A review of Cybercrime in Sub-Saharan Africa: A Study Cameroon and Nigeria

Regina Ekoa Mbella Mungwe

Abstract

Since the arrival of the internet in Sub-Saharan Africa, technology has emerged with different creations all over the continent. (for example, Automated Teller Machines (ATM), Communication Networks, Laptops and other cell phone devices). This has presented both opportunities for progress and exploitation for criminal activities. Countries like Cameroon and Nigeria have millions of people using the internet every day. Over 47.7% of Nigeria's population and 25% of Cameroon's population used the internet in 2017 (Internet World Stats: Internet Users in Africa, June 2017). The internet has provided a new arena for criminal activities in these two countries. Online scams and ATM hacks challenges the local notion of criminology, establishing contemporary methods of theft and crime in these countries.

In this paper we discuss some internet-based crimes (online scams and ATM hacks), trending in some Sub-Saharan African countries (Nigeria and Cameroon), reviewing the socio-economic consequences, to the government, individuals and Private Institutions, and Individuals. The paper reviews the current status of fighting cybercrime in Nigeria and Cameroon and observes that these countries do not have adequate professional expertise and relevant tools to combat cybercrime which is the main cause of its continuous growth. It reviews the existence of Internet Technology and observes that; as internet users increases, cybercrime increases.

Key words: Cybercrime, Hacks, Online Scams, Sub-Saharan Africa, Internet.

Methodology

This paper explains how Cameroon and Nigeria are expanding in Cybercrime activities and that this expansion is because they do not have the available tools, equipment, professional expertise to fight against these activities. This paper is explanatory in nature. The research adopts a qualitative method that explains how increase in internet technology in Nigeria and Cameroon has created different forms cybercrimes. This paper reviewed published articles of peer reviewed journals and made references to books from electronic database: Google scholar, Science Direct, EBSCO, SCOPUS. The search terms include: Cybercrime, ATM Hacks, Online Scams, Sub-Saharan Africa, Internet

Introduction

Many definitions have evolved, trying to define cybercrime; Peter Grabosky's using a metaphor describes cybercrime as a case of 'old wine in new bottles' (Grabosky 2001). Thomas and Loader (2000:3) defines cybercrime as 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks'. It involves crimes that target computer networks or devices directly, and crimes that are facilitated by computer networks or devices. The Council of Europe's Cybercrime Treaty defines "Cybercrime" as offences ranging from criminal activity against data to content and copyright infringement. In general, cybercrime may be referred to as an activity that consists in using systems, computer networks in general and the Internet in particular to perpetuate crimes prohibited by law. Sub-Saharan countries (Nigeria and Cameroon), fall among the list of countries worst affected by cybercrime in Africa. Out of the ten regions of Cameroon, the Douala region (Douala), is noted for high cybercrime rates. Cybercrime in Douala, Cameroon has been manifested in several ways amongst which the Automated Teller Machine (ATM) hacks and sim box fraud are fast developing in the center region of the country. SIM box or GSM gateway is a type of box equipped with SIM cards connected to high speed internet, which fraudulently transforms international calls to appear as local calls. For the user who receives a bypass call in this manner, the conversation is often of poor quality with a lot of interference and disruptions. The dialed number that displays on the phone screen is often a local number instead of an international number. Moreover, the correspondent cannot receive call-back. According to the director general of the National Agency for Information and communication technology (ANTIC), local banks lost over 3 billion FCFA in 2015 through ATM card hacks. With the use of special devices inserted in automated teller machines, local banks lost over 3 billion FCFA through the fraudulent act of hacking magnetic. "After pirating the electronic bank card details of unsuspecting customers, criminals then go to ATMs and withdraw money from the bank accounts of their victims,". The consequences of ATM cards hack however had far lesser impact compared to the destruction caused with the use of sim boxes in the telecommunication sector. The problem of sim box fraud had a tremendous effect in 2015 when over 18 billion FCFA was lost by the four telecom operators (Nexttel, MTN, Orange and Camtel). Cameroon's treasury also incurred a 4 billion FCFA loss in 2015 because of cybercrime. Several steps have been taking to fight against cybercrime in Cameroon, including partnering with some developed world countries such as America and some American institutions. A Centre for Digital Forensic and Cyber Security was set up under the University of Buea in partnership with the Cameroon Ministry of Posts and Telecommunications and the University of Bloomsburg in the US. This center trains young Cameroonians on how to protect the country's cyberspace. The category and nature of cybercrime in Nigeria is endless. Nigeria ranks one of the top most African country concentration with cyber criminals, also called 'Yahoo boys' s (Adeniran 2008; Longe and Chimeke 2008; Tade and Aliyu 2011). Most of these cyber criminals include young people and university students (Adeniran 2008; Tade and Aliyu 2011). They engage in fraudulent activities such as sending spam emails to deceive people which at the end they collect money and you become a victim. Other forms of cybercrime activities include; identity theft, desktop counterfeiting, internet chat room, cyber harassment, fraudulent electronic mails, Automated Teller Machine spoofing, pornography, piracy, hacking, phishing and spamming. Today, the

economy of most nations in the world is accessible through the aid of electronic through the internet. The increasing rates of cyber criminality in the society have become a strong threat to Nigeria's e-commerce growth. Even the country's reputation internationally has been affected because of the continuous rise of cybercrime.

Despite the efforts made to eliminate cyber crime, cyber crime perpetration has steadily remained on the rise with an increase in Internet diffusion in Cameroon. This research will to ask the following questions: what is the extent of (internet based) ATM attacks in the Douala area? what is the extent of (internet based) Sim box attacks in the Douala area? Are attacks on the increase? Extent of loses to individual government and private Industry.

Cybercrime in Cameroon

Until 1992, Cameroon still used the traditional media devices such as press, radio, television, based on the star model. Telephone networks provided a one on one communication. Throughout 1996, internet was regularly mentioned in the speeches of Cameroonian officials. In February 1997 and April 1999 respectively, the internet arrived Cameroon with an American firm AT&T, and with an agreement with Teleglobe, a Canadian company, which installed a second channel of arrival of the internet in Douala, Cameroon. Despite the arrival and the steadily growing Internet penetration rate (which averaged 14 percent growth per year between 2007 and 2011), Cameroon remained the least connected country in the world with only 5.5% of its population online in 2013. Even though the introduction of the internet brought development in the industrialized world, Cameroon only benefited narrowly from this development, due to weak technology. According to the International Telecommunication Union, only 1,006,494 out of the 21,700,000-estimated total population of Cameroon make use of the internet.

The arrival of hyperspace in Cameroon, nevertheless, presented a wide range of advantages and development that was lacking during its absence. In 2012, Cameroon could boast of over 10,207 internet hosts and was ranked the number 113th in the world. With regards to communication, data of 2012 figures revealed that over 737,400 fixed phone lines were in use compared to 13.1 million mobile phones (CIA World Factbook). The number off telecommunication networks increased to four over the two in 2010. Douala and Yaounde, together representing about 40% of the country's population, have more than 90% of all connections (BuddeComm,2007).

Until 2012 Cameroon operated only two communication networks (MTN and Orange). The growth in the telecommunication sector gave birth to the four telecommunication networks currently operating in Cameroon (MTN Cameroon, Orange Cameroon, Camtel and Nexttel). Competition amongst telecommunication sectors remains high as every sector is proving new forms of improvement and development to boost their services. Wireless internet service became available in 2001. However, Camtel the sole provider of fixed lines in Cameroon continues to deteriorate because of lack of investment for extension and maintenance.

The Cameroons today have recorded many positive achievements since the existence of hyperspace. Madiba Oliver a born Cameroonian, invented the Kiro's game in 2003, also known as the Kiro's studio and has been making huge financial benefits since then. Kiro'o Games is privately held video game, animation, development and publishing company based in Cameroon and has its headquarter in Yaoundé. Since April 10, 2015, Kiro'o Games announces the closing of its investment funds of 182,504 euros and is projected into the future of becoming an actual company.

Also, Arthur Zang, who is a Cameroonian invented the patented touchscreen Cardio Pad, also called Africa's first medical tablet. It permits health-care workers in rural areas to send the results of cardiac tests to heart specialists via a mobile-phone connection. Development in recent information and communications technologies (ICT), improvement in high-speed internet, are changing the way companies do business, transforming public service delivery and democratizing innovation. This has improved the working and living conditions of both customers and employees of the banking and health sectors.

The wide range of internet users in Cameroon continues to expand daily. Data reveals that young and educated people have more access to the internet, with the male gender dominating. 47.5% of internet user's respondents are male. 44.3% are under 30 years old. Regarding education, 57.6% of internet user's respondents have only primary or lower secondary education, 12.2% completed "high school", and 7.1% have a university degree. Regarding the urban repartition, sample shows that 80.6% of the internet user's respondents live in Douala. Douala is not only the largest city in Cameroon but also the economic capital of Cameroon with different business activities ongoing in the region.

The primary initiative of the arrival of internet in Cameroon was to expose the country to better opportunities, increase technology for progress. However, today this view is taking a different dimension. Internet arrival in Cameroon has not just provided an opportunity for development but has also presented a ground for exploitation for criminal activities. There is a tremendous shift from the local knowledge of criminology to cybercrime. Cybercrimes locally called "scamming", increases daily in Cameroon with new forms of attacks such as ATM hacks, simbox fraud, wildlife fraud, visa fraud and many more. Advanced technology is more of a threat to the Cameroons with ATM cards fraud and simbox fraud fast developing in different regions.

Data survey records of cybercrime activities from national and international authorities involving Cameroonians shows recent arrests of some cybercrime criminals. In a crackdown operation carried out by wildlife officials in the Litoral Regional Delegation of Forestry and wildlife and the Judicial police with technical assistance from The Last Great Ape Organization (LAGA), three cybercriminals were arrested in Akwa Douala, Cameroon during carrying out cyber theft that involved the sales of two lions and two cheetah cubs.

Three Cameroon nationals (Lawrence Njabon Francis 37yrs, Lawrence Nana Tchakounte 26 yrs, and Emmenuel Nkwate 31yrs), residing in the US on Student visas were recently arrested for cybercrime activities. According to police authorities, large amounts of money were wired through Western Union and MoneyGram at various locations in Butler, Lawrence and Mercer counties. These cybercriminals displayed puppies on the internet for sale, received huge sums of money from buyers and never made any delivery.

FIGURE 1.1

Year	Internet Users**	Penetration (% of Pop)	Total Population	Non-Users (Internet less)	1Y User Change	1Y User Change	Population Change
2016*	**4,311,178**	18 %	23,924,407	19,613,229	16.5 %	609,593	2.49 %
2015*	**3,701,585**	15.9 %	23,344,179	19,642,594	47.8 %	1,196,553	2.51 %
2014	**2,505,032**	11 %	22,773,014	20,267,982	76.2 %	1,083,517	2.53 %
2013	**1,421,515**	6.4 %	22,211,166	20,789,651	15.2 %	187,143	2.55 %
2012	**1,234,371**	5.7 %	21,659,488	20,425,117	16.9 %	178,418	2.56 %
2011	**1,055,953**	5 %	21,119,065	20,063,112	19.3 %	170,555	2.57 %
2010	**885,399**	4.3 %	20,590,666	19,705,267	14.9 %	114,537	2.57 %
2009	**770,862**	3.8 %	20,074,522	19,303,660	15.9 %	105,467	2.58 %
2008	**665,394**	3.4 %	19,570,418	18,905,024	19 %	106,406	2.58 %
2007	**558,988**	2.9 %	19,078,100	18,519,112	48.2 %	181,700	2.59 %
2006	**377,288**	2 %	18,597,109	18,219,821	48.4 %	123,029	2.59 %
2005	**254,259**	1.4 %	18,126,999	17,872,740	47.4 %	81,810	2.6 %
2004	**172,449**	1 %	17,667,576	17,495,127	70.4 %	71,269	2.61 %
2003	**101,180**	0.6 %	17,218,591	17,117,411	67.1 %	40,628	2.62 %

2002	**60,552**	0.4 %	16,779,434	16,718,882	33.7 %	15,256	2.63 %
2001	**45,296**	0.3 %	16,349,364	16,304,068	12.8 %	5,139	2.65 %
2000	**40,157**	0.3 %	15,927,713	15,887,556	100.5 %	20,133	2.67 %

Increased digital awareness and technology has also led to increased hyperspace users in the Cameroons. Figure 1.1 shows the rapid increase of hyperspace users in Cameroon since the year 2000. During 2016, internet access increased by 18% in Cameroon. There was an 18.2% growth from the 2000-2016.Population of internet users expanded from 40,157 users in the year 2000 to 4,311,178 users in 2016. This growth could relate to the increase in internet usage Longe and Chiemeke (2008).

Cybercrime in Nigeria

Until 2001, the phenomenon of Internet criminal fraud was not globally associated with Nigeria. The arrival of internet in Nigeria has enabled criminals and their activities to increase the number of their unsuspecting victims and this invariably makes it difficult to track them down (Aghatise, 2006). Cybercrime is now a serious problem in Nigeria ranks third of the top ten cyber crime hot spots in the world by a 2009 Internet Crime Report (National White-Collar Crime Centre and the Federal Bureau of Investigation, 2010). Four years in a roll (2006, 2007, 2008 and 2009) Nigeria ranks world cyber crime perpetrator countries (National White-Collar Crime Centre and the Federal Bureau of Investigation, 2010). Emerging evidence shows that cybercrime criminals in Nigeria focus exclusively on cyber-fraud (Ojedokun and Eraye, 2012; Smith, 2008; Tade and Aliyu, 2011; Adogame, 2007; Doyon-Martin, 2015; Chawki et al., 2015b; Akpome, 2015; Ellis, 2016; Ibrahim, 2016). The focus is more on economic benefits. Most Nigerian youths are actively engaged in internet fraud and it is growing in leaps and bounds, winning more souls from partner agencies, who now contribute to its successful execution. Mbaskei's publication on "Cybercrimes: Effect on Youth Development" reveals how secret agents of the UPS (United Parcel Service) recorded scam with a face value of $2.1billion (equivalent N252 billion) in Lagos. According to Ellen (2009)'s survey of 113 financial services firms, mass compromise of merchant networks and card processors is viewed as the main cause of payment-card fraud.

Increase in developed information technology (IT) infrastructure in the sub region is amongst the main reasons why we have these crimes in Nigeria today. Improvements in global telecommunication infrastructure, including computers, mobile phones, and the Internet, have brought about major transformation in world communication. Internet facilities have enabled all these devices to be accessed from anywhere in the world (homes, offices, and cyber cafes). Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims (Clough, 2010). Commonly known as "Yahoo Boys", refers to the name given to every Nigeria Cyber Criminal. Even the name '419' was adopted (to refer to cyber criminals) after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud. Advanced technology within the financial institution sectors in Nigeria have generated automated Teller Machines (ATM). These machines provide innovative service delivery mode that offers diversified financial services like cash withdrawal, funds transfer, cash deposits, payment of utility and credit card bills, cheque book requests, and other financial enquiries. Muhammad (2009). Access to these ATM machines are usually in most parts of the country 24 hours. Despite the enormous benefits provided by these machines, other people are using it as a ground for cyber hacks. ATM fraud is now a trending cybercriminal activity in Nigerian. ATM system has contributed to the increasing rate of fraud in the Nigerian banking sector.

The need for cybersecurity is becoming increasingly important due to our dependence on Information and Communication Technology (ICT) across all aspects of our cyber physical society. Cybersecurity is essential for individuals, for public and non-public organizations, however guaranteeing security often proves to be difficult. Nigeria cybercrime has evolved from silly spray-and-spray email spam campaigns to refined con games that target large business organizations. Over 8,400 malwares sample was derived from Nigeria's scam emails from July

2014 to June 2016. In Nigeria today, cyber security is now elevated to the level of being handled by the Presidency through the Office of the National Security Adviser (ONSA). According to the Office of the Nigerian National Security Adviser (2014), "National Cyber Security Strategy (NCSS) was created to be the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community".

Over the past decades, cyber security has been a major concern to many nations across Sub-Saharan Africa. Today, computers and the internet represent the fastest growing technology tools used by criminals to comprise sensitive data, networks and systems thereby causing extensive loss to national economies including posing challenging threats of cyber terrorism among nations. According to a speech presented by the Minister of Communications, Adebayo Shittu, 'The government recorded the loss of over $450 million dollars to 3,500 cyberattacks in 2015'. Between the years 2013 and 2014, fraud on e-payment platform of the Nigerian banking sector increased by 183 per cent (2014 Annual report of the Nigeria Deposit Insurance Corporation). The estimated cost of cybercrime to Nigeria was at about 0.08 per cent of their GDP, representing about N127 billion (2014 report by the Centre for Strategic and International Studies, UK). According to the Office of the National Security Adviser (ONSA) Nigeria, over N159 billion was lost by Nigerians through online scam and identity theft between 2000 and 2013 with 2,175 websites defaced within the same period. "Cyber espionage and stealing individuals" personal information was estimated to have affected more than 800 million people during 2013. Report revealed that 25% of the cybercrimes in Nigeria are unresolved and that 7.5% of the world's hackers are Nigerians (Information Security Society of Nigeria, 2015).

Combating Cybercrime

Cybercrime as stated in Longe and Chiemeke (2008) remains difficult to overcome as it attempts to hide itself in the face of development. Despite all resources put in place to combat cybercrime, in some countries like Nigeria, it remains a social problem (Ribadu, 2007). Findings from the 2002 Computer Crime and Security Survey conducted by Computer Security Institute and the U.S. Federal Bureau of Investigation, show an upward trend in the increase of cybercrime that demonstrated the need to review existing approaches to fighting cyber criminals. Cybercrime activities have become so serious that many countries are adopting several defensive approaches (regulating the use of the Internet, setting up new organizations dealing with cybercrime issues, and developing new forensics technologies). The difficulty in fighting Cyber Crimes today can be related to the fact that Cyber Crimes have been in existence for only as long as the cyber space exists. This explains the unpreparedness of society and the world in general towards combating them. A major problem that acts as a barrier for combating cybercrime in these two countries is the collaboration of cyber criminals with different financial institutions and law enforcement officers. Law enforcement officers work together with cyber criminals, preventing the strict implementation of state laws. In addition, financial institutions, facilitate this form of criminality by allowing cash the cyber criminals to freely carry out their financial transactions without notifying law enforcement. A huge percentage of financial institutions work hand in hand with cyber criminals. Financial transactions such as western union transfer, money-gram transfer and bank to bank wiring are been made on daily basis with the help of financial institutions. Several laws have been passed and law enforcement agency created to stop cybercriminals.

1. **Act of 2006, the Money Laundering Act of 2004 section 12(1) (c) - (d),** the Economic and Financial Crime Commission Act of 2005, and the Evidence Act of 1948; was created to address the menace of cybercrime directly. These laws enacted to combat cybercrime and ensure cybersecurity.
2. Advance Fee Fraud and Related Offences Act 2006 According to Section 23 of the advance fee fraud Act (Laws of the Federation of Nigeria, 2006): False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.
3. **The Cybercrimes Act of 2015.** Act 2015 has created a legal, regulatory and institutional framework that prohibits, prevents, detects, investigates and prosecute cyber criminals and other related matters. This Act of 2015 engenders a platform for cyber security and in turn, ensures the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights as well as preservation and protection of the critical national information. Development of the Nigeria's National Cybersecurity Policy and Strategy documents; Establishment of the Nigeria's Cybercrime Act 2015; Establishment of the National Cyber Monitoring Centre, which includes the Nigeria's National Computer Emergency Response Team (ngCERT) Operation Center; Establishment of National Computer Forensics Lab for cybercrime investigations by all security, intelligence and law enforcement agencies and establishment of an effective collaboration mechanism with international cybersecurity organizations across the globe.

4. **The Economic and Financial Crimes Commission (EFCC)**. This Law enforcement agency was created in Nigeria (2003) to investigate financial crimes such as advance fee fraud (419 fraud) and money laundering. This Commission has the authority for identifying, tracing, freezing, confiscating, or seizing proceeds derived from terrorist activities. The EFCC can fine, seize assets and give up to five years imprisonment depending on the nature and gravity of the offence (Ribadu, 2006, p. 4). The EFCC is partnering with worldwide Law enforcement agencies such as FBI, INTERPOL in creating an excellent workforce (Ribadu, 2006, p. 8).
5. International Criminal Police Congress was created in 1914 and by 1956 was changed to INTERPOL. This is the world's largest international police organization, with 192-member countries. Its primary objective is to enable police around the world to work together to make the world a safer place. Their high-tech infrastructure of technical and operational support helps meet the growing challenges of fighting crime in the 21st century. Interpol has been very instrumental in combating cyber criminals all over the world including Cameroon and Nigeria. Every year Interpol produces reports of criminal activities all around the world.
6. In Cameroon, the National Agency for information and Communication Technology (ANTIC) was created on April 8th, 2002 by a Presidential Decree of No 2002/092/PR. ANTIC facilitates and accelerate the uptake of ICTs in Cameroon so that they can contribute to the development of the country. This Agency is responsible for the regulation of electronic security activities in collaboration with the Telecommunications Regulatory Board.
7. LAW N° 2010/012 of 21 December 2010 relating to Cybersecurity and Cyber Criminality in Cameroon was created by the Cameroon legislation to governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon.

Policy Recommendation

"Criminal behavior is a complex affair that requires specialized, lower-level theories to adequately deal with the specific types of human conduct and social situations that are said to be characteristic of criminality or deviance" Chris (2007, 689). All forms of cyber assisted criminal activities (cyber stalking, cyber bullying, identity theft, computer-aided forgery, email scams, virus dissemination and malware attacks), is prevailing today in our Sub-Saharan African countries with little or no resources, set aside to provide long-lasting solutions. An effective and operational cyber security policy and strategy would facilitate the attainment of a reduced possibility of successful cyber incidents on a national level. Good cyber security policies would provide these countries with the capacity to prevent such attacks and swiftly address them in the event of their occurrence.

- West Africa must invest in cybersecurity training and awareness. One of the global companies working in the policy, technology and management aspects of cybersecurity and digital forensics covering the region is First Atlantic Cybersecurity Institute. Governments, schools and businesses can take advantage of the training programs provided by Fancyber.
- Lack of specialists (incompetent police). Lack of increase effectiveness and efficiency of cybercrime analysis and investigation with the help of new technologies and cybercrime specialists. It is difficult to prove cybercrime in Nigeria. This is as a result of lack of traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols.
- Cyber Security Awareness. organizations should take the (financial) plunge and either train their employees on security for the first time or double down on more robust and ongoing security awareness programs (, 2017 cybercrime report, Cyber Ventures). This has been the most under spent sector of the cyber security industry.
- There is lack of cybercrime legislation (laws) that specifically meant for cyber criminality. Available criminal laws such as; the Advance Fee Fraud Act of 2006, the Money Laundering Act of 2004 section 12(1) (c) - (d), the Economic and Financial Crime Commission Act of 2005, and the Evidence Act of 1948; are insufficient to address the increase rate of cyber criminality. Therefore, appropriate cyberlaw must be put in place urgently to tackle the activities of cybercrime and ensure cybersecurity. law enforcement fails to keep up with technological advances to prevent cybercrime (Jaishankar, Pang & Hyde, 2008; Choi, 2006), due to poor infrastructure. Anti-hacking laws, still operate under traditional approaches to crime containment. As a result, these laws have been ineffective (Sharma, 2007).
- Review of Learning Curriculum. Most university curriculums of study fail to include cybercrime related courses that may highlight to the students the existence and dangers. They do not understand the concept of 'cybersecurity'. Most internet users in Cameroon and Nigeria, use the internet without knowing the dangers it poses. The big question is; How do you fight to eliminate a problem, without first identifying the problem? The study therefore, recommends that curriculum which will include courses on cybercrime, cyber management and its prevention should be introduced to both tertiary institutions, secondary schools, and higher education to take care of the present social changes. Continuous awareness of the threat posed by cybersecurity will; enable the reduction of people's vulnerability of their Information and Communication Technology (ICT)

systems and networks, enable individuals as well as institutions to develop and nurture a culture of cyber security knowledge, and enable a wide understanding of the current trends in IT/cybercrime, and develop achievable solutions.

- An effective management strategy to prevent the risk of cybercrime will require government, organizations, private sector and civil society to cooperate and collaborate with Federal government developing "ways of countering the threats" including the review of the Evidence Act 2011 to accept electronic evidences in court.
- Organizing National Cybersecurity Capacity Building Workshop programs to serve as a timely education and awareness intervention for security and law enforcement and other ICT regulatory agencies in these countries for enhancing the security of each country's cyberspace so as to checkmate cybercrime promptly.
- Address Verification System: Address Verification System (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like United States) matches the address where the cardholder's billing statements are mailed. (Copied)
- Address Verification System: Address Verification System (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like United States) matches the address where the cardholder's billing statements are mailed.
- Cyber Ethics and Cyber Legislation Laws: Cyber ethics and cyber laws should be formulated to stop cyber-crimes. Strict adherence to these laws reduce the tension in the cyberspace caused by cyber criminals. Security software like anti viruses and anti-spywares should be installed on all computers. Internet Service Providers should also provide high level of security at their servers to keep their clients secure from all types of viruses and malicious programs.
- A possible means of curbing cybercrime activities will include enactment of enabling laws to guarantee the legality of online transactions.

References

Okonigene R. E., Adekanle B (2010) "Cyber Crime in Nigeria" *Business Intelligence Journal* Vol.3 (1), pp.93-98. (https://s3.amazonaws.com/academia.edu.documents/31188480/BIJ-Vol3No1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1519548449&Signature=YudEhYt3MWYCvIIFAx9l5WHazmQ%3D&response-content-disposition=inline%3B%20filename%3DLevel_of_job_satisfaction_and_intent_to.pdf#page=95)

Majid Yar (2005) "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory" European Journal of Criminology Vol. 2 (4), pp. 407–427 (https://s3.amazonaws.com/academia.edu.documents/30754465/10.1.1.89.1019.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1519549683&Signature=DL9Ho3TPTV2bI6qe6XUJX3oK0Jo%3D&response-content-disposition=inline%3B%20filename%3DThe_Novelty_of_Cybercrime.pdf)

Gordon S., Ford R (2006) "On the definition and classification of cybercrime" *J Comput Virol*, Vol. 2, pp 13–20.

Wingyan C., Hsinchun C., Weiping C., Shihchieh C. (2004) "Fighting cybercrime: a review and the Taiwan experience" *Elsevier*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.72.1147&rep=rep1&type=pdf (Sunday February 25th, 2018)

Anah B.H., Funmi D. L., Makinde J. (2012) "Cybercrime in Nigeria: Causes, Effects and the Way Out" *ARPN Journal of Science and Technology*, Vol 2(7), pp 626-631

OLUDAYO TADE 2013 "A SPIRITUAL DIMENSION TO CYBERCRIME IN NIGERIA: THE 'YAHOO PLUS' PHENOMENON" *HUMAN AFFAIRS*, Vol 23, pp 689–705

Odumesi J.O. (2014) "A socio-technological analysis of cybercrime and cyber security in Nigeria" *International Journal of Sociology and Anthropology*, Vol. 6(3), pp. 116-125

Folashade B. O., Abimbola K. A. (2013) "The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria" American International Journal of Contemporary Research Vol. 3(9), pp. 98-114

Ibikunle F., Eweniyi O., (2013) "APPROACH TO CYBER SECURITY ISSUES IN NIGERIA: CHALLENGES AND SOLUTION" International Journal of Cognitive Research in science, engineering and education, Vol.1(1), Retrieved from www.ijcrsee.com (Tuesday 27th February, 2018)

Killian C.N. Cameroon's dilemma in fighting cybercrime. African Independent (6th April 2016). Received from https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265

ANTIC. Cyber-Criminality Wreaking Havoc in Cameroon. Business Cameroon (4th March 2016). Received from http://www.businessincameroon.com/telecom/0403-6033-cyber-criminality-wreaking-havoc-in-cameroon-according-to-antic

Akuta E. (2014). Using the Cost Element Model to Explain Perpetrators' Perceptions to Combat Cybercrime in Cameroon: A Structural Equation Model Approach. J. Res. Peace

Gend. Dev. 4(2):27-37. Received from http://www.interesjournals.org/full-articles/using-the-cost-element-model-to-explain-perpetrators-perceptions-to-combat-cybercrime-in-cameroon-a-structural-equation-model-approach.pdf?view=inline

Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmalleger, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall. Received from http://www.jaishankar.org/theory.html

Nashipu J. Internet Development in Africa: The Case of Cameroon. Received from https://www.isoc.org/inet97/proceedings/E4/E4_1.HTM

Cameroon web. Science and Technology. Received from http://www.cameroonweb.com/CameroonHomePage/technology/

Lange. P. The Case for "Open Access" Communications Infrastructure in Africa: The SAT-3/WASC cable– Cameroon Case Study. Received from http://gb1.apc.org/pt-br/system/files/APC_SAT3Cameroon_20080516.pdf

Penard. T, Poussing. N, Mukoko. B, Tamokwe. G.B.P. (2015). Internet adoption and usage patterns in Africa: Evidence from Cameroon. Technology in Society 42 (2015) 71e80. Received from http://s3.amazonaws.com/academia.edu.documents/42649106/Internet_adoption_and_usage_patterns_in_20160213-7352-up27cq.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1500104639&Signature=4M%2B74z2pES1kLkFycNLNZKtgNxw%3D&response-content-

Cite as: Akinyokun, O. K., Alese, B. K., Oluwadare, S. A., Iyare, O., & Iwasokun, G. B. (2015). "Contributory indices to cybercrime activities in Nigeria" Proceedings of Informing Science & IT Education Conference (InSITE), pp.59-77.

Nnameziri P N., Uzodinma E.M I., Uzoma O O. (2013) "Cyber Crime Victimization among Internet active Nigerians: An Analysis of Socio Demographic Correlates" *International Journal of Criminal Justice Sciences*, Vol. 8 (2), pp 225–234.

Kshetri, N. (2010) "Diffusion and Effects of Cybercrime in Developing Economies," *Third World Quarterly*, 31(7), pp. 1057 – 1079.

Òkè R. O. M. (2012) "Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT)" *The Journal of Philosophy, Science & Law*, Vol 12(1), pp. 1-14.

Oluwafemi O., Agada D. O. (2015) "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis" *International Journal of Cyber Criminology*, Vol. 9 (1), pp. 120–143

Suleman Ibrahim (2016) "Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals" International Journal of Law, Crime and Justice, Vol 47, December 2016, pp 44-57.

Samuel Sunday Fasanmi et al. (2014) "Influence of Psycho-social Factors on Youths' Attitude towards Internet Fraud in Nigeria" *Procedia - Social and Behavioral Sciences*, Vol 182, pp 110 – 115. https://ac.els-cdn.com/S1877042815030207/1-s2.0-S1877042815030207-

main.pdf?_tid=f4f4d9a7-77a1-4fd5-9793-d3279abc83f2&acdnat=1520975376_8d690548569c5ce90f78b2ed0989cd70

H. de Bruijn, M. Janssen. (2017) "Building cybersecurity awareness: The need for evidence-based

framing strategies" *Government Information Quarterly*, Vol 34, pp 1–7.

Olusola M., Ogunlere S., Ayinde S., Adekunle Y. (2013) "Cyber Crimes and Cyber Laws in Nigeria" *The International Journal of Engineering and Science (IJES)*, Vol 2(4) pp 19-25.

Olubukola S. A. (2017) "Cybercrime and Poverty in Nigeria" Canadian Social Science Vol. 13(4), 2017, pp. 19-29.

Abdur Rahman Alfa Shaban. (2016) Africanews. Retrieved from http://www.africanews.com/2016/11/10/nigeria-suffered-3500-cyber-attacks-in-2015-lost-450m// (Monday 19th March, 2018)

Babagana Munguno. (2016) "Nigeria Loses over N127bn Annually through Cybercrime" THIS0DAY. Retrieved from https://www.thisdaylive.com/index.php/2016/04/19/nigeria-loses-over-n127bn-annually-through-cybercrime/ (Monday 19th March, 2018).

Comms week (2015) "NSA Partners Microsoft on Curbing Cybercrime Breaches" Retrieved from http://nigeriacommunicationsweek.com.ng/nsa-partners-microsoft-on-curbing-cybercrime-breaches/ (Monday 19th March, 2018)

Ibikunle F., Eweniyi O. (2013) "APPROACH TO CYBER SECURITY ISSUES IN NIGERIA: CHALLENGES AND SOLUTION" *International Journal of Cognitive Research in science, engineering and education* Vol. 1(1).

Chinedu N. Ogbuji et Al., (2012) "Analysis of the Negative Effects of the Automated Teller Machine (ATM) as a Channel for Delivering Banking Services in Nigeria" *International Journal of Business and Management*, Vol. 7(7), pp 180-190.

Chawki M. (2009) "Nigeria Tackles Advance Fee Fraud" Journal of Information Law & Technology. Retrieved from: https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/chawki/ (Monday 26th March 2018)

Steve Morgan, '2017 Cybercrime Report' Cyber Ventures. Retrieved from : https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf (Monday 26th March, 2018).

Daramola Adebayo. "Nigeria loses N127b annually to Cyber Crime – Buhari" Daily Nigeria Post. (posted March 8, 2017). Retrieved from: http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crime-buhari%E2%80%8E/ (Monday 26th March 2018).

21 OF 012/2010LAW N° DECEMBER 2010 RELATING TO CYBERSECURITY AND CYBER CRIMINALITY IN CAMEROON. Retrieved from: https://www.antic.cm/images/stories/laws/Law%20relating%20to%20cybersecurity%20and%20cybercriminality%20in%20Cameroon.pdf (Monday 26th March, 2018).

National Agency for information and Communication Technology (ANTIC) 8th April 2002. Retrieved from: https://www.antic.cm/index.php/en/ict-info/laws-governing-icts.html (Monday 26th March, 2018).