Appraisal of an Expanding Global Internet-Related Crime. The Case of Cyber Crime in Nigeria

Yusuf Usman
Bangor University
Bangor, United Kingdom
Email: usmanyusuf126@yahoo.com

Jafar Abdulkadir
Kaduna State University
Kaduna, Nigeria.
Email: abdulrkah@gmail.com

Abstract
This paper has endeavored to look at the concept of cybercrime in terms of what it is and what it is not. As individual countries are making efforts to curb the menace of cybercrime, there are also global efforts aimed at addressing the problem. Cybercrime has been a challenge to the technological development in Nigeria and other nations on earth. The perpetrators of the crime are referring to “yahoo-yahoo boys” in Nigeria, and they make use of the internet to fraud the unexpected victims in foreign transactions mostly in thousands and million dollars. Therefore, the concept of crime, cybercrimes and the tremendous challenges of cybercrimes generally were intensively discussed.

The paper recommends that the fight against cybercrime in Nigeria requires more efforts by the government to educate all agencies that are a concern with security on the knowledge of
ICT, as a basic knowledge to track down the cyber criminals despite their intelligence. The government needs to collaborate with the public or citizen to report any crime act in the society to the law enforcement agencies, and the identifies of the persons report the criminal activity should be treated with confidentiality. Therefore, people should serve as a watch dog because the criminals are living with the people in the society.

1. Introduction
The concept of crime is one of the keenly debated issues in contemporary times between Criminologists, Lawyers, and Sociologists among others. The concept of cybercrime has never been exempted from the debate of what "it is" and what "it is not". The globalisation has affected all sections where virtually everything is linked to a computer that is connected to the internet (Kemp, 2017). The report of April 2017 shows that almost 3.8 billion people across the globe had access to the internet and 93 percent of all internet users mostly access the internet through Android or Operating System Devices. Therefore, observers and experts alike claimed that the number of internet users has increased tenfold from the year 1999 to 2013. Thus, from about 4.4 million users in 2000 to 3.4 billion in 2016, (Kemp, 2017; UNODC, 2013; and Morgan, 2017).

Further, According to McAfee (2013) "that many organizations that have been cybercrime victims do not want to report the problem because they
perceive it as bad for business. Self-selection bias. Organizations that have not detected losses may be more likely to respond to cybercrime surveys than those that have. Or those that have had very public large losses may be more prone to reply than those with moderate unreported losses”.

He further added that on the reasons why some cybercrimes are not reporting that “no standard mechanism for accounting for losses. Sometimes downtime is figured into a mix. Sometimes the cost of buying new equipment in this context, this work examines the global internet with a focus of cybercrime in Nigeria. Rest of this paper is organized as follows. In section 2, Literature review is presented. In section 3, as a part of analyses and discussion several related concepts and their practical implications are examined and discussed whilst conclusion and future work are presented in section 4.

2. Literature Review

There is a growing trend of cybercrime across the globe, this form of crime may have even surpassed the traditional crimes in some European countries as acknowledged by Europol (2016) which stated that the volume, scope and material cost of cybercrime all remain on an upward trend and have reached very high levels. In 2015, according to the Norton Cybersecurity insights report, 594 million people were affected by cybercrime globally. Cybercrime was valued at. Cybercrime according to research conducted by McGuire (2018) is more than just a business, if cybercrime were a
country, it would have the 13th highest gross domestic profit in the world. Meanwhile, cybercrime is quickly developing into a zone of the flourishing market, a regularly expanding number of gangsters are abusing the speed, solace, and mystery of the internet to an extent that the criminals are proving to be far ahead of the game.

UNODC further alleged that in a 'hyper-connected world of tomorrow', it will turn out to be difficult to envision a 'complete wrongdoing', and many any wrongdoing, that does not include electronic proof connected with web convention (IP) network (UNODC, 2013).

There is no gain saying that cybercrime is regarded as the fastest growing market across the globe. According to Morgan (2017), cybercrime is one of the biggest problems with humanity and the greatest threat to every company.

Tannam (2018) also agreed that cybercrime is a booming business. Although, McGuire (2018) argued had argued that the commonly used metaphor of ‘cybercrime as a business’ is no longer adequate to capture the complexities of cybercrime. He suggests a more appropriate metaphor of ‘cybercrime as economy’, a hyper-connected sort of economic agents and economic relationships maintaining criminal revenues at an unprecedented scale.

The internet and technologies of this century are used by the criminals to further their criminal operations in the world. The criminals can easily control the internet to carry out their crimes such as sex trafficking or distributing illicit drugs. In addition, cybercrimes surely have...
social, political, public health, national security, and economic implications (US report, 2012). While, the Internet Society reported that response to cybercrime in contemporary times has been grossly insufficient and the cost is escalating, (Internet Society 2017 Report). However, cybercrime can either be carried out by an individual (individual cybercrime) or by organised groups (organise cybercrime). The effective strategies used by the cybercriminals in Nigeria is a collaboration with the security agents, bank officials, café operators, at national and international networking (Eraye, 2018). It is mostly committed in the present time in an organised manner that is seen as a business model, (EUROPOL, 2016). Despite the difficulty in getting a reliable estimate on how much the cybercrime has cost the world, reports suggest that the costs are in the hundreds of billions of dollars. In 2014, cybercrime business was worth about $500 billion USD (Grant Gross, 2018).

3. Discussion and Analysis
Nigeria as one of the developing nations that have a serious challenge of cybercrime, especially in this technological era. The youths as the leaders of tomorrow have a great role to play for the development of society, like Nigeria. Yet they are in the highest percentage who engaged in cybercrime. In Nigeria, most of the criminals fall within the youths of youthful age, and more fifty percent are students of tertiary institutions. They presently discovered several ways of manipulating the internet for criminal activities.
Therefore, due to inadequate security awareness, the cybercrimes are on the increase every day and may result to the erosion of confidence in genuine Nigerian’s credibility in the world (Okeshola & Adeta, 2013). However, the cybercrimes are being operation in any part of the world.

In Nigeria, the “Yahoo Yahoo boys” are the identified group who are engaged in cybercrimes in Nigeria. According to Okeshola, and Adeta (2013), “yahoo boys” are taking advantage of e-commerce system available on the internet to defraud victims who are mostly foreigners in thousands and sometimes millions of dollars.

In Nigeria, the cybercriminals are known as “yahoo-yahoo” as their way of living and the crimes are persistent, despite all the measures put in place to curtail them in the society (Eraye, 2016). The criminals fraudulently represent themselves as having goods to sell or are involved in a loan scheme project. They may pose to have a financial institution where money can be loaned out to prospective investors. In this regard, many people have been duped or fallen victims.

Despite all the national and international governments efforts to curb or address the cybercrimes have not been successful, because of the strategies and the nature of the crimes keep changing. Therefore, the objective of this paper is to analyse cybercrime in Nigeria, the challenges and the success recorded in the fight against cybercrime.

3.1. Conceptual Review

The definition of cybercrime agreed-upon does not exist. The
scholars and industry expert offered several definitions and its varied in their levels of breadth and specification (CRS, 2012). There are some key elements and questions that are common in almost all the definitions of cybercrime, which include “where do the criminal acts exist in the real and digital worlds and what technologies are involved”? “why are malicious activities initiated? Who is involved in carrying malicious acts? These are some of the questions to be discussed in the following sections.

3.2. Crime as a Concept
According to Lilly and others (2002:1) crime” is a multipart phenomenon that is very interesting and challenging to explain its multipart sides”. The concept according to Lacey and Zedner (2012:159) is so familiar to that it is taken for granted by both the learned and the unlearned. A challenging aspect of the concept of crime is when it is subjected to an analysis that it defies a clear description. The phenomenon of crime has been with humanity from time immemorial and this compelled scholars and writers including those who were rightly classified as criminologists and those who were not to write about crime. They mainly wrote from different viewpoints ranging from religion, medicine and philosophy, Jones (2006:1).

Some scholars such as Burke 2005, Lilly and others 2002, Akers 1991 etc., have defined crime, the crux of most of the definition of crime is the violation of criminal law. However, despite the definitions given to crime, there have been debates over the definitions
which Michalowski (2013) sees as nothing new. The debates on the meaning of the concept of crime are seen as very important because of its relevance to the field of criminology which primarily concerns itself with an objective study of the crime and all its ramifications. It is also seen to concern itself with social and individual backgrounds of crime and with the nature of crime as a societal phenomenon (Lacey and Zedner 2012:160).

3.3. The Cybercrimes
There are companies that are spending lots of money on research to ensure adequate cyber security and among these companies are Herjavec Group; IBM Security; Cisco; Symantec and McAfee. The cyber security companies are investing in research more than institutions of higher learning. There are more definitions given by some of these companies than the ones given by the academics, analysts or commentators. Therefore, the views of the companies on what is cybercrime were fully considered in this paper. Cybercrime is also known as computer crime, hi-tech crime or e-crime.

The general definition of cybercrime is as any crime that is performed by an expert in the use of a computer. Scholars like Carter (1995) defined cybercrime as any activity in which a computer or networks are a tool, a target or place of criminal activity. Cybercrime can be broadly categorised into cyber-dependent crime or cyber-enabled crime.

The term Cybercrime is a frequent world used in our contemporary societies. Cyber as a term is a prefix used to
describe an idea as part of the computer and Information age and “Crime” Can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive. While, Cybercrimes are defined as: "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 (Chatrooms, emails, notice boards and groups) and mobile phones" (Halder & Jaishankar 2012, in Anah Bijik Hassan, Fummi & David Lass, 2012). These types of crimes surely threaten the security of the nation and its entire development.

Similarly, the concept of 'cybercrime' according to the Bedfordshire Police is an 'umbrella' term for lots of different forms of crimes that either take place online or whose technology is a means and/or target for the attack. Cyber dependent crime happens where a digital system is a target as well as means of attack and these include attacks on computer systems to disrupt information technology infrastructures with the objective of stealing data over a network using malware (malicious software programs designed to infiltrate and damage computers without the knowledge of the user).

There is a remarkable development in technology that brought by the invention of the computer and the internet in the world, and they are direct or
indirectly impacting positively on the societies in several ways (Aransiola, Asindemade, & Sc, 2011). Therefore, many opportunities were provided especially for the youths and equally unlimited possibilities for criminals across the globe. The cybercrime as one of the major problems in the world emerged in the last few decades. Thus, UNODC, 2013 sees the concept of cybercrime as an aggregate term and its definition generally rely on the motivation behind utilizing the term. A predetermined number of acts against the privacy, trustworthiness, and accessibility of computer or systems speak profoundly of cybercrime.

Meanwhile, in Nigeria, the category of cyber deviants that are tarnishing the image in cyberspace generally refers to ‘Yahoo-yahoo boys’ (categories of youths in Nigeria who specialize in various types of cybercrime). According to the reports of the Internet Crime Complaint Center, (IC3), “Nigeria ranks third in 2010, among common cybercrimes in Nigerian Internet landscape include hucksters, fraudsters, piracy, and hacking.9,11-14 Some medium for perpetrating cybercrime in Nigeria include cybercafe’s (where bulk tickets are being sold for sending spam mails, some systems dedicated to fraudsters for hacking and sending fraudulent mails and sharing their bandwidth for home use),15,16 fixed wireless Internet facility, which allows fraudsters to perpetrate their acts within the comfort of their homes,8 mobile telephoning,16 use of credit cards and debit cards, postal agencies and banks that facilitate money transfer
facilities, checks, and money orders” (Aransiola et al., 2011). Despite several efforts to curb the menace by the government with the establishment of Economic and Financial Crime Commission (EFCC), the partnership with Microsoft Company, to address and sponsor the bill on cybercrime to address the issue, yet cybercrime has proved particularly resilient to remedial action (Aransiola et al., 2011).

The 2017 Norton Cyber Security Insights Report defined cybercrime as, but not limited to, “a number of specific actions, including identity theft, credit card fraud or having your account password compromised” (Symantec, 2018:28). The National Crime Agency sees cybercrime as a specialist criminal groups that target individuals, businesses both small and large to steal personal information to profit from the compromised data available to them.

4. Conclusion and Future Work

Cyber crime in our contemporary world has become a prominent practice, and fighting it requires security experts in IT on how to deal with the menace squarely. Therefore, this paper recommends that the government as a matter of urgency should provide intensive training for law enforcement agencies regularly on ICT to tackle cyber criminals. This will be supported by enacting a strong law on cybercrimes in the country by the legislative arm of government. Then more recruitments are required for the government to provide employment to our graduates,
this would serve a strategy to reduce the unemployment and poverty in the country.

There is a need for the government to educate all agencies that are a concern with security on the knowledge of ICT, as a basic knowledge to track down the cyber criminals despite their intelligence. The government needs to collaborate with the public or citizen to report any crime act in the society to the law enforcement agencies, and the identification of the persons report the criminal activity should be treated with confidentiality. Therefore, people should serve as a watchdog because the criminal living with the people in the society.

The ICT users should keep on updating their knowledge on any new changes in technology and the new strategy of criminalities.

Equally, internet users should be security conscious and not reveal their financial information to others without any strong reasons for that.

In future, further research may focus on examine some of the presented concepts in a practical environment.

References


3. Eraye, M. C. (2016). Socioeconomic Lifestyles of the


cyber-crime  (Accessed on 21/07/2018)