ISSN: 2321-8819 (Online) 2348-7186 (Print) Impact Factor: 1.498 Vol. 6, Issue 12, December, 2018

Political Perspective: Evaluating the Causes of Cybercrime in Nigeria

Okpe, Victor Vincent[1] and Shamsuddin L. Taya[2]
[1]Universiti Utara Malaysia
Sintok, Kedah, Malaysia
victorenugu47@gmail.com
[2]Universiti Utara Malasia
Sintok, Kedah, Malaysia
shamsuddin@uum.edu.my

Abstract: The influence of the internet and computers in the contemporary age cannot easily be undermined. To some scholars, they are agents of faster development. While to others, an agent of modern crime in the society which now makes the internet to exist as a double-edge sword and as a subject of debate. Thus, the aim of this study was to examine the political factors that led to cybercrime in Nigeria. The data for this study are collected mainly from both primary and secondary sources. Interviews with some knowledgeable and prominent figures who are familiar with the Nigerian political environment.. The study indicated that cybercrime in Nigeria has been encouraged by the rotten political system such as, the actions of the political elites, weak security system, poor dispensation of justice, weak security laws, colonialism as well as vengeance mission against unjust political and economic system.

Keywords: Cybercrime, Information Communication Technology, internet, Nigeria, political system.

INTRODUCTION

In the contemporary era of globalization, the emergence and the role of the Information Communication Technology (ICT) also known as the internet is seen as indispensable in societal development. In view of this, Thomas and Adam (2014) noted that the internet and computers have developed as a significant part of modern existence across the continent, impacting communications, governance, finance, education, health and many more. This global wave of connection and interaction known as the internet (Magele, 2005) has become a powerful force in almost all aspects of human existence. The internet, which occupies the center stage of this global wave, now appears as a double-edge sword, offering opportunities for people and organizations, but also comes with it an increased and huge information security risk (Magele, 2005).

The ICT, chiefly the internet has transformed both the formal and informal transaction environments. In specific, the practices of economic globalization, which are aided by the ICT, not only offer opportunities for a profitable development of a global informational markets, but equally provide an opportunity for criminal activities in the cyberspace (Castells, 1996, 1999). The internet crime, also known as cybercrime, involves any kind of unlawful activity or venture emanating from one or several internet components which include e-mail, chat rooms and web sites. Cybercrime can also involve anything that has to do with theft of trade secrets (economic espionage), hacking or computer intrusion, nondelivery of goods and services purchased online, abuse of intellectual property rights, international financial laundering, identity theft, online extortion among other computer and internet-enabled crime activities (Larkin, 2006).

As the ICT has continued to manifest itself in every human society of the world, Nigeria, standing as the giant of the African continent and the most populated black nations of the world, is not left out in this global wave of the internet age. The internet which has contributed in the development of the Nigerian health sector, sports, education, transport among others, also did not leave the country without crimes. In the light of this, Tade and Aliyu (2011) underscored that cybercrime in Nigeria has been accepted as a way of survival amongst the younger population who engage in all kinds of cyber criminalities ranging from internet fraud, money laundering, extortion and others which he attributed to the country's rotten political system. Tade and Aliyu further maintained that many individuals through this unlawful medium have achieved wealth, while some are facing the weight of the law. In April 2012 for instance, Olabisi Onabanjo University student by name Olabisi Dare, was caught in this act and was served with a jail term of five years for attempting to obtain wealth online under false pretense in a business café. Also, on June 2012, a 25 year Nigerian undergraduate at the University of Ilorin, Kwara state, Nigeria was penalized by the Nigerian Federal High Court for defrauding an Australian one thousand U.S dollars ($1, 000).

The growing rate of cybercrime activities in the country is seen as a product of the Nigerian corrupt, weak and rotten political system.

According to Mikail (2016), who noted that in Nigeria, politicians and policy decision-makers empowered by the constitution to make and implement laws as representative of the people, are corrupt and represent their own interest rather than the people. In Nigeria today, wealths are brazenly spent and celebrated in the public, chiefly among the Nigerian politicians and other public servants without interrogation and whom through this kind of life style encourage crime prone individuals to engage in online crime activities to make easy money and be celebrated too. To worsen the situation, the state politicians found stealing from the public treasury are allowed to be committee members of the state, as well as presented with national awards (Tade & Aliyu, 2011).

Given this as shown above, it becomes necessary in this study to understand the issue of cybercrime in Nigeria. Most importantly, to examine how the country's political system has led and encouraged cybercrime activities in the country. In order to achieve this, the study relied on qualitative methods, theory of anomie and historical approach. Data were generated through primary and secondary sources as interview with knowledgeable and respected individuals were also carried out. The study is divided into six components. The first component deals with the general background of the study. The second component involves clarification on the concept of cybercrime and the review of important literatures on the subject matter. The third has to do with the theoretical framework while the fourth component examines the political factors that led to cybercrime in the country. The fifth component captures its implication on the Nigerian economic development, while the last component looks into the conclusion and recommendations.

The Concept Cybercrime

The concept 'cybercrime' has not enjoyed a common or a universal agreement on what it simply portrays. In lieu of this, scholars and commentators have continued to have a heated debate over the meaning of the concept. According to Abdi and Mosud (2014), there exists an absence of a general and complete acceptable understanding of the concept among scholars. To O'Connor (2003), cybercrime by the law enforcement bodies, involves an internet crime, while academic scholars observed it as a computer deviance. In the same coin, Wall (2001) noted that online crime or internet crime, symbolizes a comparatively new area of crime that has emerged from the justice area of knowledge recognized as computer crime or simply a computer related crime.

In addition to the above, Shehu (2014) who shared a similar idea, observed that the concept cybercrime was created by Peter Cassidy to differentiate computer programs and the intertwining range of programs that are designed particularly to distinguish financial crimes from the other categories of malevolent packages. Cybercrime involves the use of computers and the internet to attack innocent users online ranging from identity theft, credit card theft, financial laundering by criminals or terrorists (Ojedokun & Eraye, 2012). In the same vein, Jaishankar and Halder (2011) viewed cybercrime as an act targeted against an individual or group of individuals with a criminal notion to intentionally cause a physical or mental harm or even abuse the status of the target directly or indirectly via the use of the present interaction gadgets which involve the internet (emails, notice boards, groups or chat rooms) and mobile phones. This definition limits cybercrime to an internet aided unlawful activities targeted at groups or an individual.

According to Kamini (2011), cybercrime denotes any crime executed on the internet or it involves the unlawful use of the computer as a device in carrying out such an act (e.g., forgery, phishing scams, fraud, identity theft, pornography, spams, online gambling, junk emails, cyber stalking, intellectual property crime and cyber defamation) or the computer being targeted as a victim (e.g. Access to network computer, denial of service, malware, data theft, malicious codes, salami attacks, email bombing, logic bombs, web jacking, internet time theft and Trojan attacks). This signifies that all internet crimes involve both the computer and the individuals as victims or targets. It all depends on which of them is the chief target. Similarly, Britz (2009) conceived cybercrime as any illegal activity which has to do with the abuse or misuse of computers connected to computer systems or the internet, which results into direct or concomitant losses. It simply involves a criminal behavior aided by the application of the internet.

Furthermore, UN Office on Drugs and Crimes (2005) observed that online crime is a conduct that involves the use of internet technologies in the exercise of a crime. While Cohen and Felson (1979) viewed it as a kind of crime opportunity executed by a motivated offender against a defenseless target. It is not different from other notable crimes; it is just the online space that makes it different (Soderman & Korsell, 2001). Cybercrime by (Thomas & Loader, 2000) equally involves a computer mediated act which is considered illegal or illicit by particular groups which can be exercised through a global electronic network. Therefore, deducing from the above, it is clear that the concept cybercrime does not enjoy a universal or simple embraced definition. Its meaning is drawn based on the person who is discussing it. It could be commonly viewed as a specific kind of crime which is chiefly executed in the cyberspace or the internet with the help of a computer, among other electronic gadgets.

Theoretical framework

This study makes use of the Theory of Anomie. This theory was founded by Emile Durkheim, a French sociologist. In his two renowned studies, “The Suicide” (1897) and “ The Division of Labor” (1893), Durkheim established that an anomie or crime occurs mostly during a time of weighty social change. As he noted, this social change may bring a loss of direction in the society especially when social control or regulation of a person’s behavior or conduct has become ineffective. This social control or regulation in this case could be the family discipline and guidance, the justice system, law enforcement agencies and the legislature (Ennin, 2015). According to Durkheim, in periods of rapid change in the society, economic collapse, social disorder, or even economic boom, individuals become more depressed, confused or even excited and this leads to a higher rate of individual disorganization such as suicide or violent crime (Ennin, 2015).

Stressing further, just as expressed above, Duekheim’s argument is that an anomie or crime could happen as a result of social instability mostly when those regulations and institutions that limit individual expectations and desires within an achievable level breakdown or no longer effective, and pave way for the pursuit of unattainable objectives through illegal means. The theory is essential in the explanation of not only internet crime in Nigeria, but amongst other crimes. In Nigeria, for example, the legal system, the security agents, the cyber laws, as well as the legislature is no longer effective and leading to the exploitation of these institutions by the cyber criminals to engage in online crimes. All these are smart indicators (Ennin, 2015). Furthermore, (Ennin, 2015) observed that people become more vulnerable and objects of target because there are absence of effective and stringent laws to penalize these criminals. In the same coin, Nigerian security agents cannot exercise control over the online space to monitor the activities of these criminals because of poor skilled manpower and dearth of modern equipment. The situation has developed a vicious circle of internet crime because it elevates the criminals confidence to persist in attacking innocent individuals on the online space due to the weak and poor regulative social system (Ennin, 2015).

In line with the above, Shehu (2014) noted that the emergence of computing and communication online and the rapid growth in online technology have brought an undoubted achievement to human existence. But these achievements as he noted further, also come with several social ills among other crimes in the society both at the national and international levels. Presently, many traditional crimes are currently being executed through the use of the networks and computers, and social ills previously never assumed by, have developed because of the unbelievable capabilities of the online system. In lieu of the above debate, internet crimes in Nigeria have been attributed to the following political factors as shown below:

The Political Elite Corruption; the high-rate of cybercrime in Nigeria has been attributed to the corrupt and weak Nigerian political system. According to Mikail (2016), the Nigerian policy makers or the politicians, as well as the other public figures empowered by the constitution of the land to formulate and implement policies in the interest of the common people are densely corrupt. Similarly, Tade and Aliyu (2011) noted that celebration of wealth in the society, particularly among the country’s political office holders serves to motivate and encourage the engagement of people who are enticed by this lifestyle to go into cybercrime to make quick wealth.

The Fragile Cyber Laws; another factor recognized as responsible for the emergence of cybercrime in Nigeria is noted as the weak and fragile cyber laws existing in the country. As observed, the Nigerian cyber laws are neither weak nor stringent enough to deter and prevent the perpetration of the crime. According to Anah, Funmi and Julius (2012), weak and fragile internet regulations exist in Nigeria, unlike in the well developed countries where internet crimes are punished with adequate penalties.

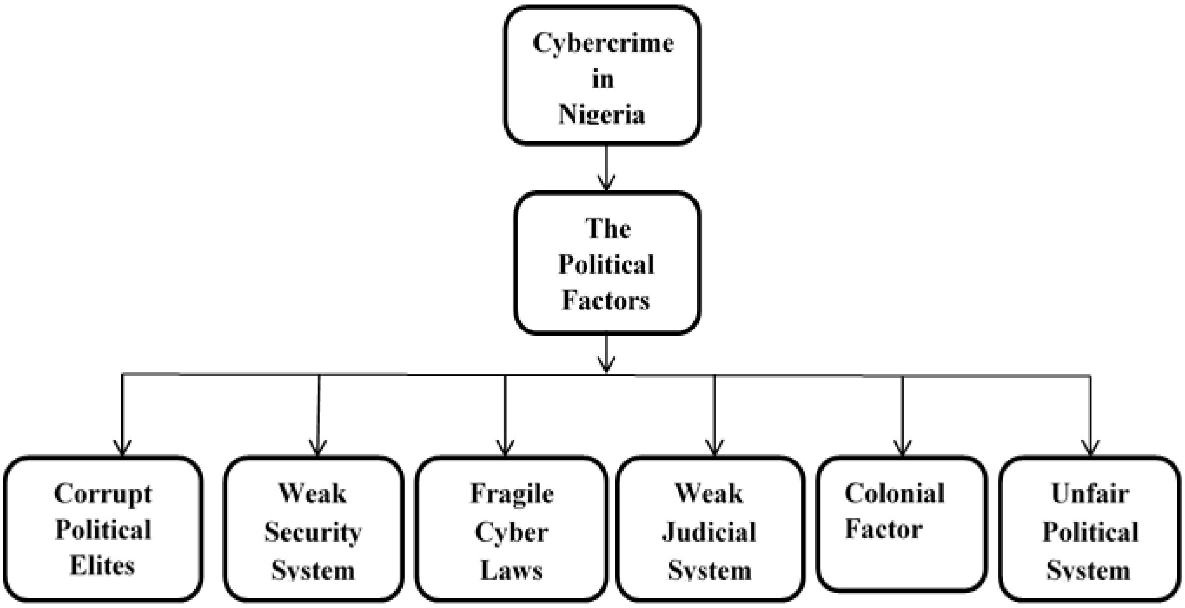
The Weak Security Agents; the Nigerian security agents are also not left behind among the political factors encouraging cyber criminality in Nigeria. In view of this, Laura (2012) noted that African nations and Nigeria in specific, has been backlashed for her poor handling of online crimes in the country due to the poor training of the nation’s law enforcements bodies most especially, in terms of personnel, intelligence, equipment and the private sector which has neither shown any serious interest nor take part in the fight.

The Weak Judicial System; one of the major functions of any responsible judicial system involves effective dispensation of justice. In Nigeria and in relation to cybercrime in particular, the judicial system has not been doing great. In addition to this, difficulties in obtaining facts and documentation to show that an online crime actually occurred make the problem complex (Kshetri, 2006). Also, resources needed to enhance investigation and trial are costly as well as energy consuming. Several courtrooms also do not have the technological gadgets needed to present evidence electronically.

Colonialism; in Africa and Nigeria to be precise, colonialism is also seen as a motivator for cybercrime. According Frank and Michael (2015), colonialism has encouraged young individuals into online criminalities in Ghana with the motion to get back or exploit the whites who assumed to have exploited and enslaved their ancestors, as well as exploited their natural resources. On the note, Oludayo (2013) viewed online crime as a vengeance enterprise against the foreigners.

Revenge on the Unfair Political System; disruption of government activities or attacking of a political system is usually seen as a way of expressing grievances against any unjust political system or government. In Nigeria, several individuals have viewed the government as unjust to their plight and in performing its responsibilities and thus encourage them to involve in all kinds of online criminalities against the state or the government. On this note, Adeniran (2008) noted that the use of the internet space to execute all sorts of crime in the country can be tied to the failure of the political leadership as well as the unfair social system in place.

Figure 1.1 Theoretical framework explaining the political factors encouraging cybercrime in Nigeria



An Overview of the Political Factors Encouraging Cybercrime in Nigeria

As observed above, the prevalence of cybercrime in Nigeria has been attributed to the country's rotten political system and the activities of the politicians amongst other public figures and office holders. In view of this, the following political factors such as, political elite corruption, weak cyber laws, Weak security system, weak judicial system, colonialism and revenge against the unfair political system have been identified as the main causes of the prevalence of cybercrime in the country and are discussed as thus:

Corrupt Political Elite

The actions of the Nigerian political office holders have been viewed as one of the factors that influence and encourage all kinds of online criminal activities in the country. In lieu of this, Adeniran (2011) noted that within the larger social superstructure of Nigeria, particularly amongst the public political figures, wealth is worshiped. On the assumption of office, the political elites place more emphasis on wealth acquisition rather than serving the interest of the masses or their electorates. In the light of this, delivery of democratic common goods to the society such as empowering the people becomes neglected. Similarly, Ojukwu & Shopeju (2010) observed that the nation's image and identity have been abused by the activities of the confused, factional and extremely corrupt political elites with a short sight for national interest. These state elites lacking vigor, viable and strong base for production, turn the country as their basic tool for wealth accumulation. At the end, the country and the people are rendered impotent thereby exposing the vulnerable ones to all sorts of social dangers and criminalities which cybercrime is not exceptional. In lieu of the ongoing, some of the informants interviewed noted that Nigerian political elites are behind most of the social crimes in the society through their corrupt activities in the system. For instance, informant (A) who took a look on the issue observed that:

> *You and I are aware that our political leaders are politically corrupt and in most of all their ways in the society. They do not think of developing the system or make life easier for the common man. They do not think of addressing hunger and crimes that are affecting the people. In this case, what do you anticipate from a leadership that is corrupt and does not represent the interest of the common people? If a leadership is corrupt, there is no doubt if the system also becomes corrupt which will pave way and promote all sorts of social crimes in the state. The politicians are in the public offices to guide the masses right via positive programs and policies, but what is before us in the country today? Politicians who promote their personal desires and encourage crime and poverty in the country. Cybercrime among the Nigerian people stands as one of the outcomes of the erroneous activities of the political office holders in power* **(Informant A1, personal communication, April 19, 2018).**

Similarly, reiterating on the corrupt political public figures in Nigeria and how they stimulate cybercrime and other social ills in the society, informant (F) expressed thus:

> *Cybercrimes in our country Nigeria are inspired by several political dynamics, in which the corrupt political elites stand as one. Political office holders in the logic that when they are elected directly or indirectly to represent the people, but were not the right candidates who supposed to man the office, they will definitely not respect and consider the public interest. In this case, the feelings and the respect for the masses will be in jeopardy. This kind of negative public servants may not render basic services to the citizens. At the end, the vulnerable citizens who become victims of these negative political incompetence and leadership may end up encouraged or motivated into cybercrime among other social ills in the society. So, wrong political office holders also encourage and promote cybercrime in the state* **(Informant F2, personal communication, April 20, 2018).**

In the above submissions, the actions of the political office holders in Nigeria leave little or no room for doubt. These public figures are extremely corrupt in that most of their unlawful activities against the state and its inhabitants not only encourage online criminal activities, but also other social crimes in the country. They frequently observe public office as an enterprise or as a venture where to satisfy their self and family's desire at the disadvantage of the common man in the society. Consequently, this kind of public priority misplacement by the politicians for personal interest, gives room for several crimes in the society in which cybercrime cannot be an exception.

The Fragile and the Feebleness of the Cyber Laws

The Nigerian cyber laws in operation as argued by many scholars and security experts are very weak and responsible for most of the cybercrime activities in the country. In relation to this, Anah, Funmi & Julius (2012) noted that the country's legislation must implement strict laws against online criminals and whenever they are found guilty, they must be allowed to face the law as their activities decrease the nation's competitive capacity, and failure to serve punishment, they will continue to take advantage of the weak and fragile existing laws in the country. In addition, weak and fragile laws regarding online criminals exist in the country and ineffective, unlike in the well developed nations where online criminals are disciplined with maximum punishments and penalties (Anah, Funmi & Julius, 2012). The case

[1] Informant (A), PhD candidate, School of International Studies, Universiti Utara, Malaysia.

[2] Informant (F), a PhD candidate, School of Business, Universiti Utara, Malaysia.

is that, cyber laws in Nigeria are very weak and fragile and thus, permit the cyber criminals to effect an attack on innocent citizens and remain undetected (Danbo, Ezinmora & Nwanyanwu, 2017).

According to Shonubi and Godwin (2017), active state's law in Nigeria is significant, particularly in the online space to guarantee security and survival of businesses online without attack or distress. As observed by Gbenga, Babatope and Bankole (2013) internet crime in the country will continue as a threat until it is properly addressed through active state legislation. In addition, Shonubi and Godwin further expressed that the current state of legislation against online crime in the state is not substantive due to the behavior of the policy makers whenever the case emerges for debate in the house. From the ongoing, informant (A) who corroborated with the above explained thus:

> *Our country lacks authentic and active cyber policy that will deter or prevent citizens from carrying out online criminal activities which are rampant in the society today among our people. This kind of situation will encourage individuals who will easily claim that Mr. 'A' executed a crime and supposed to be penalized, but he went unpunished. In this case, if Mr. 'A' can do it and go free, I can also do it and go free or unpunished. So, when the state space laws are weak and fragile, they will motivate vulnerable citizens into online criminalities. The cyber space laws need to be rigid and absolutely defined or clear* **(Informant A, personal communication, April 19, 2018).**

In line with the above assertion, informant (D) who also shed light in the same direction revealed that:

> *One of the motivating factors for online crime in Nigeria is the feeble online security laws in the country. When I said the feeble online security laws, I mean the cyber laws, we presently have in operation are not strong enough to prevent individuals from engaging in internet crime. Therefore, due to this feebleness of the laws in our security system, individuals are directly or indirectly inspired to take advantage of the weaknesses and the loopholes therein and commit crime in the cyberspace in the country. Internet crime is multidimensional, for this, rigid cyber laws become eminent to curtail them* **(Informant D**[3]**, personal communication, April 20, 2018).**

Furthermore, Oluwu (2009) who contributed to the above discourse, submits that to understand the reason why internet crime in African setting and particularly Nigeria is quite different from that of any other country on earth, one has to comprehend the state of security in the region which is highly affected by factors such as inadequate security awareness, poor regulations, delicate cross-border coalition and control, as well as inadequate law enforcement training and less reporting incidence in the setting. In the light of this, Ojedokun (2005) noted that in the absence of an actual record, one can easily argue that recording and conviction of online criminals will inescapably be less in the continent and Nigeria cannot be in the exemption. For example, cybercrime irregularities awareness is gaining momentum in Ghana, but the criminals enjoy low reporting to the state authorities from their victims. Also, the police force in Ghana and Nigeria for example, empowered by the constitution to arrest and punish these criminals lack proficient technical know-how and legal support to effectively prosecute these criminals (Richard, Longe, Robert and Joseph, 2011).

Poor Judicial System

In any political setting, an active and vibrant judicial system plays a major role in the dispensation of justice. Unlike in the developed countries where the judicial system is always active, it is not the same in Nigeria, where the cyber criminals get away with their crimes because of the poor judicial system in the dispensation of criminal justice. Though, conviction of an online criminal among other crimes requires a thorough evidence which must go above reasonable doubt to avoid complexities. In view of this, Kshetri (2006) noted that the challenges associated with the recording and documentation of facts to show that an online crime actually occurred complicate the problem. In addition, Kshetri further noted that the nature of cybercrime in contemporary time, presents real difficulties to the judicial system, as experts revealed that explaining online associated crimes to judges is often found to be difficult and challenging. Also, needed resources in the investigation and prosecution of these criminals are costly as well as energy sapping. Several courtrooms in the country are not technologically empowered with the needed tools to present evidence live via electronic channels. These

[3] Informant (D), School of Economics, Universiti Utara, Malaysia.

difficulties reveal why many online crime cases are terminated without trial or even prolonged if tried in the court in pursuit of sufficient evidence (Akin, 2011). As the debate continues and in specific to Nigeria, informant (D) who aligned with the above, revealed that:

> *Delay in the justice system represents another factor in the prevalence of internet crime in Nigeria. For example, when a person is alleged to have committed a crime traditionally or online, is arrested and taken to the law court, sometimes the legal procedures assume longer period than necessary. Most of the times, such cases are even dismissed on technical ground. Again, a well-known online criminal in this situation can be laid off the hook due to delay in the judicial proceedings. In this case, delay represents a factor and legal technicalities represents another factor. Therefore, combining the two factors produce a judicial system that is not active and sufficiently viable to prosecute online criminals. The online criminals usually exploit this advantage* **(Informant D, personal communication, April 20, 2018).**

In relation to the above, it is also argued that the reluctant interest of several judges to give room to intangible sources of evidence in the law courts makes the prosecutors to be weak in supporting cases of criminality with electronic evidence. In view of this, Brown (2015) submits that several lawyers and judges also reluctantly comprehend the intricacies in the electronic evidence at the time of trial. Supporting the above revelation and the actuality in the Nigerian justice system, informant (F) echoed that:

> *One of the primary responsibility of the government involves the provision of security for her citizenry. Provide adequate laws and ensure that they are properly enforced via the state security apparatus with the support of the law courts. But in Nigeria* for *example, an online criminal may be trapped, rather than charging him or her in the surest shortest time to the law court to face prosecution and probably imprison him or her, the case is prolonged. In this case, if the criminal is financially buoyant to buy a renowned law expert who could probably frustrate the case, that could be the end of it as every positive anticipated results from the case will be scuttled. In the event of this, this type of occasion not only promote all sorts of criminalities, it equally harbors online criminals* **(Informant F, personal communication, April 20, 2018).**

Deducing from the ongoing above justifications, one can easily conclude that the Nigerian judicial process is actually weak in the dispensation of online criminal cases. Also, the judicial system suffers capacity as well as modern technological equipments and training to convict or prosecute online criminals. Cyber criminals capitalize and exploit these loopholes in the system.

- **Colonialism**

Colonialism has been identified as one the factors responsible for cybercrime in Nigeria. In Ghana, for example, Frank and Michael (2015) noted that colonialism has inspired the citizens into committing online crime and usually with the notion to get back on the foreigners who supposedly enslaved their ancestors and exploited their natural resources. The online criminals see it as a payback opportunity and that inspires them to engage in such illegal act. In addition to the above, the actors expressed that the acts are not executed against the local citizens as the drive is usually towards the whites. In supporting the above argument, informant (A) observed that:

> *Going by the narratives of colonialism on the African continent, the Europeans exploited the indigenous people, took away their natural resources and heritage. In this situation, some of the criminals caught in this unethical act try to make reason out of it. Several of them believe that it is a payback period what has been exploited from their people, their heritage and birthright stolen by the foreigners. Several of them also confessed that they attack only the foreigners and not the local citizens due to their stolen resources and impoverishment from the white men. In this case, the foreigners who are enticed to fall into their hook, become prey and are exploited.* **(Informant A, personal communication, April 19, 2018)**

Closely, online crime is seen as a vengeance mission against the whites (Oludayo, 2013). Individuals who are involved in this nature of criminality reported that the 'whites' exploited their fathers to develop their countries while impoverished them. They employ the logic of self-justification to denounce those condemning their activities as well define their preys as being selfish and greedy. On this note, Warner (2011) explained that in Ghana, online criminals do not see online crime as illegal, but as a movement of redemption for social justice over the whites' colonization of their fathers. However, Informant (E) who disagreed with this submission has this to say:

> *Colonial factor or motivation is a misguided reason for online crime in our country. I do not accept that it can encourage people into committing an online crime. The motivation is usually for financial reward because if they engage in it and there are no financial returns, they will easily give up. For example, if an individual lives in Nigeria, but hacks another individual's account in Ghana, was Nigeria colonized by Ghana? Also, if a Nigerian citizen commits an online crime against Malaysian citizen, was Nigeria colonized by Malaysia? In this case, it cannot stand as a logic for the act. The only major motivation is for the financial reward* **(Informant E4, personal communication, April 20, 2018).**

Deducing from the ongoing above, it cannot easily be dismissed that the whites colonized the African citizens and Nigeria in particular. Also, exploited their human and natural resources, but cannot be enough justification to take part in the acts of cyber criminality. Just as Informant (E) noted that sometimes these acts are carried out against fellow African citizens and if considered on colonial justification, why fellow Africans become victims?

- **Revenge Over an Unfair Political System**

In Africa and Nigeria in particular, several citizens argued the political system as not being fair to them. To them, it is enough justification to engage in online criminal activities to get back at the system and as a way of expressing their anger. In line with this, Adeniran (2008) expressed that the illegal use of the cyberspace in Nigeria for criminality can be attributed to the failure of the political leadership and the unfair social system. According to Jainshankar (2011), the online criminals proudly claim that their actions in online space serve as an avenue to get back to the government and its unjust political and social system in an unaggressive manner. On the note of this, informant (B) who contributed to the debate noted that:

> *Politically, there are individuals either because they failed in election or felt being sidelined in the government appointments, they become inspired to hack the government's website online. They usually intend to discredit, blackmail or even make the government less popular. They assume that the fastest way of achieving such intention is by attacking the government online. In some occasions, the signature or the letter headed paper of the presidency is hacked and used to discredit the government or make it unpopular. All these are internet crimes or fraud, just to express their grievances by discrediting the government.* **(Informant B5, personal communication, April 20, 2018).**

Similarly, a number of online crimes are inspired by the agitation for a religious or political ideology. Ideological online criminals attack government owned websites to establish their grievances and promote their political and religious ideologies. In 2001, for example, Cyber-jihad, a body of Indonesian online criminals attacked the website of the police department in their country with the notion to mount pressure on them to free a Muslim militant leader who supposed to be their leader and mentor (Antariksa, 2001). Closely, in 2001, an online criminal in China substituted the Chinese government website with a pornographic movie (De Kloet, 2002). Corroborating the above revelations, Informant (D) observed that:

> *Individuals with an intensive skill of computer and internet facilities frequently apply such skill in fighting any government, social or political system they perceived as unfair and unjust to them. It could be unfair economic, religious, political or social system. For example, in Nigeria, the violent Boko Haram*

[4] Informant (E), a PhD candidate, School of Business, Universiti Utara, Malaysia.

[5] Informant (B) a PhD candidate, School of Government, University Utara, Malaysia.

> *believes that the government and the social system are unfair to sharia teachings. The citizens in the south-south region argued that they are confronting an unfair economic system. Unlike the south-south and the Boko Haram, some agitators do not pick-up arms, they do not protest on the street, they do not cause damage to physical infrastructures, inside their confines or rooms, they use the online space to cause damage to the system. So, it is equally one of the factors that encourage online crime in the country* **(Informant D, personal communication, April 20, 2018).**

The ongoing debate stands as a clear manifestation that the Nigerian political system has been unfair to its citizenry. But, it is not a clear logical conclusion to engage in cybercrime against the state or the government. In some occasions, the political elites equally sponsor online criminality, especially when they need an indicting and vital information to bring down their political opponents. They employ and reward handsomely individuals with an acute cyber skill to do the job for them.

Implication of Cybercrime on the Nigerian Socioeconomic Development

Generally, it is frequently assumed that the entire African states will catch cold if Nigeria sneezes. It is on this submission that Shunubi and Godwin (2017) observed that there is every need to know that if Nigeria declines in its ability to fight the menace 'cybercrime', the entire continent will suffer the disaster economically. The singular honor it enjoys as the giant of Africa, as well as the biggest economy in the African continent will not only remain questionable or vanish away, but will strongly drag the country's honor and international image and reputation into a mud. According to Shonubi and Godwin (2017) who noted that due to the activities of cyber criminals in the country, Nigeria has lost prospective investors who ordinarily would have provided employment for the indigenous people. In addition, they further noted that if active measures are not initiated or not seen to be established by the government, the risk of losing much existing transnational investors in the country will not only hit the nation, but will equally continue to scare away incoming investors with potential investment (Shonubi and Godwin, 2017). In Nigeria, employment rate is very low and if potential investors continue to be scared away due to the activities of these online criminals, it will be bad for the growing population in getting jobs in the future.

Conclusion

As earlier observed, Information Communication Technology (ICT) or simply the internet and computers have become a global trend. This internet according to many, has brought and aided in the development of several critical sectors in societies and nations such as, health, education, transportation and sports. However, it is also observed by some as an agent of many social ills and crimes in the society especially the ones performed online, such as, online theft, fraud, identity theft, money laundering, cyber stalking, online data attack and others. In addition, the above description and submission now makes it to exist as a double-edge sword and become debatable among scholars and commentators. The study found out that cybercrime in Nigeria caused by the rotten political system such as, the actions of the political elites, weak security system, poor dispensation of justice, weak security laws, colonialism as well as vengeance mission against unjust political and economic system.

References

Abdi, O. S. & Mosud, T. A. (2014). Islam and the cyber world. *Journal of education and social research, 4 (6), 513-520.*

Adeniran A.I. (2011). Café culture and heresy of yahoo-boyismin Nigeria in K. Jaishankar (eds) Cyber Criminology: *Exploring Internet Crimes & Criminal Behavior: New York: CRC Press.*

Adeniran, A., I. (2008). The Internet and Emergence of Yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2(2), 368-381.*

Akin, T. (2011). Cybercrime: Response, investigation, and prosecution. *Encyclopedia of Information Assurance* (pp. *749-753). New York: Taylor and Francis*.

Antariksa (2001) “I Am a Thief, Not a Hacker: Indonesia’s Electronic Underground,” *Latitudes Magazine, Retrived April, 2018. p.12–17.181.*

Anah B., Funmi D. and Julius M. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology. VOL. 2 (7). 2225-7217.*

Britz, M. T. (2009). Computer Forensics and Cybercrime. New Jersey: Pearson Education.

Brown, S, D. (2015). Investigating and Prosecuting Cybercrime: Forensic Dependencies and Barriers to Justice*: International Journal of Cyber Criminology, Vol (9)1.*

Bunch, C. (2005). “Not by Degrees: Feminist Theory and Education.” In Kolmar Wendy et“al (ed) *Feminist Theory (2nd ed).* Boston: McGraw Hill.

Castell, M. (1996). The information age: economic, society and culture. The rise of the network society, 1, *Blackwell publishers, Oxford*.

Castells, M. (1999). Information technology, globalization and social development: *United Nations Research Institute for Social Development.* (114).

Cohen, L. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *Amerian Sociological Review, 44, 588-608.*

Dambo, Ezimora and Nwanyanwu (2017). Cyberspace Technology: Cybercrime, Cyber Security and Models of Cyber Solution. *International Journal of Computer Science and Mobile Computing, Vol.6 Issue.11, p. 94-113.*

De Kloet, J. (2010). *China with a cut: globalisation, urban youth and popular music.* Amsterdam University Press. (3)

Ennin, D. A. N. I. E. L. (2015). *Cybercrime in Ghana A Study of Offenders, Victims and the Law* (Doctoral dissertation, University of Ghana).

Frank A. and Michael K. (2015). The Impact of Cybercrime on the Development of Electronic Business in Ghana. *European Journal of Business and Social Sciences, Vol. 4(1) ISSN: 2235 -767X.*

Gbenga, S., Babatope, S. and Bankole, O. (2013). Economic Cost of Cybercrime in Nigeria. Retrieved May 22, 2015, from Paradigim Initiative Nigeria: https://www.pinigeria.org/download/ cybercrimecost.pdf.

Goode, W. J. & Hatt, P. K. (1952). Methods of social research, McGraw-Hill, New York.

Jaishankar, K. (Ed.). (2011). *Cyber criminology: exploring internet crimes and criminal behavior*. CRC Press.

Jaishankar, K. & Halder, D. (2011). Cybercrime and the victimization of women: Laws, rights and regulations. PA, USA: IGI Global. ISBN 978-1-60960-830-9.

Kamini D. (2011). Cybercrime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Science 3(1), 240-259.*

Kshetri N., (2006) “The Simple Economics of Cybercrimes”, IEEE Security and Privacy, 4(1).

Larkin, D. (2006).“Fig hting online crime”, available at: http://usinfo.state.gov/journals/itgic/0306/ijge/larkin.htm (accessed 10 january, 2007).

Magele, T. (2005, February 16/17). E-security in South Africa, White paper prepared for the forgeahead e-security event. Retrived April 22,2018 from www. Forgeahead.co.za/sa.

Mikail I. (2016). Corruption and Nigerian Political Economy. UUM Press

O’Connor. T. (2003). Glee, elation and glory as motives for cybercrime, at the annual meeting of the south criminal justice association, Nashville (March). Available online: http://faculty.ncwc.edu/(toconnor/gleelationglory.htm. Retrieved 11th March, 2018.

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International journal of sociology and anthropology, 6 (3), 116-125.*

Ojedokun, U. A. & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International journal of cyber criminology, 6(2), 1001-1013.*

Ojedokun, A. A. (2005). The evolving sophistication of Internet abuses in Africa. *The International Information & Library Review*, *37*(1), 11-17.

Ojukwu and Shopeju (2010). Elite corruption and the culture of primitive Accumulation in 21st century Nigeria. *International Journal of Peace and Development Studies Vol. 1(2), pp. 15-24, ISSN 2141-2677.*

Oludayo T. (2013). A Spiritual Dimention Cybercrime in Nigeria: The '*Yahoo Plus*' Phenomenon. Human Affairs *23*, 689–705, 2013, DOI: 10.2478/s13374-013-0158-9.

Olowu, D. (2009). Cyber-crimes and the boundaries of domestic legal responses: Case for an Inclusionary Framework for Africa. *Journal of Information, Law and Technology (JILT), 1,* 1-18.

Omotola, Shola J. (2007) "What is this Gender Talk all about after all? Gender, Power and Politics in Contemporary Nigeria." *African Study Monographs* Vol. 28. No. 1.

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.*

Sheila, J. (2010). A new climate for society: theory, culture and society, SAGE publishers, 27 (2-3), 233-253.

Shonubi and Godwin (2017). Cybercrimes in Nigeria and Counter Measures. *International Journal of Innovative Research and Advanced Studies (IJIRAS) Volume 4 Issue 4, ISSN: 2394-4404*

Soderman, K. & Korsell, E. L. (2001). IT-related crime, old crime in a new guise, but new directions too. *Journal of Scandinavian studies in criminology and crime prevention, 2 (1), 5-14.*

Tade, O., & Aliyu, A. (2011). Social Organization of Internet Fraud among University

Undergraduates in Nigeria. *International Journal of Cyber Criminology,* 5 (2), 860-875.

Thomas, J. Holt. & Adam, M. Bossler (2014) An Assessment of the Current State of Cybercrime Scholarship, Deviant Behavior, 35:1, 20-40, DOI: 10.1080/01639625.2013.822209.

Thomas, D. & Loader, E. B. (2000). Cybercrime: law, enforcement, secutiry and surveillance in the information age. London: Routledge, 2000.

UNODC, (2005). United Nations Office on Drugs and Crime: United Nations Publications Sales No. E.05. xi.10. ISBN 92-1-148200-3 (1).

Wall, D. (2001). Cybercrimes and the internet. In D. Wall (ed.) crime and the internet. London: Routledge.

Warner, J. (2011). Understanding Cybercrime in Ghana: A View from Below. *International Journal of Cyber-Criminology 5* (1), 736-749.