Journal of Computer Science & Its Applications, June 2007, Vol. 14 No. 1

Emerging Technologies' Revolution and Daunting Challenges Facing the Law Enforcement Agencies

Charles O. UWADIA,
Department of Computer Sciences,
University of Lagos, Nigeria
couwadia@unilag.edu.ng, couwadia@yahoo.com

Zacchaeus Oni OMOGBADEGUN
Lecturer II, Department of Computer and Information Sciences,
College of Science and Technology,
Covenant University, Ota, Ogun State, Nigeria
oniomogbadegun@yahoo.com

ABSTRACT

The conduct of any business activity must be done under the law for it to be considered legal. This business conduct has since 1994 till date been transformed and overtaken by the stormy revolution of information and communications technologies leading to daunting challenges necessitated by the new wave of criminal activities in every sector. The use of Information and Communications Technology by government, non-government, and international criminal organizations will therefore clearly have an increasingly important impact on the functioning of law enforcement and security agencies in the information age. The countermeasures to high tech crimes also raise fundamental questions for the study of criminology, the law and policing policies. Locally, there is a widespread of Information Communications Technology-related crimes in the developing countries. The growth of technology and Internet use offers more opportunities to criminals with larger payoffs and fewer risks. The obvious ones that are found around on daily basis include software piracy, cases of advance fee fraud (419) which has given Nigeria the greatest dent on her image, Internet fraud at Cyber cafés, electronic funds transfer with telecommunications infrastructures, etc. Law enforcement has withstood many challenges over the years. Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct e-business within a country and across national boundaries. One of the most worrisome of these areas has been the combination of the law enforcement and the judicial system where several archaic laws are overdue for revision and be enforced so as to be kept consistent with "untameable" / "unstoppable" borderless Internet developments.

In preventing IT and legal professionals from professional suicide in the face of ever evolving high-tech crimes, etc, this paper covers, among other areas, reviews and examinations of the existing criminal laws for adequacy and/or comprehensiveness in tackling computer-related crimes; computer crime statutes enactment and/or development; identification and/or resolution of the problems and/or challenges encountered by the laws enforcement agents in this new area of computer crime laws; and provides guidance in preparing for administrative, civil, and criminal proceedings associates with computer crime with an exposure of the tools and techniques employed by law enforcement agencies worldwide to track down computer hackers.

Keywords: computer crime, statutes, forensics, law enforcement agency, hackers

1. Introduction

Information Technology experts and researchers have ascertained that the rapidly increasing applications of computer-based information technology in realms of social activity have considerable impact on society itself. According to these experts, this is certainly to be expected. Information is one of the most critical assets of an organization, and unlike other assets, its value often depends on how well a company can keep the information to itself. The exchange and use of information about individual persons lie at the very heart of such private social institutions as banking, credit, insurance, and medical care. Numerous governmental activities such as taxation, census taking, licensing of drivers, students' records, international passport processing, etc. also rely greatly on personal information. More personal social relationships such as trust, friendship, and love depend even more critically on the personal information that individuals choose to share with one another.

The nascent threat of information technology-related crimes to affect national and international economies, security and social and political relations provides a serious challenge to the future roles and practices of law enforcement agencies and security services. The very technologies, which enable multinational corporations to do business more easily and challenge the individual controls and regulations of nation states, also offer the prospect of globally organized criminal networks (Castells 1998). Moreover, the free flow of uncensored information on electronic networks and websites is as attractive to insurgents and extremist groups as it is to dissidents proclaiming their human rights.

While the developed countries have taken pragmatic approaches to face these challenges, the developing countries on the other hand (e.g. Nigeria) still seem to be waking up. Yet, businesses have to be conducted with the developing countries by the developed countries! An Information Technology (IT) professional, on whose shoulders lie the responsibility of the information systems in supporting organizations, can no longer claim ignorance of the legal requirements in performing his obligations under professional ethics and the other requisite norms to avoid professional suicide.

1.1 Definition of Terms

Various terms are used (and misused) to define cyber crime. For this paper, we define cyber crime as, "A criminal offense that has been created or made possible by the advent of computer technology, or a traditional crime which has been so transformed by the use of a computer that law enforcement investigators need a basic understanding of computers in order to investigate the crime." Within that broad definition lie two distinct sub-categories:

1.1.1 Computer Crime and Computer-related Crime.

Computer Crime involves the use of a computer as the primary instrument to facilitate the crime and the target thereof. While state laws vary somewhat, these crimes usually include the unauthorized:

- use, access or damage to a computer system;
- taking, copying, altering, deleting, or destroying computer data, software or programs;
- disrupting computer services or denying computer services to an authorized user;
- introducing a computer contaminant (viruses) into any computer or system; or,
- misuse of someone else's Internet domain name.

Computer-related Crime involves the use of a computer to commit a crime and/or as a repository of evidence related to the crime. Generally, this includes traditional crimes that have been transformed by computer technology such as:

- computer-generated counterfeit documents;
- computer generated threats;
- possession of computer-based child pornography images; or,
- any crime in which documents or evidence is stored in a computer such as records of narcotic distribution, gambling or embezzlement.

Computer-related crime can involve use of the Internet to facilitate crimes such as:

- Internet auction fraud (primarily thefts);
- criminal threats;
- stalking (cyber stalking);
- threatening or annoying electronic mail;
- distribution of child pornography;
- online gambling;
- fraudulent credit card transactions;
- fraudulent application for goods or services; or,
- identity theft.

The importance of recognizing these two distinct categories is critical in that they require varying levels of investigative skill. Specifically, computer crimes require a much higher degree of technical knowledge than computer-related crimes. Throughout this paper, we will make specific observations regarding these two categories of cyber crimes [2].

The history of 'computer crime' dates back to the 1960s when first articles on cases of so-called "computer crime" or 'computer-related crime' were published in the public press and in scientific literature. These cases primarily included computer manipulation, computer sabotage, computer espionage and the illegal use of computer systems. However, due to the fact that most reports were based on newspaper clippings, it was controversially discussed whether or not this new phenomenon of computer crime had any plausible reasons.

Computer crime has expanded in scope far beyond mere economic crime, and can be expected to include attacks against national infrastructure, security and social well being. Computer-related

criminal law has undergone similar changes, in response to the criminal evolution enabled and enhanced by information technology.

1.2. Classification / Categories of High Tech Crime

Among the fraud schemes targeted are those involving on-line auction fraud, systemic non-delivery of merchandise purchased over the Internet, credit/debit card fraud, bank fraud, investment fraud, multi-level marketing and Ponzi/Pyramid schemes. Internet fraud can be defined as any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms, and e-mail, play a significant role in offering non-existent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators. Many of these cases were initiated as a result of fraud complaints the Internet Fraud Complaint Center received from individuals and businesses.

Discussions of emerging technological crimes center mostly on computer crime, with the inference that there is only one type of offences. This is not, however, the case, because specific categories of computer crime exist. As computer-related crimes become more prevalent, an increasing need emerges for police personnel--particularly those who do not have expertise in computer technology--to understand how these crimes vary. An understanding of the types of computer-related crimes will assist law enforcement by providing insight for investigative strategies.

1.2.1 Types of Computer Crimes

Different authors have presented different types and/or categories of high tech crime. McConnell International's report looked at ten different types of cyber crime in four categories: data-related crimes, including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery. There are primarily four general types of computer crimes: Computer As the Target, Computer As the Instrumentality of the Crime, Computer Is Incidental to Other Crimes, and Crimes Associated With the Prevalence of Computers. In practice, multiple crimes i.e. concurrent criminality or lesser offenses, can occur during any given criminal transaction, resulting in an overlap between the classifications [3].

1.2.2. Incidents of High-Technology Crimes

A significant research found was that undertaken by McConnell International LLC and the World Information Technology Services Alliance in December 2000. In other words, it is a green area probably due to the low literacy level of our legal system functionaries in Information Technology combined with the lack of interest by the Information Technology practitioners in getting bogged down with legal details. We would in future encourage the two disciplines to form a formidable alliance for a joint purpose at exchanging technical programmes.

In this computer-literate age, sophisticated criminals are using computers in their illegal activities.ÊAdvances in computer technology have provided criminals with a powerful tool.Ê Reported incidents of high-technology theft and computer-related crime are increasing dramatically and

successful investigations and prosecutions will be dependent on investigators' computer skills.ÊÊIn the last fifty and more years there have been enormous advances and development with science and technology. Unfortunately human rights laws and instruments were developed for earlier times and have not kept pace. they have been patched up. It is time for a major overhaul of legislation at a local and international level [4].

As an example the Australian Commonwealth Privacy Act 1988 is being updated with an amendment in 2000 [5]. This reflects how the law passed twelve years ago is unable to grapple with issues associated with the internet. The issues generating the change include the massive explosion of data now being collected by organisations on individuals and the ease with which it can be manipulated, copied and distributed.

Rising to the prevalence of sophisticated crimes being perpetrated with the new weapon, the National White Collar Crime Center (NW3C), a non-profit organization funded by the U.S. Department of Justice, Bureau of Justice Assistance, provides support to local and state enforcement agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime. NW3C training incorporates the best current practices of experts in the field of financial investigations and computer forensic and investigations courses.

2. Computer-Crime Statistics

The statistics on computer-crime indicate that the technologically-oriented approach to fixing information security problems is not working. Both the incidence and the seriousness of losses are increasing year after year. On January 24, 1996, the Scripps Howard News service reported "Computer crime costs Britain $1.5billion a year". What is in dire need of management attention at many organizations is the people side of information security.

The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, has established the National Infrastructure Protection Center (NIPC) located at FBI headquarters and the Regional Computer Intrusion Squads located in selected offices throughout the United States. The NIPC, a joint partnership among federal agencies and private industry, is designed to serve as the government's lead mechanism for preventing and responding to cyber attacks on the nation's infrastructures. (These infrastructures include telecommunications, energy, transportation, banking and finance, emergency services and government operations). The mission of Regional Computer Intrusion Squads is to investigate violations of Computer Fraud and Abuse Act (Title 8, Section 1030), including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes.

3. Technology, Laws, and Standards: Is the Law getting left behind?

In view of both the worldwide notoriety and far-reaching damage caused and being caused by the high tech crimes perpetrated through the internet the latest high tech weapon capitalized upon by criminals for sophisticated crimes this paper focuses more on this internet technology in its scope while the other related matters build around it. Using United States of America, United

Kingdom, Canada, and South Africa as benchmarks, the research method used for this paper is a field study involving the reviewing existing Federal Laws (Criminal Laws, precisely) for adequacy and comprehensiveness in combating the new wave of crimes associated with Information Technology; law enforcement agents' Information Technology literacy level and preparedness to arrest, investigate, and prosecute Information Technology-related crime suspects; court criminal proceedings; review of technology infrastructure to preserve evidence necessary for a successful prosecution vis-à-vis the situations in the benchmarks utilizing interviews, surveys, press reviews, news accounts, and document research as the means for data collection so as to ascertain the effectiveness of the Information Technology Laws (and as applicable in Nigeria), the degree to which components of the Information Technology Laws are temporally and spatially integrated, and how the legal system measures productivity at combating the new wave of electronic crimes perpetrated and/or facilitated by Nigerians and non-Nigerians in Nigeria.

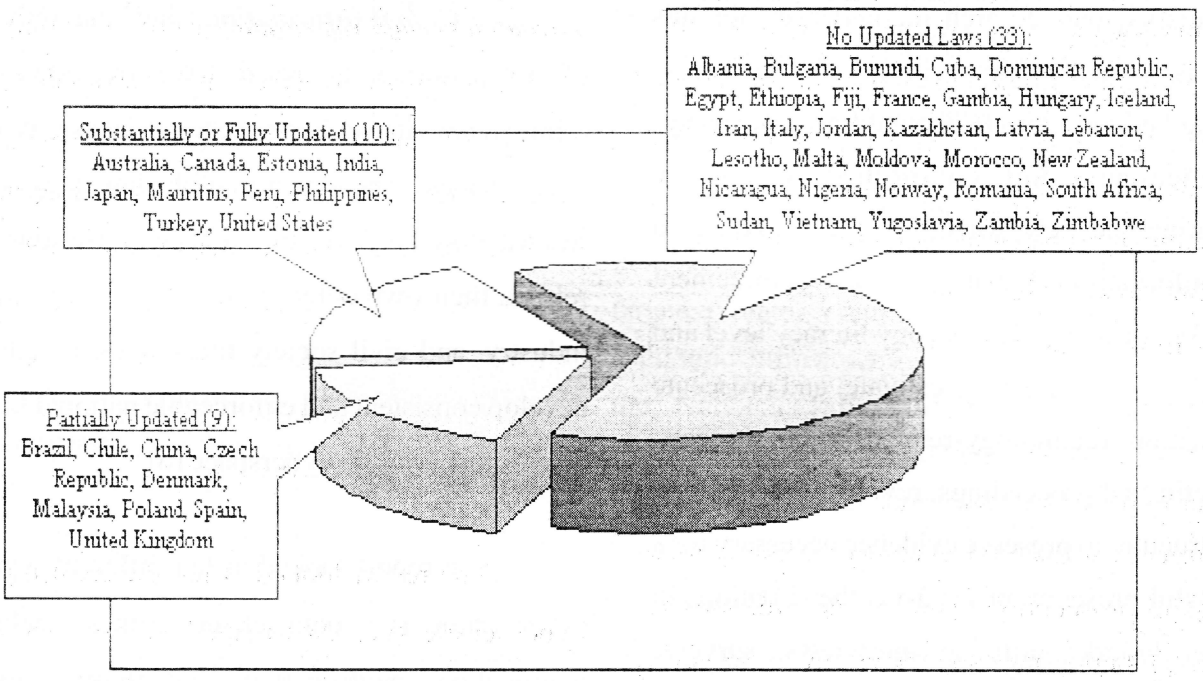
3.1. United Nations Project

Washington's Press Release ("Global Cyber Crime: Weak Laws Threaten E-Commerce *Self-Protection Is Principal Defense*") revealed that gaps in national criminal laws make successful prosecution of international cyber crimes uncertain in many countries, according to a report issued 7 December 2000 by McConnell International LLC, a global policy and technology management consulting firm. The report, ***Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information,*** finds that only nine of 52 countries analysed have extended their criminal laws into cyberspace to cover most types of cyber crimes. The long arm of the law does not yet reach across the global Internet. Organizations must rely on their own defenses for now. Governments, industry, and civil society must work together to develop consistent and enforceable national laws to deter future crime in cyberspace [6].

The report looked at ten different types of cyber crime (i.e. data-related crimes, including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery) in four categories: data-related crimes, including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery.

Thirty-three of the countries surveyed (including **Nigeria**), the reported added, have not yet updated their laws to address any type of cyber crime. Of the remaining countries, ten have enacted legislation to address five or fewer types of cyber crime, and nine have updated their laws to prosecute against six or more of the ten types.

Figure 1: Extent of Progress on Updating Cyber Crime Laws



Source: McConnell International LLC: , ***Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information***, December 2000

Figure 2: Countries with Updated Laws

Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	X	X	X	X		X			X	X
Brazil		X			X	X		X		
Canada	X	X	X	X	X	X	X			X
Chile	X	X	X	X	X					
China		X		X			X			
Czech Republic		X	X		X	X				X
Denmark		X		X						X
Estonia		X	X	X	X	X	X	X		X
India		X	X	X	X	X	X	X		X
Japan	X	X	X	X	X	X		X	X	X
Malaysia		X				X		X		X
Mauritius	X	X		X	X	X	X	X	X	
Peru	X	X	X	X	X	X				X
Philippines	X	X	X	X	X	X	X	X	X	X
Poland		X	X	X				X		
Spain	X	X	X					X		X
Turkey		X	X	X	X		X	X	X	X
United Kingdom		X		X	X	X		X		
United States	X	X	X	X	X	X	X	X		X

Source: McConnell International LLC: , ***Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information***, December 2000

Key for Figure 2

Data Interception: Interception of data in transmission.
Data Modification: Alteration, destruction, or erasing of data.
Data Theft: Taking or copying data, regardless of whether it is protected by other laws, e.g., copyright, privacy, etc.
Network Interference: Impeding or preventing access for others. The most common example of this action is instigating a distributed denial of service (DDOS) attack, flooding Web sites or Internet Service Providers. DDOS attacks are often launched from numerous computers that have been hacked to obey commands of the perpetrator.
Network Sabotage: Modification or destruction of a network or system.
Unauthorized Access: Hacking or cracking to gain access to a system or data.
Virus Dissemination: Introduction of software damaging to systems or data.
Aiding and Abetting: Enabling the commission of a cyber crime.
Computer-Related Forgery: Alteration of data with intent to represent as authentic.
Computer-Related Fraud: Alteration of data with intent to derive economic benefit from its misrepresentation.

Source: McConnell International LLC: , ***Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information,*** December 2000

Figure 3: Progress Underway in 13 Countries Without Updated Laws

Albania	The Authority for the Regulation of Telecommunications began discussions earlier this year on the topic of cyber laws, with the goal of preparing protocols of collaboration and exchanging information.
Cuba*	A working group of the Ministry of Justice has planned modifications to the Penal Code.
Gambia	Gambia is planning a national information technology initiative, although the capacity for the drawing up a legal framework is limited. Gambia may look towards international organizations to spearhead this effort so that it could replicate or amend the needed laws.
Iran	For the past six years, Iran has examined various aspects of cyber law, although no law or regulation in regard to computer offenses has been implemented. The areas that have been considered are: computer offenses, intellectual property issues, privacy/data protection, and freedom of information.
Kazakhstan	State bodies in Kazakhstan are currently developing a law regarding cyber offences. Also in development is a special state program on the protection of information resources, including technical and software protection.
Latvia*	Amendments to the Criminal Code have been drafted envisaging considerable punishment for computer-related criminal acts. Corresponding additions would be made to the Administrative Offence Code.
Lesotho	Lesotho has established special interest groups to look at the various aspects of information security relating to e-commerce.
Malta*	In May 2000, Malta announced its goal of providing a strong legal framework for e-commerce, data protection, and computer misuse. The relevant Bills to develop a legislative framework for information practices were published in September 2000 and will be discussed in parliament in the coming months.
Morocco	In Morocco, there is an inter-ministerial commission sponsored by the Prime Ministerworking on security issues.
New Zealand*	At present there are no general computer crime offences in New Zealand. However, the country is currently drafting a Crimes Amendment Bill (No. 6).
Sudan	The Sudan intends to invite lawyers, legislators and computer professionals to a workshop where ideas on the nature of computer crimes and the ways of dealing with them by means of the appropriate legal codes will be exchanged.
Vietnam	Vietnam is in the process of gathering information to make proposals for amendments to its laws.
Zambia*	Zambia has made available a draft of its Telecommunications and Information Technology Council Act.

* Copies of relevant drafts are available at www.mcconnellinternational.com.

Source: McConnell International LLC: , ***Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information,*** December 2000

4. Perspective on Legal Issues

Offences vary by both the criminal act and the jurisdiction. Some States have enacted laws specifically directed toward crimes involving computers, while other States rely fundamentally on the common law as it applies to current and emerging technology. As with any other crime, the elements of a computer-related offences must be established for successful prosecution, not a particularly easy task in light of the nature of computer technology.

Similarly, the physical act of a computer-related crime, actus reus, may be demonstrated best by an electronic impulse that, unfortunately, is difficult to define and track, considering that a computer crime can occur in 3 milliseconds using a program code that tells the software to erase itself after the computer executes the action. Essentially, this eliminates the evidentiary trail.

These issues provide similar problems for the criminal element of causation, typically found in statutes relying on the common law. Causation in this regard relates to the self-destruction of computer programs that facilitate "cyber" crimes. How can an investigator show causation if the offender erases the executing instructions? Additionally, the electronic data interchange (EDI) and its networks complicate the legal elements by making it more difficult for law enforcement to specify, document, and materially link the crime to an individual.

Legal reforms have taken place in many countries (mostly European) since the 1970s, reflecting not only changes in technology, but also a change in legal paradigms. Prior to the mid-twentieth century, all countries' criminal codes focused principally on the protection of tangible objects. However, the emergence of an information-based society placing great value and dependence on incorporeal values and information has predicated the development of new laws to protect incorporeal values [7].

The criminal law must therefore keep abreast of these technological developments which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse.

The question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (*locus delicti*) and which law should accordingly apply, including the problem of *ne bis idem* in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts pose a serious setback in administering justice in cyber crime cases.

Computer crime laws in many states prohibit a person from performing certain acts without authorization, including 1) accessing a computer, system, or network; 2) modifying, damaging, using, disclosing, copying, or taking programs or data; 3) introducing a virus or other contaminant into a computer system; 4) using a computer in a

scheme to defraud; 5) interfering with someone else's computer access or use; 6) using encryption in aid of a crime; 7) falsifying e-mail source information; and 8) stealing an information service from a provider (www.criminal.findlaw.com/crimes/a-z/computer_crime.html).

4.1. Many Nations Lack Effective Computer Crime Laws

A recent study has found that Russia and many other CIS countries, as well as some nations in Eastern Europe, lack effective laws for fighting computer crime. That makes them fertile ground for various kinds of Internet- or computer-based fraud and, at the same time, undermines their participation in the growing international Internet economy [8].

"The reason for this is that existing laws may not cover the crimes that are committed in cyber space, either crimes committed by computers or crimes against computers. So, as the Philippines found out, even though they have laws against destruction of property and breaking in and entering and all the normal crimes, [the laws] did not cover the particular activities [of] the "Love Bug" virus perpetrator. And so, we're just warning that may be the case in other countries as well."

Even among countries rated with "substantially" or "partially" updated legislation, the report says crimes are not defined in the same way. In some countries, unauthorized access to a computer is a crime only if harmful intent is present. In others, data theft is a crime only if the data relates specifically to an individual's religion or health, or if the intent is to defraud. Many laws are described as biased in favor of the government.

One of the critical issues for effective enforcement of existing or upcoming computer legislation in all countries is the readiness of law-enforcement officials to cooperate internationally. The very nature of computer crime makes it global and the point of origin is often irrelevant [8].

5. Nigerian Government's Historic Move

The Nigerian Government made a historic move with the National Committee on Financial Crimes (inaugurated December 4, 2001) clamped down on fraudsters in the country by arresting 62 suspect dupes (now facing interrogation) to shut down all business centers, cyber cafes, and internet service providers engaged in scams. The committee had started probing many advance fee fraud cases having international linkages as well as cases within the country involving huge amounts of money. The *modus operandi* of international scam is the connivance of some Nigerian businessmen with foreign counterparts to dupe victims who are eager to import goods to the country. He cited the incident that occurred in Dubai, where some Nigerian businessmen lured some persons to transfer money abroad for the purpose of receiving goods, which were not seen many months after [9].

On September 24, 2002, we received the following e-mail with "US warns Nigeria over online fraud schemes" as subject from Gideon F. For-Mukwai of IDG News Service\Southern Africa bureau (IDG.net): Online schemes operating out of Nigeria that have defrauded

victims out of tens of millions of dollars have become so pervasive that the U.S. government has given the West African country until November to take steps to decrease such crimes or face sanctions.

Financial fraud is now reportedly one of the three largest industries in Nigeria, where the anonymity of the Internet is being used to give crime syndicates a windfall. One oft-used form of fraud is known as "419," a reference to Article 419 of the Nigerian criminal code, and involves scam artists sending unsolicited e-mail, fax or letter proposing either an illegal or a legal business deal that requires the victim to pay an advance fee, transfer tax or performance bond or to allow credit to the sender of the message.

Victims who pay the fees are then informed that "complications" have arisen and they are asked to send more payments, according to The 419 Coalition Web site, which explains the scam, offers rules for doing business with Nigerian companies and individuals and provides specific instructions for recourse to residents of Canada, the U.S., the U.K. and South Africa. The global scam, which has been going on since the early 1980s had defrauded victims out of $5 billion as of 1996, according to the Web site. The 419 scams and other online fraud are causing damage to the budding Internet markets of West Africa because consumers are wary of doing business with Nigerian companies and those in neighbouring countries. Europeans have been victimized more by the fake online investment deals than have others, according to government and media reports.

The U.K. National Crime Intelligence Service has counted more than 78,000 letters linked to online schemes sent to London residents. The letters have defrauded residents there out of more than £24 million (US$37.2 million). Some of the criminals are full-time professionals who have set up sophisticated but bogus e-commerce shop fronts with high-class Web sites, Emmanuel Akutu, of Softrail Nigeria has said.

5.1. Computer Crime Act (Nigeria)

The online criminal activity has spread to other countries, including Ghana, Liberia, Togo and the Ivory Coast, where technology literacy is improving rapidly with government aid and policies of promoting Internet penetration. Of all these nations, only Ghana has a viable Computer Crime Act that was one of the first in the world. Nigeria is preparing to enact such Act as it has set up a committee (National Committee on Financial Crimes, hereinafter abbreviated as NCFC) comprising IT professionals, representatives of the Ministries of Justice and Science and Technology, the National Assembly, the Central Bank of Nigeria (CBN), State Security Services (SSS), and the Nigeria Intelligence Agency (NIA). Already, the Nigerian government has set up a special fraud unit, which includes members from a range of agencies including the State Security Service and the Nigeria Intelligence Agency with Mr. Charles Akaya, doubling as Commissioner of Police and Chairman. The fraud unit has made many arrests, but no one has been successfully prosecuted, according to news

accounts, because of paucity of computer related Criminal Act in the country's legal books. The Nigerian Government has also set up a website to help investors deal with fraud in addition to media campaign in US and Europe, aimed at tackling the scheme.

The most recent action on this has been the presentation of THE COMPUTER SECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION BILL 2005 (Sb254, 2005) to the National Assembly for consideration. This Bill has passed second reading. The Bill seeks to secure computer systems and networks in Nigeria as well as protect critical information infrastructure by providing criminal liabilities and penalties for undesirable activities carried out using computers and other information and communication technology devices [10].

5.2. Nigerians arrested over Internet Fraud (South Africa)

No fewer than 15 Nigerians among others were arrested and being quizzed over Internet fraud in South Africa. A group of suspected Internet racketeers, who fooled people into sending them money from the central bank of South Africa, have been arrested, detained and would appear in court, showing that South Africa has updated her laws to deal with Internet fraud. The gang was reported to be diverting phone calls and creating fictitious email addresses to fool people [11a].

Nigerian money offers like this have been described as the fastest growing type of internet fraud. Reports of e-mailed Nigerian money scams designed to obtain recipients' bank account details by offering to transfer large sums to them for safekeeping rose by 900 percent between 2000 and 2001, according to NCL, the main United States of America consumer lobby. Sadly, scams of this kind, which often emanate from Nigeria or other African countries, have been circulating for years through the post or by fax. In 1996, global scam defrauded victims $5 billion according to the figures released by the 419 coalition. The United Kingdom (UK) National Crime Intelligence Service said it has received over 78,000 letters linked to online schemes to London residents. The letters were used to defraud residents of more than $37.2 million.

All these illegal activities supported by the catalogue of several incidents with no feasible or concrete steps taken by the home country (Nigeria) to stem the rising tide made the US Government send out the stern warning to the Nigerian Government.

5.3. Anti-fraud Bill signed by President Obasanjo (Nigeria)

A Paris-based Financial Action Task Force (FATF) gave Nigeria December 13, 2002 deadline to enforce stiffer penalties on financial crimes or face blacklisting for failing to join other nations at combating sophisticated organized crimes. In a quick response to this threatening warning (not an empty threat considering the high rate of high tech crimes linked with Nigerians in the recent months), President Olusegun Obasanjo of Nigeria forwarded three separate bills to the National

Assembly praying the legislators for expeditious consideration. According to the news accounts, the three bills sent were: Bank and Other Financial Institutions (Amendment) Bill; The Anti-Terrorism, Economic and Financial Crimes Commission Bill; and The Money Laundering (Amendment) Bill. The implications of any sanctions on Nigeria as a result of her failure to act promptly, positively, and be demonstrated as the true sense of purpose of the move against high tech crimes would include a stoppage of financial flows accruing from international trade and business transactions [11b].

Prior to the warning from FATF, the report added, the Central Bank of Nigeria had written to the Federal Government alerting her of Nigeria's inclusion in the list of countries to be blacklisted by the FATF for failing to join the war against terrorism as well as financial and economic crimes.

Reports also had it that the National Assembly considered the Bills expeditiously for the President's assent on December 12, 2002 to beat the December 13 deadline for Nigeria to be left off the hook. Between December 12 and 13, 2002, President Olusegun Obasanjo of the Federal Republic of Nigeria assented to the bills passed by the National Assembly to deal decisively with various Information and Communications Technology-related crimes in a quick move to avert US sanctions.

The question that remains unanswered is: Have we taken steps to ensure the appropriate members of our federal/state/local judiciary system, and sworn law enforcement officers from the federal/state/local agencies, and the Law enforcement support personnel from federal/state/local agencies, i.e. enforcement analysts, crime scene/crime lab personnel, information systems personnel, evidence technicians, etc. been equipped with the requisite technical training to collect, analyze, preserve, and present technical and/or electronic evidence that would be adjudged "admissible evidence" to pursue and prosecute the arrested crime suspects and future suspects? From my findings during the course of this project, the answer to this one million naira question is capital NO.

Another positive step recorded by Nigeria, was another news accounts that Nigeria and the US on Wednesday, January 15, 2003, exchanged the instrument of a treaty symbolizing an exchange of mutual legal assistance in criminal matters to fight against transnational crimes. The event executed by Nigeria's Minister of State for Foreign Affairs, Chief Dubem Onyia, and the US Ambassador to Nigeria, Mr. Howard Jeter on behalf of their countries, represented in no small measure the sincerity of purpose expressed by Nigerian President when he addressed the UN Assembly session in September 2002 to leave no stone unturned at achieving victory in warring against the image damaging high tech crimes. This was again stressed by Chief Onyia at the occasion by saying the treaty was expected to provide relevant cooperation in the fight against modern transnational organized crimes, listed as including drug trafficking, financial crimes, terrorism, and human trafficking. The treaty containing 23

articles was designed to be self-executing to enhance the ability of both countries to investigate and prosecute drug offences, money laundering, and related transnational crimes, the report concluded [12].

6. Challenges To The Law Enforcement Agencies

The technology revolution is here and it's not only assisting law enforcement, it's working overtime for criminals. Is your agency ready to respond? Electronic crime is having a serious impact on law enforcement. The growth of technology and Internet use offers more opportunities to criminals with larger payoffs and fewer risks. For state or local law enforcement agencies with limited personnel and resources, staying current on the latest computer technologies and scams has proven to be a daunting, sometimes insurmountable task.

The use of Information and Communication Technology by government, non-government, and international criminal organizations will therefore clearly have an increasingly important impact upon the functioning of law enforcement and security agencies in the information age. The countermeasures to high tech crimes also raise fundamental questions for the study of criminology, the law and policing policies.

Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct e-business within a country and across national boundaries.[Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e-commerce.ÊAs e-business expands globally, the need for strong and consistent means to protect networked information will grow.

6.1. Obtaining evidence of criminality

Several factors make high tech type of criminality difficult to address. Lawbreakers have integrated highly technical methods with traditional crimes and developed creative new types of crime, as well. They use computers to cross state and national boundaries electronically, thus complicating investigations. Moreover, the evidence of these crimes is neither physical nor human but, if it exists, is little more than electronic impulses and programming codes. Regrettably, the police have fallen behind in the computer age and must overcome a steep learning curve. To make matters worse, computer crime is sometimes difficult for police officials to comprehend and to accept as a major problem with a local impact, regardless of the size or location of their communities.

This includes computers or other items of hardware upon which allegedly illegal material is held. Provisions exist such that:

- where a computer system has been used for purposes other than the distribution of pornography, would it be wrong to seize the whole system? Would it be admissible as 'best evidence' if investigators could copy the required material from the system?

- where the conduct occurs entirely on the premises of the victim, no particular problems may be anticipated. In the acquisition of evidence. All matters will be within the control of the computer user and, assuming their willingness to cooperate, there are no legal problems facing the acquisition of evidence.
- greater difficulties arise where access is obtained remotely;
- the problem may remain of identifying the intruder. The introduction of systems of caller identification might facilitate the task of obtaining such information, at least at the level of identifying the telephone number from which a call originated.

6.2. The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 replaced the Interception of Communications Act 1985. However, the new Act retains the basic structure for the provision of warrants to authorise the interception of communications where this is considered by the Secretary of State to be necessary i.e.

(a) in the interests of national security

(b) for the purpose of preventing or detecting serious crimes

(c) for the purpose of safeguarding the economic well-being of the nation; or

(d) for giving effect to international mutual assistance agreements in connection with the prevention or detection of serious crimes.

6.3. Public Awareness and Education

Public awareness and education is number one. For law enforcement, increased training is keynot only for the people responsible for protecting the industry from these types of attacks, but also for those investigating it. Law enforcement agencies must respond to the world-wide growth in computer-related crime. Law enforcement has withstood many challenges over the years. Prohibition, organized crime, riots, drug trafficking, and violent crime exemplify some of the complex problems the police have faced. Now law enforcement confronts another problem that is somewhat unusual--computer-related crime.

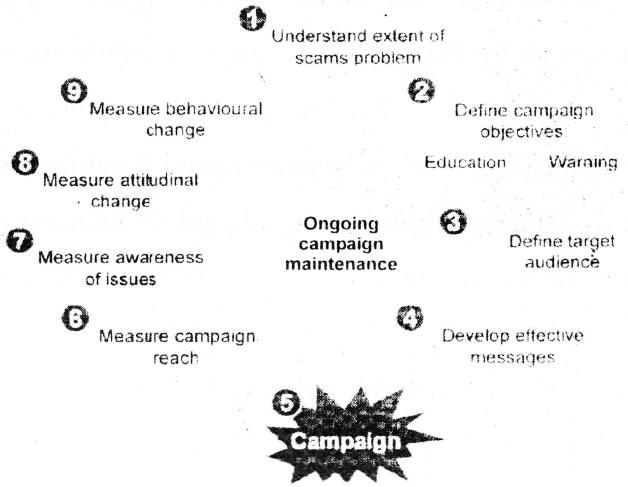


Figure 1 Good Practice in anti-spam campaign
Source: OECD, 2005

Table 1 Good practice in evaluating anti-spam campaigns

Stage	Key questions	Examples of approaches
1	What types of spam are occurring? How big is the spam problem? Who is affected?	▪ Operational information from enforcement agencies ▪ Quantitative surveys to measure consumer knowledge and stated confidence ▪ Qualitative discussions to elicit real levels of knowledge and information needs
2	What skills do consumers need to deal effectively with spams? What information/warnings do they need to avoid specific spams?	
3	Which consumers are at greatest risk?	▪ Operational and survey data analysed to identify demographic groups with high vulnerability ▪ Segmentation analysis to identify clusters of consumers who share similar attitudes or behaviours likely to put them at risk
4	How can we reach these audiences? Which approaches communicate the messages in the most compelling way?	▪ Strategic media planning to identify suitable channels to reach specific audiences ▪ Qualitative discussions and pre-testing to refine creative routes by exposing members of the target audience to draft messages or advertisements
5	What response is the campaign generating?	▪ Monitoring and analysing the source and nature of calls to helpline, visits to Web sites
6	Who has been exposed to the different campaign elements? What do they remember about them?	▪ Media analysis of PR coverage ▪ Quantitative pre-campaign and post-campaign surveys to measure changes in levels of campaign recall and recognition, and shifts in attitudes ▪ Further systematic survey measurements over time to track changes in attitudes and behaviour
7	Are the target audiences aware of the dangers and sources of help?	
8	Have the attitudes of the target audiences changed as a result of the campaign?	
9	Has the way people deal with spams changed as a result of the campaign?	

Source: Summary table of good practice in evaluating anti-spam campaigns by OECD, 2005 [13]

6.4. Computer Crime Task Forces.

Consideration should be given to a task force approach for investigating Computer Crimes and providing the investigators with the forensic resources so critical to these investigations. This is especially true for those agencies without sufficient crime loads to justify staffing these units full time. The pooling of talent, resources and funding can have a significant impact on these types of investigations. This does not necessarily mean that the member agencies need to be housed in the same facility. The most important aspect of the task force effort is that the agencies work together on coordinated efforts. State and federal grants would certainly encourage development of these task forces [2].

7. Conclusion

Computer-related crime, like other crimes, is a growing problem in both the Government and the private sectors. The pace at which IT is moving is difficult to be caught up with by non-practitioners of related functions and capabilities, while the criminals have no other assignment than to be advancing in their knowledge acquisition to beat the laws.

Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tends to be far greater than the losses associated with each incident of other white collar crimes. Sources of illegal activity often require advanced computer skills to be detected as a consequence of their anonymous character. Cases of bank robbers using portable radios to intercept police transmissions and more recently the utilization of mobile cellular phones for evading police detection are now witnessed in Nigeria.

Most computer-related crimes are not reported to the Police, especially those affecting financial, insurance, and healthcare services providers for fear of losing their customers' confidence, except rare cases of huge amounts. The opportunities for computer-related crimes in financial institutions, government programmes, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great. Financial fraud is the most leading industry in Nigeria, where the anonymity of the Internet is being used to give crime syndicates a windfall.

This paper has exposed the various areas of Information Communications Technology-related crime perpetrated in and around Nigeria, by Nigerians and non-Nigerians (pseudonym Nigerians) to serve as a working document towards: abrogating archaic laws and enhancing our legal system in dealing with the latest crime wave especially those that are IT-related; enhancing and empowering our law enforcement agents in analysing and presenting computer-evidence as admissible in law courts for prosecuting and/or convicting IT-enabled crime suspects; building confidence in computer users to use computers and other emerging technological resources with assurance of a reasonable level of protection of their rights and property; guaranteeing privacy protection, protection of intellectual property rights and discourage piracy; and deploying and using Information Technology within adequate legal framework.

References

[1] M. **Castells**, 1998. *The Information Age*. Volume 3: *End of the Millennium*. Oxford: Blackwell.

[2] **Koenig,** Dan (2002) Investigation of Cybercrime and Technology-related Crime, Los Angeles Police Department, Los Angeles, California, USA, *March 2002*, http://www.neiassociates.org/cybercrime.htm accessed December 7, 2006

[3] **Carter**, David L, and Andra J. Katz (1997) "*Computer Crime: An Emerging Challenge for Law Enforcement*", http://www.fbi.gov/leb/dec961.txt, February 03, 1997

[4] **Kirby**, Michael (1999) *Privacy in Cyberspace*. University of NSW Law Journal.

[5] Commonwealth Government (June 2000) *Advisory Report on the Privacy Amendment Bill 2000*..

[6] **McConnell**, Bruce W (2000), "*Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*", McConnell International LLC, December 2000. (www.mcconnellinternational.com)

[7] **Goodman**, Marc D. and Susan W.. **Brenner** (2000).The Emerging Consensus On Criminal Conduct In Cyberspace

[8] **Krastev**, Nikola (2000) " East: Many Nations Lack Effective Computer Crime Laws", Radio Free Europe / Radio Liberty, Inc., http://www.rferl.org

[9]. **Akaya**, Charles[Commissioner of Nigeria Police], and Olise, Alex[Police Affairs Reporter] (2002) "*Anti-scam body trails fraudsters, arrests 62*" , "The Guardian Nigeria-based newspaper", Monday November 25, 2002, last page.

[10] FGN (2005) Federal Government of Nigeria's Computer Security & Critical Information Infrastructure Protection Act 2005 (http://www.cybercrimelaw.net/laws/countries/nigeria.htm)

[11a] "The Punch - Nigeria-based newspaper" (2002b), "*15 Nigerians, among others quizzed over Internet fraud*" The Punch - Nigeria-based newspaper, Tuesday, August 20, 2002, page 30.

[11b] "The Punch", Nigeria-based newspaper" (2002d). Wednesday, November 20, 2002 p. 64 (last page). Senan John Murray, the Abuja correspondent in "*Financial crime: Nigeria set to beat deadline on legislation:*".

[12] "The Punch" of Thursday, January 16, 2003 (p.8) *"Nigeria, US seal pact on organized crimes"* - Chinwe Ogbuka

[13] OECD (2005), Examining consumer policy: A report on consumer information campaigns concerning scams, *UK Central Office of Information (COI), UK Department of Trade and Industry*, **OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France** , internet material , accessed December 6, 2006, available at www.olis.oecd.org/.../43bb6130e5e86e5fc12569fa005d004c/911996b0a67a8e9cc12570dd003bd320/$FILE/JT00196254.DOC