Journal of Computer Science & Its Applications, December 2006, Vol. 13 No.1

Cybercrime Pervasiveness, Consequences, and Sustainable Counter Strategies

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

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

Fasina E. P.
Department of Computer Sciences,
University of Lagos, Nigeria
epfash@yahoo.com

ABSTRACT

As our connectivity and dependency on technology increases, so does our vulnerability. Technology has provided not only new tools, but also new opportunities for criminals in the digital world. The abuse of new technologies has been threatening economic and financial security and actually devastating the lives of affected individuals. In Nigeria, cybercrime has recorded mostly foregin-based individuals and organizations as victims thereby getting Nigeria ranked among the nations with notorious pervasiveness of high-tech crimes. Indeed, adequately formulating a strategy to contain the menace of cybercrime presents a formidable challenge to law enforcement. This paper x-rays noted instances of cybercrime pervasiveness, its devastating consequences, and up-to-date countermeasures in Nigeria. It develops an enforceable/sustainable framework to determine how critical infrastructures are put at risk and how law enforcement should react in responding to the threats.

1. Introduction

The last 20 years have been characterized by rapid improvements in information technology and have come to be regarded as the "Information Revolution." The Information Revolution is changing the speed at which information is communicated, the facility with which calculations can be conducted in real time, and the costs and speed of observation of physical phenomena. Applications of IT in transportation mean that people and goods can be moved more efficiently; applications to the production process mean that goods and services can be produced more efficiently [1].

The Internet is making the world smaller through improved communication and simplifying logistical barriers for businesses. It breaks down barriers between (and within) nations, opening up economies and democratizing societies. The Internet makes it possible to distribute any kind of digital information, from software to books, music, and video, instantly and at virtually no cost. Protecting intellectual property and regulating global

commerce are significant challenges, however, and we are only at the dawn of the Internet Age. Given the needs of effective prevention and prosecution of cybercrime and the associated privacy issues, the potential impact on business activities, and other relevant factors, the views of interested parties, including law enforcement, nongovernmental and private sector organisations, may be useful to these consultations.

Data held by Internet service providers and other private sector entities is often critical to identifying criminals and solving law enforcement investigations. In the year 2004, a new form of Internet attack has increased in use and sophistication: *phishing*. Criminals send users emails that appear to be from their bank, Internet service provider, or other online service asking them to input their passwords, bank account numbers, or credit card numbers. They then use this information for their own financial gain. Hackers have created large networks of computers that they can control using *bots*. Criminals use these *botnets* to deliver powerful denial of service attacks, to extort people and companies, and to send spam.

Many APEC Members have considered how best to protect their critical infrastructures – those systems, such as electrical power, banking and finance, and telecommunications, that underlie the health and stability of an economy. In particular, as these functions are increasingly controlled by computers and computer networks, how are critical infrastructures put at risk, and what should we do to provide an effective response to cyber-based attacks on them? In responding to the threat of Phishing, Identity Theft, and Botnets, pertinent questions to be answered include: How should we respond to these growing threats? Are there technical solutions? How should law enforcement react? Are there actions that should be taken together? In recent years, legislatures around the world have examined legal frameworks for combating cybercrime and have enacted new laws to address the threat. Certain economies have recently amended their cybercrime laws or are in the process of amending them now. Cybercrime investigations routinely require cooperation between law enforcement agencies [2].

Americans face growing security threats, both at home and abroad, from international terrorist networks and their allies in the illegal drug trade and international criminal enterprises. Illegal drugs impose a staggering toll, killing more than 19,000 Americans annually and costing more than $160 billion in terms of law enforcement, drug-related heath care, and lost productivity. This is in addition to the wasted lives; the devastating impact on families, schools, and communities; and the generally corrosive effect on public institutions. International crime groups also pose critical threats to U.S. interests, undermine the rule of law and enable transnational threats to grow. International trafficking in persons, smuggling of migrants and contraband, money laundering, cyber crime, theft of intellectual property rights, vehicle theft, public corruption, environmental crimes, and trafficking in small arms cost U.S. taxpayers and businesses billions of dollars each year. Experts estimate that non-drug crime accounts for half of the estimated $1.8 trillion of money laundered each year globally [3].

The rapid adoption in emerging countries of the new information and communication (ICT) infrastructures such as the internet is creating new opportunities for these countries and their citizens to participate in the world's flow of information, ideas and commerce. However, new opportunities offered by the use of ICT also generate new risks and vulnerabilities. In developing countries, ICT Ministers are also seeking to stimulate the use of the internet and similar technologies to broadly offer their citizens new e-economy and e-government services such as email and online banking, often for the first time.

These efforts may be vulnerable due to a lack of cyber security; there are reports that the great majority (95%) of email traffic in developing countries is spam. This level of spam discourages people from using email, greatly decreasing the utility of email, and reduces user's confidence in any online activity. Multinational corporations who are seeking to do business in such countries, either by outsourcing tens of millions of dollars of work or investing hundreds of millions of dollars to build a plant locally, have to be certain that ICT-based capabilities they develop are going to be accessible and secure. This means that countries who want investment must have a rational approach to cyber security—it is becoming part of the package corporations must and will consider [4].

Cyber-Crime ('computer crime') is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. In a wider sense, 'computer - related crime' can be any illegal behavior committed by means of, or in relation to, a computer system or network, however, this is not cyber-crime.

The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Vienna, 10-17 April 2000) categorized five offenses as cyber-crime: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception of data to, from and within a system or network, and computer espionage.

Cybercrimes are becoming increasingly pervasive and sophisticated, and can have more severe economic impact than many conventional crimes. Technology and skill intensiveness, a high degree of globalization, and their newness make cybercrimes structurally different. The characteristics of cybercriminals, cybercrime victims, and law enforcement agencies have a reinforcing effect on each other, leading to a vicious circle of cybercrime [5]. Current and ongoing Internet trends and schemes have been identified by the Internet Crime Complaint Center as: Auction Fraud; Auction Fraud - Romania ; Counterfeit Cashier's Check ; Credit Card Fraud ; Debt Elimination ; Parcel Courier Email Scheme; Employment/Business Opportunities; Escrow Services Fraud; Identity Theft; Internet Extortion; Investment Fraud; Lotteries; Nigerian Letter or "419"; Phishing/Spoofing; Ponzi/Pyramid; Reshipping; Spam; and Third Party Receiver of Funds.

2. Forms of Cybercrime

Cybercrimes range from economic offenses (fraud, theft, industrial espionage, sabotage and extortion, product piracy, etc.) to infringements on privacy, propagation of illegal and harmful content, facilitation of prostitution and other moral offenses , and organized crime. At its most severe, cybercrime borders on terrorism, encompassing attacks against human life and against national security establishments, critical infrastructure, and other vital veins of society.

Cybercrimes travel well internationally – some are activated from one country and target another; others are transferred when coming to the end of their life cycle in their country of origin. However, despite the variety of cybercrimes found in various countries, there are just four main templates being used:

1. Advance fee fraud. This covers the range of cybercrimes where the victim is encouraged to send payment in advance to facilitate a larger payment back. It includes bogus lotteries and prize draws, so-called '419' cybercrimes, loans and other financial services. Many work-at-home schemes also follow this format, as do pyramid selling schemes that require payment up front.
2. Mis-sold goods/investments. This covers those

cybercrimes where the value of the product purchased does not match the sales pitch. 'Miracle' health cures are one example here; worthless investments (often sold in telephone sales rooms, dubbed 'boiler rooms') are another. The Internet has provided many new opportunities here, as consumers do not have the same expectations of seeing the product before committing to purchase. The increasing popularity of Internet auction sites in particular encourages cybercriminemers to explore this area.

3. 'Free' offers. These are incentives given to make a purchase that – on receipt – is not what it seems. Free holidays to timeshare resorts are a key example here.
4. Hidden charges. Hidden premium rate telephone services (perhaps to claim a prize) are the classic hidden charge cybercrime [6].

The Cyber-Crime and Intellectual Property Theft program seeks to collect and disseminate data and research on six 'popular' categories of cyber-crime that directly impact citizens and consumers and to educate these groups on the scope and depth of the problem, as well as current policies and research aimed at addressing the issue.

The categories of cyber-crime addressed are:

- Financial - crimes which disrupt businesses' ability to conduct 'e-commerce' (or electronic commerce).
- Piracy - the act of copying copyrighted material. The personal computer and the Internet both offer new mediums for committing an 'old' crime. Online theft is defined as any type of 'piracy' that involves the use of the Internet to market or distribute creative works protected by copyright.
- Hacking - the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism, etc.) are committed.
- Cyber-terrorism - the effect of acts of hacking designed to cause terror. Like conventional terrorism, 'e-terrorism' is classified as such if the result of hacking is to cause violence against persons or property, or at least cause enough harm to generate fear.
- Online Pornography - According to 18 USC 2252 and 18 USC 2252A, possessing or distributing child pornography is against federal law and under 47 USC 223 distributing pornography of any form to a minor is illegal. The Internet is merely a new medium for this 'old' crime, but how best to regulate this global medium of communication across international boundaries and age groups has sparked a great deal of controversy and debate [7].

3. Pervasiveness of Cybercrime

While agreeing that greed forms a major causative factor in the spread of cyber crime in Nigeria, one cannot actually shy away from the fact that the harsh economic situation in the country, which has created mass unemployment and of course the high rate of corruption in the society is the fuel that fans its embers [8]. 419 is one of the ills of the society and there is nobody that will feel happy about it except that person is a 419er. It is one of the negative things that we have in our society and it is unfortunate.

4. Consequences of Cybercrime

Cybercrime presents the nations of the world with a problem they have never before had to address, i.e., the permeability of national borders. As long as crime remained a "real world" phenomenon which required the commission of some overt act or omission which, by definition, had a circumscribed geographical reach, localized, idiosyncratic criminal laws were sufficient to protect a nation's citizens from those who would do them harm [9].

Cyber crime covers all forms of Internet fraud, which involve the use of computers or the Internet to access information illegally. The criminals take advantage of the unique peculiarity of the spread of the Internet to send information from any part of the world and access it in other parts of the world in a matter of seconds or minutes [8].

The use of electronic media, especially the Internet to commit crime has been a major form of embarrassment for Nigeria for sometime. Time and again, the news from many parts of the world is that Nigerians keep swindling people through the Internet and by credit card. While some perpetrators of such crimes in the home front have been arrested in the past, one of the limitations in prosecuting such persons is the inadequate legislation that currently exists and the inability of the Nigerian law enforcement agencies to handle such issues, given the technical requirements [10].

Cyber crime has denied Nigeria a lot of investment and educational opportunities and dented the country's image very badly in the international community. This illegality could be perpetrated through hacking, distribution of hostile softw are such as viruses and worms, e-mail scams, denial of service attacks, theft of data, fraud, impersonation and extortion [8].

The 2005 report of the Internet Crime Complaint Center says "Of those individuals who reported a dollar loss, the highest median losses were found among Nigerian letter fraud ($5,000), check fraud ($3,800), and other confidence fraud ($2,025) complainants. The 2001 report says the "Nigerian Letter Scam" was the third highest cause for complaints with 15.5% of complaints; the median amount loss was $5,575 [11].

Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security. Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal. In actual fact, each category of computer crime identified by McConnell International LLC and Professor David L. Carter exists in each developing country, including Nigeria. The identification and awareness of these developments are being checked in the developed countries where stiff penalties have been stipulated in their revised criminal laws, most of the developing countries including Nigeria are yet to take update their archaic laws as rightly pointed out in McConnell International LLC's report.

5. Global Cybercrime Convention

Owing the dangers of cybercrime and the need for common minimum technical and legal standards to fight such crime at a global level, the Convention on cybercrime (ETS N° 185) was prepared by Council of Europe member States and Canada, Japan, South Africa and the United States. It entered with force on 1 July 2004. Its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS N° 189) entered into force on 1 March 2006.

The Convention is the only binding international instrument dealing with cybercrime. It has received widespread international support and is open to all States. The Convention provides for consultations of the Parties (the Convention Committee on Cybercrime [12].

6. Success Stories

In recent years, legislatures around the world have examined legal frameworks for combating cybercrime and have enacted new laws to address the threat. Certain economies have recently amended their cybercrime laws or are in the process of amending them now. Such progress, however, is rarely quick or easy (KOO, et al, 2005).

THE COMPUTER SECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION BILL 2005 which 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 has been introduced in the National Assembly [13].

6.1. Nigeria's EFCC Efforts

Economic and financial crimes like Advance Fee Fraud (419), money laundering, and corruption etc have had severe negative consequences on Nigeria, including decreased foreign direct Investments in the country and tainting of Nigeria's national image. Recognition of the magnitude and gravity of the situation led to the establishment of the Economic and Financial Crimes Commission (EFCC)

(http://www.ex.ac.uk/~RDavies/arian/scandals/official.html).

Among the businesses that have altered the estate's (Festac Town, Lagos) skyline are the ubiquitous cyber cafes, which were opened by discerning entrepreneurs to bring the benefits of advances in information and computer technology to the doorsteps of ICT freaks in the neighborhood. That industry is one of internet fraudsters. Indeed, youngsters in their teens or early 20s have found the settlement a natural haven for new wave of advance fee fraud in the mould of internet fraud and other cyber crimes. These genres of fraudsters who are the nouvre riches in the area are called 'Yahoo Yahoo Boys', for their penchant to always visit the cyber cafés that dot the neighborhood to surf the net. Their life styles betray their involvement in hi-tech cyber crimes. They drive the most expensive cars; wear designer clothes and hang out in the coolest spots in the neighborhood. Because the crime is cyberbased, locating the crooks is particularly difficult.

As it was, EFCC had proved beyond the case against Odiawa beyond reasonable doubts. At least 48 of the 58-count charge preferred against Odiawa were upheld by the judge. The pronouncement of the trial judge, Justice Olubunmi Oyewole that "I hereby convict the accused person as charged on each of the said counts respectively," effectively opened the prison gates for Odiawa. As the judge rose, Odiawa walked slowly out of the dock into the waiting alms of the prison officials with his head bowed. He was chained on both hands and legs and taken to the Kirikiri maximum security prisons in Lagos, for his 376 jail term, which the court said, was to run concurrently for 12 years. Odiawa was first arraigned before the court on a 54-count charge on January 10, 2005, to which he pleaded not guilty. Subsequently, the charge was amended on a number of occasions until it became 58 counts on July 14, 2005.

The judge noted that there was indeed a scam to which the American businessman fell victim due to what the judge described as greed and naivety, a situation that led to his financial impoverishment and subsequent

indictment and conviction for which he is presently serving prison term in the United States of America, his home country. Satisfied that the telephone lines with which the fraud was alleged facilitated were recovered from the accused person, the court agreed with prosecution that all the payment into the coffers of the syndicates were all at the express consent of the accused with whom the victim had interacted for over a hundred times through telephone conversations, emails and telex. Odiawa is paying the price for conning an American, George Blick and obtaining money totaling N3billion from him over period of one year, from April 2003 to August 2004 [14].

Nigerian Amaka Anajemba, who had been widowed at the young age of 37, was caught in the largest financial scam of its type in her country's history, one in which the perpetrators stole a total of $242 million. But before you work up too much sympathy for Anajemba, you should know that she wasn't a victim of the scam — she was one of its perpetrators. The $100 million we've confiscated from spammers and other defendants is the least that cybercrime has cost our country. Our economy has lost hundreds of millions of dollars in foreign investment because our credibility and the trust of the international community have been affected. Nigerians can't even use financial instruments as basic as mail orders; if it comes from Nigeria, it's suspect [15a]. We're interested in fighting cybercrime globally, of course, but working with Nigeria held particular attractions for us. The EFCC is a skilled organisation, with a significant law enforcement infrastructure backing it, and Nigeria has the political willingness to take action against cyber criminals. As much as they were doing on their own, they were comfortable with the idea of getting help from us to do even more [15b].

Three Internet fraudsters who connived with an employee of a courier company to dupe a Swiss national have been held by the police in Oyo State. The suspects, Jeremiah Elijah, Bukola Adefisayo and Bawa Monsur, were alleged to have defrauded one Mrs. Goedner, through Adefisayo who worked with the company [16].

6.2. EFCC's IT Strategy To Contain Cybercrime

Cyber crime presents a major challenge to the Economic & Financial Crimes Commission (EFCC) struggle to rid the country of Economic and Financial crimes and other related crimes. Whereas the traditional crime is local and easily understood, cyber crime is complex and most often requires enormous resources and expertise to contain. Today, the computer has become an integral part of our way of life. However, as our connectivity and dependency on technology increases, so does our vulnerability. The abuse of new technologies may threaten economic and financial security and actually devastate the lives of affected individuals. It is estimated that nearly every crime committed today has a technology component, usually a computer. Technology has provided not only new tools, but also new opportunities for criminals in the digital world. Indeed, adequately formulating a strategy to contain the menaces of cyber crime presents a formidable challenge to law enforcement. Cyber crime today is characterized by profit driven motives involving organized crime syndicate like the "Yahoo Boys".

It is therefore reasonable to assume that the growth in technology uptake will be accompanied by an increase in the incidence, scope and complexity of cyber crime. Along with a strong enforcement regime, the EFCC has adopted the following IT based strategy to deal with the menace of cyber crime:

Partnerships:

The EFCC has signed a Memorandum of Understanding, MOU, with Microsoft to specifically combat Cyber Crime through information sharing,

collaboration and capacity building. The EFCC - Microsoft MOU is historic, the first of its kind MOU between an African government and Microsoft which defined the framework for cooperation between EFCC and Microsoft to fight cyber crime. The Commission having recognized the need for collaboration to facilitate the exchange of information and intelligence in order to detect, prevent and respond to cyber crime, has also signed MOUs with a number of international agencies like the Office of Fair Trading, UK (OFT), Spots Spam of EU, Gi8 24/7 Network, NHTCU, etc.

Resources and capacity: The EFCC has also recognized the need to enhance capacity and thus embarked on skills acquisition particularly in the area of specialist forensic computing which involves the process of identifying, preserving, analyzing and presenting digital evidence.

Prevention: The Commission has identified the need to acquire interception and surveillance capabilities to effectively respond to the threat of cyber crime.

Regulation and Legislation: the Advance Fee Fraud and other related offices (Amendment) Act 2005 invests on the Commission among other things the responsibilities and power to:

a. Effectively monitor and supervise Internet Service Providers (ISPs), Cyber Café's etc.

b. Prescribe penalties for non-compliance.

However, the nature and methods of cyber crime is constantly changing. Therefore the Commission would continually strive for improve legislation to address the complexities associated with cyber crime. Finally, cyber crime presents a unique challenge that requires a well co-ordinated strategy for enhanced national and international collaboration between the law enforcement agency and the private sector as exemplified in the EFCC-Microsoft partnership. The Commission has set itself the goal of curtailing the menace of cyber crime particularly the scam mails a.k.a. 419 mails originating from Nigeria. It is a goal that is achievable with appropriate technology, collaboration: information sharing and people based solutions [17].

6.3. US Department of Justice [18].

- Defendant Sentenced in Online Piracy Crackdown (December 19, 2006)
- Two Michigan Residents Plead Guilty to Criminal Copyright Infringement (December 15, 2006)
- Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China: Third Foreign Economic Espionage Indictment in the United States Since the Enactment of Economic Espionage Act of 1996; Source Code Used for Military Combat Simulation and Banned for Export Without License (December 14, 2006)
- Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China: First Conviction in the Country for Foreign Economic Espionage (December 14, 2006)
- Utah Man Sentenced to 24 Months in Prison for Bringing Down Wireless Internet Services (December 14, 2006)
- Vermilion, Ohio Man Charged with Wire Fraud (December 14, 2006)
- Hollywood Movie Pirate Sentenced to 7 Years in Prison for Copyright Infringement and Escape (December 1, 2006)
- Former Vancouver Area Man Sentenced to Five Years in Prison for Conspiracy Involving Counterfeit Software and Money Laundering: Web of Companies Sold up to $20 million of

Microsoft Software with Altered Licenses (November 29, 2006)

- Camcorder Pleads Guilty to Infringing Copyright of Mission Impossible III (November 13, 2006)
- Operator of For-Profit Software Piracy Web Site Pleads Guilty: Caused up to $25 Million in Losses to Software Industry (November 9, 2006)
- California Man Sentenced for Recklessly Damaging a Protected Computer Owned by his Former Employer (October 16, 2006)
- Local Business Owner Sentenced to Year In Jail for Copyright Infringement Conspiracy Related to the Sales of Counterfeit Goods (October 16, 2006)
- California Man Sentenced for Electronically Stealing Trade Secrets from his Former Employer, a Construction Contractor (October 13, 2006)
- Wise, Virginia Man Sentenced in Peer-to-Peer Piracy Crackdown (October 17, 2006)
- Pharmacist Sentenced to Prison for Ordering and Receiving Counterfeit Pharmaceutical Drugs (September 25, 2006)
- Pharmaceutical Distributor Pleads Guilty to Selling Counterfeit Drugs (October 18, 2006)
- Owner of P.C. Consultants of Wadsworth, Inc. Charged with Computer Intrusion of Merrick Graphics' Computer System (September 22, 2006)
- Developer of "HU Loader" Pleads Guilty in Satellite Television Piracy Case (September 21, 2006)
- Hi-Tech Pharmaceuticals & 11 Individuals Indicted for "Generic" Pill Fraud Scheme: Defendants Allegedly Sold Millions of Pills Over the Internet (September 20, 2006)

7. Jurisdictional issues

International fraud is a serious problem. It is essential that persons who commit frauds related to a country should not be able to avoid the jurisdiction of that country's courts simply on outdated or technical grounds or because of the form in which they cloak the substance of their fraud.

"Fraud committed via the Internet makes investigation and prosecution difficult because the offender and victim may be located thousands of miles apart. This borderless phenomena is a unique characteristic of Internet crime and is not found with many other types of traditional crime. Jurisdictional issues often require the cooperation of multiple agencies to resolve a case. This is a hallmark of the Internet Fraud Complaint Center. It streamlines the case initiation effort and saves victims and enforcement agencies a great deal of time." [19].

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes [20].

The news reports of arrest and subsequent

prosecution of 15 Nigerians among others for Internet fraud in South Africa is a clear enforcement of the provisions of the Jurisdiction over Fraud Offences with a Foreign Element Act 1987. More specifically, provision exists for dual jurisdiction where a continuous crime is involved with both countries concerned: "... *where a crime is such that it has to originate with the forming of a fraudulent scheme, and that thereafter various steps have to be taken to bring that fraudulent plan into fruition, if some of these subsequent steps take place in one jurisdiction and some in another, then if the totality of the events in one country plays a material part in the operation and fulfilment of the fraudulent scheme as a whole there should be jurisdiction in that country...*". The basis for any court to claim jurisdiction will be the existence of a significant link with the country in question. Law enforcement officials cannot take action against cybercriminals unless countries first enact laws which criminalize the activities in which these offenders engage.

8. Sustainable Strategies

For the effective implementation of this war plan against cyber crime in Nigeria, the security agencies must be well equipped with up-to-date IT security equipment, software, knowledge and training. The general public, cyber café operators, all tiers of government, security agencies, the Internet Service Providers (ISPs), Internet users, etc., must be enlightened on the need to be alert about security. Nigerian Communications Commission (NCC) needs to mandate cyber café operators to install within their system software packages that will easily detect and filter out scam e-mails. Internet Service Providers should also look into the possibility of making their services more affordable so that many more individuals can have personal access to the Internet from their homes or offices [8].

A holistic strategy for cyber defense and preparedness can prevent liability on behalf of client management, avert potential lawsuits or regulatory action, recover lost revenue, and maintain or restore the reputation and integrity of the firm. Integrated security policies, employee training, and awareness can be a competitive advantage in a business environment increasingly dependent on security and reliability of computer networks.

The urgent need for skilled personnel in all aspects of ICT adoption is therefore one of the clearest priorities in most developing countries. Regrettably the high demand for people with ICT skills ensures that publicly-funded training centres, for example, simply cannot afford to retain good instructors in these areas. Competent people are quickly attracted into the private sector, and policy-makers may have to look here, therefore, if they are to cope with the great demand [21].

A need to train law enforcement agents had become necessary because the sphere of influence of electronic systems was growing by the day. The era where law enforcement agents had only one area of specialization had gone past and such bodies must have local capacity to deal with cybercrime. A secured cyberspace was a complex and evolving challenge and requires close collaboration with key sectors of the economy that relied on cyberspace such as banks, federal, state and local governments, higher institutions and law enforcement agencies. Creation of a national cyberspace security response system to include first responders and emergency workers has been advocated [10].

As cybercrime matures, it is imperative that law enforcement develops and maintains strong working relationships with its private sector counterparts to cooperatively investigate crimes of mutual interest. Law enforcement officers, investigators, and prosecutors must be trained to use the Internet and to handle

computer-based evidence. A national repository should be established for computer crimes as well as a national clearinghouse for proactive Internet investigations into crimes such as child sexual exploitation, bookmaking and prostitution. Legislation must be enacted that ensures ISPs maintain transactional records, improves law enforcement's ability to trace the origin of communications, and allows law enforcement to serve ISPs with legal processes. Law enforcement must take the lead in developing Computer Crime prevention materials for public education. [22].

It has been advocated that implementing a comprehensive online risk management and compliance platform gives management the insights they want and the control they need to maintain a trusted Web channel. Ensuring security, privacy and accessibility for your online business is simply good business.

The implementation by all nations (developed and developing) of the following resolutions at the international Conference on "Cybercrime: A Global Challenge, A Global Response" held in Madrid, Spain, on 12 and 13 December 2005 would go a long way at curtailing the scourge of cybercrime worldwide;

- *Bearing in mind United Nations General Assembly Resolution 55/63 (2000);*
- *Having regard to the Convention on Cybercrime (2001) and its additional Protocol concerning the acts of a racist and xenophobic nature committed through computer systems (2003);*
- *Having regard to the Declaration of Warsaw adopted at the Third Summit of Heads of State and Government of the Council of Europe, held in Warsaw, on 16 and 17 May 2005;*
- *Bearing in mind the results of the 5th Conference of Ministers of Justice and Attorneys General of the Organisation of American States held in Washington D.C., from 28 to 30 April 2004, which recommended « that Member States evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001), and consider the possibility of acceding to that convention »;*
- *Bearing in mind the Bangkok Declaration « Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice » adopted at the 11th United Nations Congress on Crime Prevention and Criminal Justice held in Bangkok, from 18 to 25 April 2005;*
- *Bearing in mind the Resolution adopted at the 6th International INTERPOL Conference on Cyber Crime held in Cairo, from 13 to 15 April 2005, which recommended « that the Convention on Cyber Crime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it »;*
- *Having regard to the Declaration of Salamanca adopted at the XV Ibero-American Summit of Heads of State and Government held in Salamanca, on 14 and 15 October 2005;*
- *Stressing the importance of ensuring a proper balance between the need to fight cybercrime and the respect of fundamental human rights such as the freedom of expression, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and the 1969*

American Convention on Human Rights, as well as other international human rights treaties;

- *EXPRESS CONCERN about the rapidly growing dangers and serious social and economic consequences of cybercrime including terrorist activity on the Internet;*
- *NOTE that most cybercrime is international cybercrime;*
- *RECOGNISE the need for effective and compatible laws and tools to enable States to co-operate efficiently in the fight against this scourge;*
- *WELCOME the steps already taken by States, International Organisations and the private sector to co-operate in the fight against high-technology and computer-related crime;*
- *CALL UPON States, International Organisations and the private sector to strengthen their co-operation in order to raise awareness of the need for appropriate legislation, based on existing international standards, as well as for appropriate training to combat cybercrime;*
- *ACKNOWLEDGE the importance of the only international treaty in this field: the Convention on Cybercrime which is open to all States as well as the importance of strengthening the international legal framework;*
- *STRONGLY ENCOURAGE States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international cooperation;*
- *RECOGNISE the need of pursuing co-operation, providing technical assistance and organising similar events in other regions of the world;*
- *WELCOME the holding of the first meeting of the Cybercrime Convention Committee which will take place in Strasbourg on 20 and 21 March 2006 and encourage States to participate; [23].*

9. Conclusion

Cybercrime has been delicately defined as the illegal use of the internet technologies to obtain money, goods and services by fraudulent means through pseudonymity (assuming the identity of another person on-line), use of stolen credit card, and other electronic payment systems, etc. Information and Communications Technologies (ICTs)' revolution with the advent of the Internet has led to an increase in cybercrime as the abuse of these new technologies on record threaten economic and financial security and actually devastate the lives of affected individuals.

Most companies today have focused their security efforts on networks, servers and desktops, but web applications present the greatest risk and vulnerability. By their very nature, they are decentralized, difficult to manage and often collect sensitive data that places organizations at risk to hackers and other web attacks. By ensuring the security of your web applications across the enterprise, you can minimize your online risk and improve the effectiveness and efficiency of your online channel.

You're aware that information security and privacy are not just technical challenges — they require processes and management oversight. Now advanced

software solutions can be efficiently and cost-effectively deployed to reduce the risks and vulnerabilities that pervade an agency's online operations.

This paper has identified panacea for success including strategies for improving the odds of capturing and convicting cyber-criminals lurking in international cyberspace, how to build and deploy practical defense systems, 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. This includes an establishment of a college of information technology dedicated to equip the named sector with the skills; incorporation of computers and the laws of information technology course in university curriculum for both law and computer science undergraduates; and collaboration of Nigeria's Economic & Financial Crimes Commission (EFCC) with the Interpol, FBI/Internet Crime Complaint Center and the developing nations' law enforcement and judiciary sector, etc, to sanitize Nigeria of high-tech crimes in an implementable, enforceable and sustainable framework.

References

[1] **(NIC, 2002)** National Intelligence Council, Workshop on Information Technology in Africa *Conference Proceedings 2-3 October 2001 CR-2002-01, May 2002, available at http://www.dni.gov/nic/PDF_GIF_confreports/africa_it.pdf*

[2] KOO, Tae-eon; Simon LARDNER ; Ahmad RAMLI; Haibin BI; and others (2005): CYBERCRIME LEGISLATION AND ENFORCEMENT CAPACITY BUILDING PROJECT, 3ND CONFERENCE OF EXPERTS AND TRAINING SEMINAR, 22-24 June 2005, Seoul, Korea

[3] USAID (2006). Strategic Goal Chapter 5: International Crime and Drugs, Department of State and U.S. Agency for International Development FY 2007 Joint Performance Summary

[4] Robert **Bruce**, Scott **Dynes**, Hans **Brechbuhl**, Bill **Brown**, Eric **Goetz**, Pascal **Verhoest**, Eric **Luiijf**, and Sandra **Helmus** (2005) International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues, TNO Information and Communication Technology, Delft, Netherlands, June 30, 2005 available at cds-1.dartmouth.edu/docs/discussion_paper_final.pdf, accessed December 5, 2006.

[5] Nir **Kshetri** (2006), The Simple Economics of Cybercrimes University of North Carolina, IEEE Security & Privacy, January/February, 2006, 4(1), 33-39.

[6] 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** www.olis.oecd.org/.../43bb6130e5e86e5fc12569fa005d004c/911996b0a67a8e9cc12570dd003bd320/$FILE/JT00196254.DOC, accessed December 18, 2006

[7] www.playitcybersafe.com//cybercrime/index.cfm

[8] Bala **Ciroma (2006),** EFCC And National Security Imperatives, Zero Tolerance, The Magazine of the Economic & Financial Crimes Commission (EFCC), 1(1), July, 2006 p.9

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

[10] Jonah **Iboma (2006).** Cybercrime: Govt to empower law enforcement agencies, *The Punch*, Monday, November 27, 2006 p. 72

[11] http://www.ic3.gov/

[12] http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/6_cybercrime/T-CY/Default.asp#.

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

[14] **Sumainah**, Abu (2006). Day Internet Fraudstar Met His Waterloo, *ZeroTolerance* [The Magazine of Nigeria's Economic and Financial Crimes Commission), 1(1), p 40, July 2006 [15a & b] Nuhu **Ribadu**, and Jean-Christophe Le **Toquin** (2006). Spammers Beware: Microsoft and Nigeria Team up to Fight Cybercrime, July 19, 2006 http://www.efccnigeria.org/index.php?option=com_content&task=view&id=960&Itemid=2

[16] **Omole**, Rotimi (2006) Nigerian Tribune: 3 Internet fraudsters held for duping Swiss national, 12.10.2006 (www.tribune.com.ng/12102006/news/news9.html)

[17] **Ibrahim**, MKG (2006). EFCC's IT Strategy To Contain Cybercrime, *ZeroTolerance* [The Magazine of Nigeria's Economic and Financial Crimes Commission), 1(1), pp 38-39, July 2006

[18] **USdoj** (2006), Latest Press Releases, U.S. Department of Justice, 10th & Constitution Ave., NW, Criminal Division, (Computer Crime & Intellectual Property Section), John C. Keeney Building, Suite 600, Washington, DC 20530 http://www.cybercrime.gov/, accessed December 24, 2006

[19] Daniel **Thomas**, New crackdown on cyber crime. Computing, 11 May 2006, (www.itweek.co.uk/computing/news/2155797/crackdown-cyber-crime).

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

[21] Jim **Tanburn** and Alwyn Didar **Singh** (2001), ICTs and Enterprises in Developing Countries: Hype or Opportunity? http://www.ilo.org/dyn/empent/docs/F1089912836/WP17-2001.pdf;

[22] Interpol (2005) 6th International Conference on Cyber Crime, Convention on Cybercrime (ETS no. 185), www.interpol.int/Public/TechnologyCrime/default.asp and www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/ExplanatoryReport.pdf Cairo, Egypt, 13-15 April 2005

[23] *http://www.coe.int/t/e/legal_affairs/about_us/cooperation/CYB%20_2005_%20Conclusions%20E.pdf*