Journal of Information Technology Impact
Vol. 9, No. 3, pp. 155-172, 2009

Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives

Olumide Longe[1] Oneurine Ngwa[2] Friday Wada[3] Victor Mbarika[4]
Southern University and A&M College
Louisiana, USA

Lynette Kvasny[5]
Pennsylvania State University
Pennsylvania, USA

Abstract

The proliferation of Information and Communication Technology (ICT) in Sub-Saharan Africa has brought with it tremendous positive changes in socio-economic growth and development within the region. Paradoxically, ICT has also evolved to become a sophisticated tool in the hand of criminal for perpetrating different forms of cyber crime. Unintended issues such as e-mail scam, identity theft, child pornography, organized crime and solicitation for prostitution are some of the vices that have become recurring indices on the internet. A wave of fraudulent mails and other sharp practices referred to as "419 scamming" generally believed to be traceable to Nigeria pervades the West African internet webscape. This trend if not combated could serve as a breeding ground for cyber terrorism where some African countries harboring terrorists could recruit, train and plan terrorist attacks with just laptops and internet access. This study presents an overview of criminal uses of ICTs in Sub-Saharan Africa with special emphasis on the Nigerian 419 scam. We examined the emergence, trend, concerns and effects of these malaises and seek to present strategic policy perspectives on how to address the dilemma. The strategies proposed represent a set of commonalities among developing nations, similar to those of Sub-Saharan Africa, that are confronted with these problems. We conclude with implications and recommendations for research and practice.

Keywords: Cyber-crime, scamming, cyber-terrorism.

Introduction

Sub-Saharan Africa (SSA) is the last continent to embrace ICTs such as the Internet and mobile technologies. A decade ago only a very limited number of countries had local Internet access. Today, the situation is quite different. Internet penetration is on the increase in Sub-Saharan Africa with most countries depending on public and commercial internet access points such as cybercafés for rudimentary internet access. Cybercafés exploit this opportunity by charging exorbitant fees for their services. Despite this monumental growth in ICT adoption, fundamental problems of erratic power supply loom large. Inadequate telecommunication infrastructure has also continued to hinder the continent from uninterrupted access to innovative information technology applications such as e-government, e-commerce, telemedicine, teleconferencing, and teledemocracy. The current level of ICT penetration has brought renewed interest in the investment and innovative use of Information and Communications Technology (ICT) for modern development. This is evident in the proliferation of the internet access points, the use of cell phones, IPods, I-Phones, ATMs, credit cards etc. According to Internet World Stats (IWS, 2008) Nigeria, our country of interest in this study, accounts for the highest number of users in Africa as of November 2007. By June, 2009, available statistics showed that Egypt is on the lead followed by Nigeria (See Figure 1 & 2). Overall, some countries in Africa, such as the Democratic Republic of Congo and Somalia, have experienced over 35,000% growth in Internet usage during the period 2000-2007. Research is therefore warranted into the implications of ICT usage as well as any form of abuse that portend danger to ICT further contributing to the growth and development of Sub-Saharan Africa. The remaining part of the paper is organized as follows: In the next section we discussed the growth of ICT in Sub-Saharan Africa. This is followed by a section that addresses the use of ICT for criminal activities in Sub-Saharan Africa with specific emphasis on the forms of crime. The section that follows provides insight on crime and social change. The research implications are highlighted in the last section. The paper concludes with recommendations for research and practice.

ICT Growth in Sub Saharan Africa

The expansion of Africa’s online population is unprecedented. Available statistics show that there is a 1000% increase from the year 2000 figure as at the time of writing. Africa now boasts of over 50 million internet users, representing about 5% internet penetration rate on the continent. Some parts of sub-Saharan Africa, notably West Africa is taking the lead to bridge the digital divide by connecting to other parts of the world through fiber-optic cable (SAT-3/WASC). Countries such as Seychelles and Mauritius have benefitted from the advantage of established infrastructure and have been able to overcome teething problems resulting from ICT spread. For most of the countries in east Africa, internet access still depends on Satellite links for connection. This has resulted in a very expensive connection fees in some part of sub-Saharan Africa as compared to the advanced countries of the world (ITU, 2005; IWS, 2008). This high costs of internet access, epileptic power supply and lack of provision of enabling environment for a virile ICT-based infrastructure remains inimical to the full realization of the benefits accruable from full ICT penetration.

Besides accounting for the highest percentage growth in mobile phones in the World, African countries have deployed more mobile phones on the continent than fixed lines. This has led to a corresponding growth in the use of Short Message Service (SMS). For example, in South Africa, 37.5 Million users, accounting for 75% of active users, perform about 90 million SMS transmissions per day. This growth of ICTs has been extremely beneficial in several sectors of the economies of countries within the continent. Development researchers have hailed the new ICT as the “great equalizer”, revolutionary technological tools that can enable efficient transfer of information on a global scale (Kaba et al., 2008; Meso et al., 2007, Brynjolfsson & Smith, 2000). ICTs are now a tool for setting up businesses such as cyber cafes, international trade, FOREX trade, online digital libraries, online education, telemedicine, e-government and many other applications that address critical socio-economic and political problems in the developing world These applications are helping push sub Saharan Africa up the economic ladder and making the region a growing critical trade partner in the international community (AODL, 2008, Okoli et al., 2004, Kifle et al., 2006, Kifle et al., 2008; Meso et al., 2008, Thomas et al., 2004, Mbarika et al., 2007).

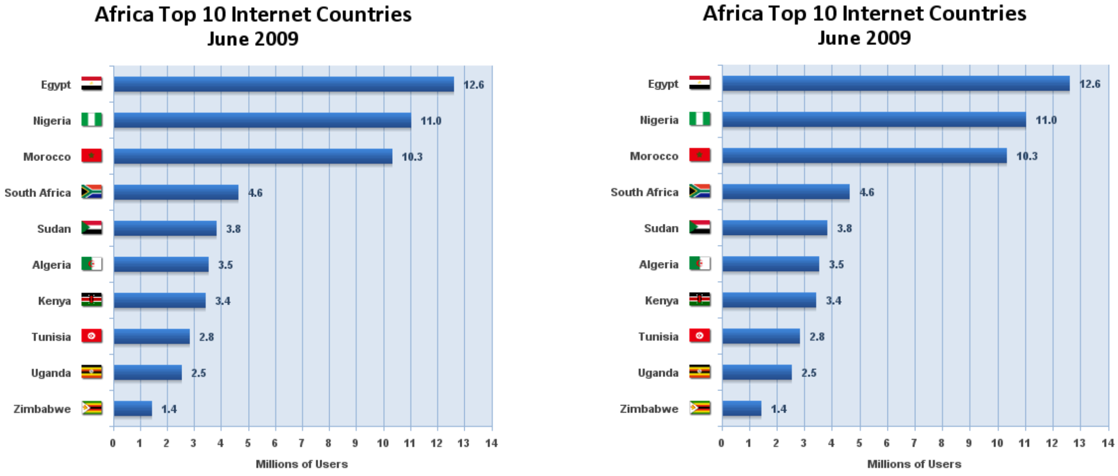

Figure 1. Country-Based Internet Usage in Africa as at November 2007 and June, 2009
Source: www.internetworldsstats.com/africa.htm

The use of mobile phones, represent about 90% of all telephone lines in Africa today and the subscriber base is still growing at about 50% per year. (Mbarika & Mbarika, 2005). With a superior national coverage and large subscriber base, Africa's mobile network operators have built up a great level of market to an extent where they have been called the incumbents. A new coverage licensing has also been introduced, whose regimes have increased the competitive pressure in a number of markets, at the same time allow the mobile operators to create new service segment branches. Due to Africa's poor fixed line infrastructure, the mobile networks have begun to play an increasing role in the provision of internet service. This is achieved by a welcome for new revenue stream in an almost entirely prepaid environment of low average revenue per user levels. Another emerging key trend that is revolutionizing Africa's financial sector is the Mobile banking. This provides an anytime anywhere banking services to customers and makes fund transfer seamless and has reduced the rate at which raw cash or bank notes are carried.

ICT Initiatives in Nigeria

In Nigeria, various means of disseminating information in the past consists of the Post offices, Town criers, Public Switched telecommunication network (PSTN) and Telegrams. ICT initiatives began in the 1950s with focus on newspapers and the electronic media such as the radio and television. These media were owned, controlled and monopolized by the government and so produced no major policy or other outcome. In 2001, the National Information Technology

Development Agency (NITDA) was established as a bureau for the implementation of national policy on Information Technology. NITDAs main focus is to fashion best practices policies that will enable effective and efficient usage of ICT facilities and infrastructures in the country (Longe & Chiemeke, 2007). Today, there are private radio and television stations in Nigeria. Digital satellite television is also in operation using pre-paid services to stream contents to subscribers. Internet services are available on mobile phones making it possible to transact a wide range of services in electronic form. Fixed and mobile wireless systems offer key advantages in these regards with the advantage of speed and universal availability. Fast deployment means quicker connection to subscribers resulting in faster payback of capital investment. The rapid rate of deployment has also made phones services widely available thereby accelerating the pace of economic development and growth. Table 1 show the growth of mobile phone subscription and penetration rates in Nigeria between 1998 and 2008.

Table 1. Mobile subscribers and penetration rate in Nigeria – 1998 - 2008

Year	Subscribers (million)	Penetration
1998	0.02	0.02%
1999	0.03	0.02%
2000	0.04	0.03%
2001	0.35	0.28%
2002	1.46	1.15%
2003	3.35	2.49%
2004	9.39	6.85%
2005	18.40	13.20%
2006	29.10	20.00%
2007	41.60	29.00%
2008 (March)	44.40	31.00%

Source: Paul Budde Comm based on NCC, Global Mobile, EMC and industry data

Despite all the positive implications of this trend, the country's image has also been dented in the ICT world as a result of the activities of some Nigerians (as well as those who claimed to be Nigerians), who has turned the internet into a cheap channel for the perpetration of online crimes, particularly, the 'Advanced Fee Fraud (AFF)' popularly known as '419'. Nigeria has therefore carved a niche for herself as the origin of most fraudulent Spam mails find in cyberspace. Unfortunately, this fact is corroborated by the volume of spamming activities that emanate from the country. Spamming was said to be one the most prevalent activities on the Nigerian Internet landscape accounting for the 18% of all online activities amongst others (Longe et al., 2007a).

Trends in ICT Usage for Criminal Activities

An elusive scenario creates the right breeding place for crime because crime ever strives to hide itself. Different nations have adopted different strategies to contend with crimes depending on their nature. Certainly, a nation with high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development (Sylvester, 2001). A number of studies have reviewed and examined the evolution, trend and use of ICT for criminal activities in Africa (Ayoku, 2005; Longe et al., 2008; Longe & Chiemeke, 2007, Smith et al., 1999; Ribadu, 2005, Adomi & Igun, 2007, Sylvester, 2001). The consensus is that despite the seemingly glowing developments in ICTs in sub-Saharan Africa, there are surges of use of these technologies for criminal activities and other social ills, hence creating a scenario where technology is used for purposes other than that for which they were originally developed. In the past ten years, examples of these "unintended" consequences of ICTs in Africa' include the use of the internet and cell phones as tools for identity theft, e-mail scam, trafficking, sexual exploitation and prostitution.

Electronic Mail Scams

A most nauseating phenomenon among cyber crimes is e-mail scam and phishing. These schemes solicit and present false financial investment opportunities to potential victims. In some cases, the scammers will pose as the wife or heir to a very wealthy dead African man or woman, mostly presidents, senators or a bank managers that left behind a large fortune that the scammer needs the victim's assistance to claim. These potential victims are promised a substantial percentage of the fortune on condition that they make a stated deposit to help process the needed paperwork. For the most part the potential victim is coerced to provide very personal information (phishing) such as their bank account information. At the end, people who fall for these baits only discover thousands to millions of dollars taken away from their bank accounts without traces.

These scammers' operate under the slogan "I Go Chop Your Dollar." They also call it a '419' game (named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud). The criminals take great pride in how much they can exploit victims (usually from the western world) and make a fortune from the greed of some individuals that want to "make quick money" (NCC, 2007). Some even claim it is payback for what the "Whiteman" has done to Africa. In essence, they believe that scamming is just a game with a winner and a loser. Equally important to address are the unintended consequences of mobile phones in Africa. Just as cybercrime is growing in Africa, mobile phones are increasingly used for prostitution and other social ills. Given the already abominable impact of the HIV/AIDS pandemic in Africa, using mobile phones to promote prostitution in Africa seem to only exacerbate the problem. There is also the case of child pornography and internet sex chat rooms (Longe & Longe, 2005).

There is no doubt that scamming using different forms of ICTs is an African-wide phenomenon. For example, since January 2001, the US Internet Fraud Complaint Center (UIFCC) web site received 49,711 complaints. The mission of IFCC, a partnership between the national white Collar Crime Center (NWCCC) and the Federal Bureau of Investigation (FBI), which began operation on May 8, 2000, is to address Internet fraud. Their website serves as a repository through which complainants file online tips with the FBI regarding Internet attacks. While perpetrators come from a varied international background, significant representations have also been found in Nigeria. In the Internet fraud report by IFCC, 2.7% of total perpetrators have been found to be from Nigeria, 0.5% from South Africa, and 0.3% from Togo (National White Collar Crime Center, 2002). In the battle against cyber crimes in Nigeria,, efforts are now being directed at the sources and channels through which Cyber-crimes are being perpetuated – the most popular one being Internet access points. Majority of the Cyber-crimes perpetrated in Nigeria generally are targeted at individuals and not necessarily computer systems, hence they require less technical expertise on the part of these criminals. Human weaknesses such as greed and gullibility are generally exploited and the criminal act usually dealt a psychological and financial blow on the victims. These crimes are just like theft and other means of swindling victims that has existed offline before the advent of the internet. The world wide web has simply provide a platform which increases the potential pool of victims for these criminals and makes it more challenging to trace and apprehend them (Aghatise, 2006).

Although electronic scam mails are generally believed to be linked to Nigeria, the scam is now prevalent in many other African countries, and the targets are usually gullible individuals who could be anywhere in the world. Many of them are linked to countries such as Ghana, Benin, Togo, Sierra Leone, the Democratic Republic of the Congo and South Africa. For example, using the Nigerian scam letter style, some tricksters in Zimbabwe are beginning to use the controversial land crises in their e-mail scam letters to deceive innocent people into parting with their money with the hopes they will receive large portions of the (sometimes) illegally distributed land (Standard Correspondent, 2004). Such individuals usually see the proposed offer as a means of making quick money and will not relent to risk their savings and even borrow to meet the demand of the tricksters with such hopes for a richer future. The Michigan District Export Council Website and the 419 coalition website provide examples of these scams to alert users about their existence. The African Scams Site (2003) reports other variations of the African Internet-based scam letters to include:

1. The transfer of money from over invoiced contracts,
2. Contract fraud, (C.O.D delivery of goods and services),
3. Conversion of Hard Currency(Hard money)
4. Sale of crude oil at below market price,
5. Purchase of real Estate,
6. Disbursement of Money from wills,
7. Clearing House.

Communication between the scammers and victims are through fax messages, courier mails, electronic mails and cell phones. This aids anonymity and make verification difficult. They gain access to active telephone lines that have been abandoned by owners who could not keep up with the cost and use them without the knowledge of the owners. For example, they can use a phone line that is registered to someone living in a different part of the city, making it almost impossible to trace (CFR, 2008). The section that follows explains some forms of Advanced fee Fraud.

(a) Transfer of Money from Over-Invoiced Contracts.

> Today, about 90% of the advanced fee fraud is by over-invoiced contract scams. This scam involves an offer to transfer large sums of money into an oversea bank account owned by a foreign company (Shaer, 2009). The scammer claims to be a government or a bank official, willing to pay the victim a reasonable amount of money, up to 30% for assisting in the transfer of funds. The victim can keep on paying for months or years the various fees and taxes before realizing that the money does not exist. (Cooper, 2005).

(b) Conversion of Hard Currency (Black Money).

> This fraud called conversion of hard currency or 'wash wash' as lay Africans will call it operates this way. Once victims accepts to allow the criminal to obtain a visa for them, so they can meet in a neutral country, the victim will be shown a suitcase filled with US dollars, defaced with waxy material to mask its origin. The victim is compelled that in other to remove this material, the criminal will have to buy a chemical. An experiment is done right before the victim in which the criminal pretend to wash the currency in order to reveal the true values. With that, the victim falls for the trick and produce the money they need to buy the chemicals. Unknowingly, he has just lost his cash to conmen (Wang, 2007).

(c) Sale of Crude oil at below market prices.

> The victim is offered special crude oil provision at a lower rate than the market rate. As in other business proposals, the victim is required to pay a registration and licensing fee to acquire crude oil at the reduced rate (INLEA, 2007). Once the price is paid, the sellers disappear, living the victim frustrated and duped

(d) Disbursement of money from wills.

> The criminals may write as an individual, charities or religious groups and claim to be the next of kin to a supposed dead multi millionaire. They then promise the victim or the third party to help transfer this money to a foreign bank account. A percentage of the money is promised to be given to the victim on successful completion of the deal. Before the contribution can be released, the recipient must first pay an inheritance tax or other fees and taxes.

(e) Charity or Relief Organization Scam.

> Another form of Advance Fee Fraud is one where the perpetrators built multiple websites, and pretend that the websites are legitimate organizations (a form of phishing website). As an example, a fraudulent website was set up after the event of Hurricane Katrina. The purpose of these websites is to ask for donations to assist victims of the Hurricane, but these fund, once collected, needless to say are going to be spent somewhere else by the scammers. Of course that is the end of the site. Most of these scammers have never been the US, let alone New Orleans, but are posing as Katrina Relief organizations.

Internet- and Mobile Phone- based Prostitution

One of the most popular cyber crimes is the act of prostitution through the use of the internet. The important question is how the internet will influence the act of prostitution both in the least sub Saharan Africa and in developed countries (Aiyar, 2006). The stakeholders involved in the business of prostitution are sex workers who work in any or all domain of the sex industry. These constitute anyone from pornography film stars to escorts mail order brides, and prostitutes (DeCurtis, 2005). Most clients of these prostitutes are tourists from the Western world. These tourists get hooked up by the internet when they seek information regarding travel location and or destination (Barrack & Fisher, 2005). They are either misled onto websites that advertise sex tour, or practically offered these baits as travel incentives (www.worldsexguide.org).

Internet-Based Child Trafficking

There is a clear overlap between the trafficking of children and their commercial sexual exploitation. Many of those trafficked from Africa into western countries will end up working on the streets, in brothels or in massage parlors (Akhilomen, 2006). Data on numbers are limited, given the covert nature of the activity and the fact that social services have only recently started to note these cases, but a report by UNICEF suggests there are 250 children known to have been trafficked into the UK in a five-year period (Gary et al., 2007). A study of the response of London social services departments to children trafficking suggest that, although social workers are aware of this issue, they do not feel adequately skilled to identify such cases or to respond appropriately. A few councils have developed policies to respond to this issue (Vock, 2007).

Internet Pornography

The usage of the web for sexual abuse remains a very active research interest. Researchers have investigated the involvement of youths and children, who are involved with online sexual activities such. These researchers have used time spent online in viewing sexual activities as a yardstick for measuring susceptibility to violent sexual conducts (Cooper et al, 2000, Brown and Eisenberg, 1995). They found out that excessive usage positively related to sexual sensation and stress among youths. The same phenomenon was replicated in the study by Goodson et al. (2003), in which participants' attitude towards seeking sex information and sexual entertainment varied based on the frequency of their Internet usage. Scholars have established positive correlations between exposure to spurious web content and sexual beliefs, attitudes, and behaviors (Young & Rogers, 1998, Kraut et al. 1998). Longe & Longe (2005) x-rayed internet pornography in Nigeria and advocates the use of web filtering programs as a robust measure against unwanted Internet content.

Crime and Social Change

The classical sociologists define crime as those activities that break the law of the land and are subject to official punishment.' For example, Abort and Clinard (1974) defined crime and delinquency as the obvious forms of social deviance. While some criminologists see crime as culturally determined, others try to explain the phenomenon from a functionalist perspective.

Durkheim (1951), Cohen (1955) and Murray (1994) argue that crime is not only inevitable and a normal aspect of human life but functional; it only become dysfunctional when social contracts or institutional arrangements for human interaction begins to malfunction. Based on that they argue that an explanation of crime should, out of necessity, provide a full social account, respect the authenticity, purposefulness of action and avoid value-laden concepts of individual pathology. In view of this, we define crime in this discourse as social actions and activities that are disapproved of by most members of the society which may or may not have been codified by the state legal apparatus.

Another concept closely related to crime and relevant to our discussion is social and cultural change. Cultures and sub-cultures are constantly changing - some rapidly and others very slowly. Likewise, social change is continuous and irresistible; only its speed and direction vary. There is a distinction between *social change which depicts* changes in the social structure and social relationships of the society and *cultural* change which implies changes in the norms, beliefs and traditions of a society (Digital Review, 2009). Some social changes might include decline of informality and personal neighborliness as people move from villages to urban centers; changes in the relationship between workers and employers; or the change in the role the husband from being a boss to a partner in today's democratic family. Cultural changes might include the changing concepts of propriety and morality; additions to new words to our language; and the invention and popularization of the application and use of computers in everyday activity. Nearly all important changes involve both social and cultural aspects. Crime in its subtle nature can easily flow along with these changes and evolve as the changes themselves permeate society. Cutting-edge technology in computing, telecommunications and electronics has created a digital world in a bewildered pattern of computer networks via telecommunication facilities and thus facilitating the emergence of the information super highway, otherwise known as the *Internet*, bringing with it a new networked society and a radical social and cultural metamorphosis.

Anonymity and Cybercrime

As measures for detecting crimes and criminals advance, criminals also look for a means to remain anonymous. The internet provides a hiding place for fraudsters who have simply migrated from the streets to an electronic platform. Anonymity has been an aid to most crimes perpetrated in cyber space. For instance, immoral contents can be streamed from the closet on a laptop or palmtop without limit. For the consumer or victim, the reservation that any other person will know about the content being consumed is also removed. ICT-induced anonymity has popularized cybercrime and internet pornography more than any other means of advertisement (Longe et al, 2007). With unlimited access to a variety of websites, and the impediment of needing to enter a brothel physically removed, immoral gratification is just the click of a mouse away from any intending consumer (Sackson, 1996).

The evolution of fixed wireless facilities in Nigerian and other Sub Saharan African countries has added another dimension to the cybercrime problem. Fraudsters who can afford to pay for Internet connection via fixed wireless lines can now perpetrate their evil acts within the comfort of their homes. In some cyber cafes, a number of systems are dedicated to fraudsters (popularly referred to as "yahoo boys") for the sole purpose of hacking and sending fraudulent mails. Other cyber cafes share their bandwidth (popularly referred to as home use) to some categories of customers who acquire systems for home use in order to perpetuate cybercrimes from their homes. The limitations experienced in combating Cyber-crimes is related to the fact that these crimes have only been in existence for only as long as the internet exists. This explains why it seems criminologists and other user protection agencies are ill-prepared towards fighting cyber crime. Numerous crimes of this nature are committed daily on the Internet with Nigerians at the forefront of sending fraudulent and bogus financial proposals all over the world. Nigeria has therefore carved a niche for herself as the source of what is now generally referred to as '419' scam and phishing e-mails.

Organized Crime in Nigeria

An advance fee fraud is a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain. The 419 scam originated in the early 1980s as the oil-based Nigerian economy declined. Several unemployed university graduates first used this scam as a means of manipulating business visitors interested in shady deals in the Nigerian oil sector before targeting businessmen in the west, and later the wider population. Scammers in the early-to-mid 1990s targeted companies, sending scam messages via letter, fax, or Telex. The spread of e-mail and easy access to e-mail-harvesting software made the cost of sending scam letters through the Internet inexpensive. In the 2000s, the 419 scam has spurred imitations from other locations in Africa, Asia and Eastern Europe.

No discussion about organized financial crime is complete in Nigeria without mentioning Fred Ajudua a Nigerian fraud kingpin. He was sometime ago tried on charges relating to collecting money under false pretences from Nelson Allen, a Canadian who allegedly lost $285,000 to Ajudua and is the only foreigner to have given mail-fraud evidence in a Nigerian court of law. He has also duped other victims such as Technex Import and Export Company of Germany, which lost the equivalent of $230,000 USD, and a German citizen who lost the equivalent of $350,000 USD trying to collect purported dividends left by her late husband. Witnesses gave a vivid image of how one Allen visited the Central Bank of Nigeria with Ajudua and met an assistant director who opened a file containing original documents of the contract and check for $28.5 million (The Wikipedia Project, 2008).

For Nigeria, a nation that has gained the unenviable reputation of being the centre of electronic spam mail, efforts to curb cyber crime are now being directed at the sources and channels through which cyber crimes are being perpetuated – the most popular being Internet access points. The Economic and Financial Crimes Commission (EFCC), saddled with the responsibility of addressing the cyber crime malaise, and which has previously relied on raiding cyber cafes and complaints from the public to clampdown on the crime, said it has now adopted smart technology working in conjunction with Microsoft, to track down fraudulent emails (Afrigood, 2009). The dividends and effectiveness of these measures are in trickles. Fraudulent e-mails are on the rise as scammers "spam" recipients with e-mail frauds that range from the very simple to the very sophisticated, which can fool even the savvy Internet user. With the increase in use of internet facilities and ATM machines for banking and other financial transactions in Nigeria, phishing attacks are also on the increase. Although online banking provides more secure identity protection than paper and mail based systems, many people in Nigeria believe using on-line banking increases the likelihood that they will become victims of identity theft (Longe et al, 2007b).

Prosecuting Cyber Crimes in Nigeria

The digital revolution has dissolved physical boundaries of nations making those with inadequate Cyber-crimes or Internet related offences laws like Nigeria vulnerable to criminals that commits such crimes. Unfortunately, legal experts always disagree on matters relating to the territorial jurisdiction for the trial of the aforesaid offences. This situation makes the investigation and prosecution of cyber-crime offences extremely difficult. Ribadu (2005) addressing the House Committee on Anti-corruption , National Ethics and Values, exhort the need to amend the Nigerian Evidence Act, the Criminal Procedure Act and the Criminal Procedure Code to accommodate technological advancement and challenges of information technology-induced criminal activities. The most popular of the abuses however is the so-called Nigerian fee scam letters. The Internet Fraud Complaint Center reports that the Nigerian fraud letters made up 15.5% of complaints received mostly from individuals. Sometimes these frauds are carried out in collaboration with other nationals (e.g. South Africans and Cameroonians) (Wearden, 2002). Speaking to newsmen in Abuja, lately, the Economic and Financial Crimes Commission (EFCC) boss Farida Waziri said Nigeria's anti-corruption police had shut down some 800 scam websites and busted 18 syndicates of email fraudsters in a drive to curb cyber-crime in the country. Over 800 fraudulent e-mail addresses have been identified and shut down and there have been 18 arrests of high profile syndicates operating cyber-crime organizations (Afrigood, 2009).

Research Finding and Implications

While Information and communication technology had been relatively successful in sub-Saharan Africa, there exists the problem of cyber crimes. Access to ICT in most sub-Saharan African countries have also provided a platform for a criminal invasion and a spree of cyber abuses. As discussed earlier, the Nigerian government is now cracking down on e-mail fraud, and working to come up with solutions to fix the damage e-mail scam has done to the country's global reputation. Most of these criminals are motivated not just by greed, but a desire to leave their country. The US Secret Service, which investigates and monitors these crimes, says they are a hundreds of millions of dollars annually and the losses are continuing to escalate. The Economic and Financial Crime Commission (EFCC), and other government agencies are engaged with the task of fighting cyber crimes and have placed a ban on all-night browsing in cyber cafes across Nigeria. This is to reduce the rate of online scamming, whose perpetrators are believed to mostly operate in the cybercafés at night. The EFCC has also been playing a great part to catch cyber criminals in the act. Unlike other anti-corruption agencies, it has registered some rare successes in the fight against economic crimes, especially in its anti-fraud efforts.

After months of investigation conducted by the agency into what has been described as the biggest cyber scam in Nigerian history, a $242mn online fraud that involved big businessmen and that led to the bankruptcy of one of Latin America’s biggest banks, ended with the successful prosecution of some very prominent Nigerians last year. In 2004, the EFCC also returned $4m naira to a Hong Kong resident after arresting the fraudsters who swindled her out of her money. In 2004, government established a cyber-crime think tank, the Nigeria Cyber Working Group (NCWG) to provide direction for its fight against cyber criminals. Its efforts and those of other similar government agencies have resulted in Nigeria's first cyber crime bill. The bill, which is before the National Assembly, recommends punishment ranging from N15mn (about $1.2mn) to N20mn and a maximum of 30 years' imprisonment for anyone found guilty of cyber-related crimes

In April, 2009, stakeholders in the ICT industry in Nigeria met to discuss how to assist information security and come up with steps to be taken to reduce cyber crime in Africa. The meeting came up with the communiqué that Computer Security and Cyber crime awareness should be created with a view to sensitizing all users of the internet facility with the merging indicators of crime and fraud being committed through the use of the computer. Some of the organizations that have been created in many African countries to assist eradicate this problem are: (NSA), the Nigerian Communications Commission (NCC), Department of State Services (DSS), National Intelligence Agency (NIA), (ISPAN); International Information Technology Development Agency. Also, at the UN Congress on Crime Prevention and Criminal Justice, at Bangkok in 2005, many African countries that has been suffering from technological crimes gave their suggestions as to steps which can be taken to address the problem. They opined that it is necessary to adopt a global policy on the internet crimes, and all other technological crimes in the form of modern laws and the enhancement of financial systems. Present in this meetings were representatives from Ghana and also Cameroon.

An important outcome of the meeting was the desire to come up with a framework to deal with cyber crime. Kenya, Uganda and Tanzania are in the process of adopting harmonized cyber laws to enable the establishment of e-government and e-commerce programs. The cyber laws will cover data security, network security, cyber crime, information systems and electronic transactions. Supported by the United Nations and Canada, the East African Community is expected to follow the process already started by the South African Development Community. That region - including South Africa - began harmonizing its laws to prosecute cyber criminals operating across national boundaries.

Policy Recommendations

Information and communication technology, though an indispensable tool for national development can portend very great danger if not well managed. The responsibility of preventing and resolving technological crimes against victims is not merely a federal or local government issue. Events and trends has shown that it is a global responsibility as cyber crime is a borderless crime. By making information communities, harmonize existing preventive frameworks and having legal authorities take active role based on the following recommendations, we can make the journey through cyber space safer for many people.

Commercial banks in Nigeria serve as a conduit for funds transfer and foreign remittances to the country and these banks in turn disburses the funds to the beneficiaries. The Central Bank of Nigeria (CBN) which regulates and control Commercial Banking operations and activities have no reporting policy that is incumbent on commercial banks to report the identity of all recipients of foreign remittances to the CBN or other agencies of the state. Such reporting policies when in place will create a database from which the Economic and Financial crime commission (EFCC) can review on regular basis activities involving suspicious foreign remittances. The report should be broadened to include all reasonable information such as the name of the sender and the receiver, purpose of the transaction and relationship between the parties, time frame of these transactions as well as addresses of parties involved.

As discussed earlier, the Economic and Financial Crime Commission in Nigeria in her bid to stem the tide of e-mail scam and phishing fraud prohibited night browsing in cybercafés. This attempt may temporarily slow the internet traffic for scammers who usually hack peoples email addresses and send out unsolicited bulk emails at night using cybercafés. It should be noted that prices of Laptops have dropped significantly in the last few years and many of these scammers have acquired internet enabled Laptops which they can use from the comfort of their homes and launch out their nefarious activities. We recommend that the Nigerian Telecommunication Commission (TCC) put in place a policy mandating Internet service providers in Nigeria to report suspicious and unusual bulk emails traffic per service points going through their systems. This practice could flag off the identification of the scammers, their locations and their eventual prosecution.

There is also the need for various security and regulating agencies in Nigeria to collaborate to fight the menace of cybercrime collectively. Such collaborations could be in the area of information sharing, infrastructure and personnel. Since cyber crime transcends borders, it is therefore a global phenomenon that requires a global solution. Collaborations with other African Countries and major International security agencies such as the FBI, INTERPOL, and CIA need to be mustered for a global crack-down on the crime. Finally, we wish to reiterate the need for continued Government support by creating and maintaining enabling environment that will make the work of all the agencies responsible for curbing this crime easier and more targets driven. They can demonstrate their support by generous funding of the programs and projects of these agencies. These recommendations are equally valid for instances of the cyber crime problem anywhere in Sub Saharan Africa and the world at large.

Acknowledgements:

This research is supported by the John T and Katherine D. Macarthur Staff Development and Capacity Building Fund domiciled at the University of Ibadan, Ibadan Nigeria and the National Science Foundation Grant at the International Centre for Information Technology & Development (ICITD) College of Business, Southern University, Baton Rouge LA. These funding are gratefully acknowledged.

References

Abbott, D. J., & Clinard, M. B. (1973). *Crime in developing countries: A comparative perspective*. New York: John Wiley and Sons.

Adebayo, D. O., Udegbe, I. B., & Sunmola, A. M. (2006). Gender, Internet use, and sexual behavior orientation among young Nigerians. *CyberPsychology & Behaviour*, *9*(6), 742–752. doi: 10.1089/cpb.2006.9.742.

Adomi, E. E., & Igun, S. E. (2008). Combating cyber crime in Nigeria. *The Electronic Library, 26*(5), 716-725. doi: 10.1108/02640470810910738

Afrigood. (2009, October 23). Nigeria's anti-graft police shut 800 scam websites. *Africa: the Good News*. Retrieved from http://www.africagoodnews.com/ict/nigerias-anti-graft-police-shut-800-scam-websites.html

Aghatise, E. J. (2006, June 28). Cybercrime definition. *Computer Crime Research Center*. Retrieved from http://www.crime-research.org/articles/joseph06/2

Aiyar, P. (2006, February 26). In the line of fire. *The Hindu*. Retrieved from http://www.hinduonnet.com/thehindu/mag/2006/02/26/stories/2006022600090500.htm

Akhilomen, D. O. (2006). Addressing child abuse in Southern Nigeria: The role of the church. *Studies in World Christianity, 12*(3), 235-248. doi: 10.1353/swc.2006.0018

AODL. (2008). Building digital libraries in Africa. *The African Online Digital Library*. Retrieved from http://www.aodl.org/

Ayoku, A. O. (2005): The evolving sophistication of Internet abuses in Africa. *The International Information & Library Review, 37*(1), 11-17. doi:10.1016/j.iilr.2005.01.002

Barak, A., & Fisher, W. A. (2005). The future of Internet sexuality. In A. Cooper (Ed.), *Sex and the Internet: A guidebook for clinicians* (pp. 263-280). New York: Routledge.

Brown, S. S., & Eisenberg, L. (Eds.). (1995). *The best intentions: Unintended pregnancy and the well-being of children and families.* Washington, DC: National Academy Press.

Brynjolfsson, E., & Kahin, B. (Eds.) (2000a). *Understanding the digital economy*. Cambridge, MA: MIT Press.

Brynjolfsson, E., & Smith, M. (2000b). *The great equalizer? Consumer choice behavior at Internet shopbots*. Cambridge, MA: MIT Working Paper.

Cohen, A. K. (1955). *Delinquent boys: The culture of the gang*. Glencoe, IL: The Free Press.

Consumer Fraud Reporting. (2008). How the money transfer and bank account frauds -- so-called "Nigerian", "419" and "Dutch" scams work. *Consumer Fraud Reporting*. Retrieved from http:// www.consumerfraudreporting.org/nigerianAFF.php

Cooper, A., McLoughlin, I. P., & Campbell, K.M. (2000). Sexuality in cyberspace: Update for the 21st century. *CyberPsychology & Behavior*, *3*(4), 521–536.

Craig, G., Gaus, A., Wilkinson., Skrivankova, K. & McQuade, A. (2007). *Contemporary Slavery in the UK.* York, England: Joseph Rowntree Foundation. Retrieved from http://www.jrf.org.uk/sites/files/jrf/2016-contemporary-slavery-uk.pdf

DeCurtis, C. (2003). Prostitution, sex tourism on the Internet: Whose voice is being heard? *ACM SIGCAS Computers and Society, 33*(1), 3-11.

Digital Review. (2009). Community and family life in the digital age. *Digital Review of Asia Pacific*. Retrieved from http://www.digital-review.org/themes/26-social-political-and-cultural-aspects-of-icts.html

Durkheim, E. (1951). The normal and the pathological. In M. Wolfgang, et. al., (Eds.) (1970). *The Sociology of Crime and Delinquency* (3rd ed., pp. 75-215). Hoboken, NJ: John Wiley and Sons, Inc.

Global Advances. (2009, February 7). *Africa's climb to an Internet revolution* [Web log message]. Retrieved from http://globaladvances.com/blog/?p=92

Goodson, P., McCormick, D., & Evans, A. (2003). Sex and the Internet: A Survey Instrument to Assess College Students' Behavior and Attitudes. *CyberPsychology & Behavior, 3*(2), 129-149. Retrieved from http://www.liebertonline.com/doi/abs/10.1089/109493100315987

INLEA. (2007). International narcotics and law enforcement affairs (INL), United States bureau of. *Encyclopedia of Espionage, Intelligence, and Security.* Retrieved from http://www.encyclopedia.com/doc/1G2-3403300397.html

ITU. (2005). Access indicators for the information society. (2005). *World Summit on the Information Society.* Tunis, 2005

IWS. (2008). Internet world stats: African Internet Usage. *Internet World Stats*. Retrieved from http://www.internetworldstats.com/africa.htm

Kaba, B., N'Da, K. and Mbarika V. (2008, January). Understanding the factors influencing the attitude toward and the use of mobile technology in developing countries: A model of cellular phone use in Guinea. *Proceedings of the 41st Hawaii International Conference on System Sciences* (IEEE Computer Society), 127. doi: 10.1109/HICSS.2008.479

Kifle, M., Mbarika, V., & Bradley, R.V. (2006). Global diffusion of the Internet X: The diffusion of telemedicine in Ethiopia: Potential benefits, present challenges, and potential factors. *Communications of the Association for Information Systems*, *18*(30), 612-640.

Kifle, M., Mbarika, V., Okoli, C., Tsuma, C., Wilkerson, D., & Tan, J. (2008, January). A telemedicine transfer model for Sub-Saharan Africa. *Proceedings of the 41st Hawaii International Conference on System Sciences* (IEEE Computer Society).

Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukophadhyay, T., & Scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological well-being? *American Psychologist, 53*(9), 1017–1031.

Longe, O. B., & Chiemeke, S. C. (2007). Information and communication technology penetration in Nigeria: Prospects, challenges and metrics. *Asian Journal of Information Technology, 6*(3), 280–287. Retrieved from http://www.medwellonline.net/fulltext/ajit/2007/280-287.pdf

Longe, O. B., Chiemeke, S. C, Onifade, O. F. W., Balogun, F. M., Longe, F. A. & Otti, V. U. (2007). Exposure of children and teenagers to Internet pornography In South Western Nigeria: Concerns, trends & implications. *Journal of Information Technology Impact*, *7*(3), 195-212. Retrieved from http://www.jiti.net/v07/jiti.v7n3.195-212.pdf

Longe, O. B., Chiemeke, S. C., Onifade, O. F. W., & Longe, F. A. (2008). Camouflages and token manipulations: The changing faces of the Nigerian fraudulent 419 spammers. *African Journal of Information Technology*, *4*(3), 87-98.

Longe, O. B., & Longe, F. A. (2005). The Nigerian Web content: Combating the pornographic malaise using Web filters. *Journal of Information Technology Impact*, *5*(2), 59-64. Retrieved from http://www.jiti.net/v05/jiti.v5n2.059-064.pdf

Longe, O. B., Onifade, O. F., Chiemeke, S. C., & Longe, F. A. (2007, October). User acceptance of Web-marketing in Nigeria: Significance of factors. *Proceedings of the International Conference on Applied Business & Economics*. Piraeus, Greece.

Meso, P., Datta, P., & Mbarika, V. (2006). Moderating information and communication technologies' influences on socioeconomic development with good governance: A study of the developing countries. *Journal of the American Society for Information Science and Technology, 57*(2), 186-197.

Murray, C. (1994). The physical environment. In J. Q. Wilson & J. Petersilia, (Eds.), *Crime*. San Francisco, CA: Institute for Contemporary Studies.

Nigeria -- The 419 Coalition. We fight the Nigerian scam with education. *Nigeria -- The 419 Coalition*. Retrieved from http://home.rmci.net/alphae/419coal/

Nigerian Criminal Code. (2007). Retrieved from http://www.nigeria-law.org/CriminalCodeAct-Tables.htm

NWCCC. (2002). IFCC 2001 Internet fraud report: January 1–December 31, 2001. *National White Collar Crime Center*. Retrieved from http://www.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf.

Okoli, C., Mbarika, V.W.A., & McCoy, S. (2004, June). The effects of culture on e-business in Sub-Saharan Africa. *Proceedings of the Fifth Annual Global Information Technology Management (GITM) World Conference*, 170-172. San Diego, CA.

Paul Budde Communication Pty Ltd. (2008). *African mobile communications and mobile data markets*. Retrieved from http://www.marketresearch.com/product/display.asp?productid=2107634

Ribadu, N. (2004, November). *Obstacles to the effective prosecution of corrupt practices and financial crime cases in Nigeria*. Paper Presented at the Summit on Corrupt Practices and Financial Crimes in Nigeria, Kaduna, Nigeria.

Sackson, M. (1996, March). Computer ethics: Are students concerned? *First Annual Ethics Conference*, Chicago, Loyola University. Retrieved from http://webpages.cs.luc.edu/~laufer/ethics96/papers/sackson.doc

Shaer, M. (2009, June 9). Ransoming data: The new weapon of choice for cyber criminals? *The Christian Science Monitor*. Retrieved from http://features.csmonitor.com/innovation/2009/06/09/ransoming-data-the-new-weapon-of-choice-for-cyber-criminals/

Smith, R. G., Holmes, M. N., & Kaufmann, P. (1999). Nigerian advance fee fraud. *Trends and Issues in Crime and Criminal Justice*, 121, Canberra: Australian Institute of Criminology. (Republished in *The Reformer*, February 2000, 17-19). Retrieved from http://www.aic.gov.au

Standard Correspondent. (2004, June). Internet fraudsters reap from Zimbabwe land crisis. Retrieved from http://www.eastandard.net/headlines/news10060407.htm

Sylvester, L. (2001): *The importance of victimology in criminal profiling*. Retrieved from http://isuisse.ifrance.com/emmaf/base/impvic.html

Vock, D. C. (2007, November 27). *Police join feds to tackle immigration*. Stateline.org. Retrieved from http://archive.stateline.org/weekly/Stateline.org-Weekly-Original-Content-2007-11-26.pdf

Wang, S. (2007). Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer Standards & Interfaces, 29*(2), 216-223.

The Wikipedia Project. (2008). Advance-fee fraud. *The Wikipedia Project*. Retrieved from http://en.wikipedia.org/wiki/ Advance_fee_fraud

Young, K. S., & Rogers, R. C. (1998). The relationship between depression and Internet addiction. *CyberPsychology & Behavior, 1*(1), 25-28. Retrieved from http://www.netaddiction.com/articles/cyberpsychology.htm.

[1] Olumide Longe is on the faculty at the Department of Computer Science, University of Ibadan, Nigeria. His research focuses on the use of machine learning techniques to secure electronic mailing systems and for controlling cyber crime. Currently a MacArthur Scholar to the International Centre for Information Technology and Development, (ICITD) Southern University and A&M College, Baton Rouge, Louisiana, U.S.A. He can be reached at: longeolumide@icitd.org; Phone: +12256506530.

[2] Oneurine Ngwa is an associate researcher at the International Centre for Information Technology and Development, College of Business, Southern University and A&M College, Baton Rouge, Louisiana. Her research focuses on how to use business models to solve the cyber crime problem. She can be reached at: oneurine@icitd.com; Phone +12252477676

[3] Friday Wada is on the doctoral program at the Nelson Mandela School of Policy and Urban Affairs. His research interest is the application of pragmatic policy theories and practices to solving information technology related problems as it applies to the developing countries. He collaborates with ICITD on research into ICT transfer to sub-Saharan Africa with special interest on cyber crime. He can be reached at: friwada@yahoo.com; Phone +12255880012

[4] Victor Mbarika is a Professor and Director of the International Centre for Information Technology and Development, College of Business, Southern University and A&M College, Baton Rouge, Louisiana. His research focuses on the interactions of social, cultural, and infrastructural aspects of information technology transfer to developing nations, particularly in Sub-Saharan Africa His research provides theoretically-informed framework for understanding ICTs in less developed countries. He can be reached at: victor@mbarika.com; Phone +1(225) 572-1042 or +1(225) 771-5640

[5] Lynette Kvasny is a Professor at the College of Information Sciences and Technology, Pennsylvania State University. Her research focuses on how and why historically underserved groups appropriate information and communication technologies (ICT). Her research contributes to socio-technical policy interventions for redressing digital inequality, and critical and feminist perspectives on the intersection of gender, race and class in shaping digital inequality. She can be reached at: lkvasny@ ist.psu.edu; Phone +11.814.865.6458