. USA: Elsevier Digital Press.
- Salifu, A. (2008). Impact of internet crime on development. *Journal of Financial Crime*, 15(4), 432–444.
- Sampson, R.J., & Groves, W. B. (1989). Community structure and crime: Testing social-disorganization theory. *American journal of sociology*, 94(4): 774-802.
- Saul, H. (2007). *Social network launches worldwide spam campaign*. New York: New York Times.
- Shadow Market 2011 (2012). *Global software piracy study Ninth edition*. May 2012. Retrieved 12th September, 2011 from <https://techpost.bsa.org/2012/05/15/shadow-market-global-software-piracy-study/>.
- Shaw, C.R., & McKay, H.D. (1942). *Juvenile delinquency in urban areas: A study of rates of delinquency in relation to differential characteristics of local communities in American cities*. Chicago, Illinois: University of Chicago Press.
- Shehu, Y.A. (2014). Emerging issues in cybercrime: Causes, implications and effects for the legal profession. *Online Journal of Social Sciences Research*, 3(7): 169-180.
- Shinder, D.L. (2002). *Scene of the cybercrime*. Computer Forensics Handbook. Syngress Publishing Inc,
- Shneiderman, B. (2010). *Designing the user interface: strategies for effective human-computer interaction*. New Delhi: Pearson Education India.

- Shuaibu, H., Jogana, M.A., & Mukhtar, N. (2018). Integrating entrepreneurship and technical education as a panacea for graduates unemployment in Nigeria. *British Journal of Education*, 6(3): 57-71.
- Siegel, L.J. (2007). *Criminology: Theories patterns and typologies*. (9th Edn.), Washington DC: Thomson Wadsworth.
- Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, 58(1): 22-23.
- Sodipo, O.O. (2014). Employability of tertiary education graduates in Nigeria: Closing the skills gap. *Global Journal of Human Resources Management*, 2(3): 22-36.
- Sutherland, E.H., & Schuessler, K. (1973). *On analysing crime*. Chicago: University of Chicago Press.
- Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, 23: 689-705.
- Tade, O., & Aliyu, I. (2011). Social Organisation of Internet Fraud among University Undergraduates in Nigeria. *International Journal of Cyber Criminology*, 5(2): 71-85.
- Van Vuuren, J.C.J. (2016). *Methodology and Model to Establish Cybersecurity for National Security in Africa using South Africa as a Case Study* (Doctoral dissertation). Submitted on the 26th February, 2016 to the University of Venda, South Africa.
- Voigt, K. (2011). Analysis: The hidden cost of cybercrime. Retrieved 7 June, 2011 from www.edition.cnn.com
- Waziri, F. (2011). *Towards increasing capital flow to Africa: EFCC's reforms and way forward*. Paper Presented at UN Conférence on Least Developed Countries, Istanbul Turkey.
- White, G.B., Fisch, E.A., & Pooch, U.W. (2017). *Computer system and network security*. CRC Press.
- Whitty, M.T., & Ng, M. (2017). *Literature review for underware: understanding West African culture to prevent cybercrimes*. Report for the National Cyber Security Centre as part of a group of studies funded in the Research Institute in Science of Cyber Security. Retrieved 7 June, 2011 from https://minerva-access.unimelb.edu.au/bitstream/handle/11343/198264/underware_literature_review_whitty.pdf?sequence=1&isAllowed=y
- Wirth, L. (1964). *On cities and social life*. Chicago: London.
- Wirth, L. (1938). Urbanism as a way of life. *The American Journal of Sociology*, 44(1): 1-24.
- Young Media Association (2007). *The internet: Benefits, dangers and strategies*. Australia: Young Media Association.

Youth against Cybercrime and Fraud in Nigeria (2008). *Statement of problem.*

Retrieved January 5th 2009 from www.yaccfin.org.

Zenou, Y. (2000). Urban unemployment, agglomeration and transportation policies. *Journal of Public Economics*, 77(1): 97-133.

Zero Tolerance (2006). Retiree in trouble over internet fraud. *Economic and Financial Crime Commission*, 1(2): 39-41.