(IJCRSEE) International Journal of Cognitive Research in science, engineering and education
Vol. 1, No.1, 2013.

APPROACH TO CYBER SECURITY ISSUES IN NIGERIA: CHALLENGES AND SOLUTION

Dr. Ibikunle Frank, Department of Electrical & Information Engineering, Covenant University, Nigeria
E-mail: faibikunle2@yahoo.co.uk
Eweniyi Odunayo, Department of Electrical & Information Engineering, Covenant University, Nigeria
E-mail: odunayoeweniyi@yahoo.com

Abstract: Cyber-space refers to the boundless space known as the internet. Cyber-security is the body of rules put in place for the protection of the cyber space. Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. The Internet is one of the fastest-growing areas of technical infrastructure development. Over the past decades, the growth of the internet and its use afforded everyone this opportunity. Google, Wikipedia and Bing to mention a few, give detailed answers to millions of questions every day. Cyberspace is a world that contains just about anything one is searching for. With the advent of these advancements in information accessibility and the advantages and applications of the internet comes an exponentially growing disadvantage- Cyber Crime. Cyber security has risen to become a national concern as threats concerning it now need to be taken more seriously. This paper attempts to provide an overview of Cybercrime and Cyber-security. It defines the concept of cybercrime, identify reasons for cyber-crime and its eradication. It look at those involved and the reasons for their involvement. Methods of stepping up cyber security and the recommendations that would help in checking the increasing rate of cyber-crimes were highlighted. The paper also attempts to name some challenges of cybercrime and present practical and logical solutions to these threats.

Keywords: Cyber-space Cyber-security Cyber-crime, ICT, Internet

1. Introduction

From business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and a blossoming haven for cybercriminal miscreants to perpetrate their insidious acts.[13] This paper hopes to paint a developing scenario of the evolution of new type of war - the internet cybercrime - which will cause destruction of greater magnitude than the two past world wars- if not properly nipped in the bud. It has been established that Nigeria is an impressionable country. The advent of the internet to her was both welcome and full of disadvantages. The exceptional outbreak of cyber-crime in Nigeria in recent times was quite alarming, and the negative impact on the socio-economy of the country is highly disturbing.

Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users.

The first recorded cyber murder was committed in the United States seven years ago. According to the Indian Express, January 2002, an underworld don in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient.[10] Statistically, all over the world, there has been a form of cyber-crime committed every day since 2006.[15] Prior to the year 2001, the phenomenon of cyber-crime was not

globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet.[14] Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters.[18] Since the issue of cyber security is raising a number of questions in the minds of Nigerians, it is only fair that we answer these questions. This paper seeks to give an overview of cyber-crime and cyber-security, outline some challenges and proffer solutions.

2. Literature review

The issue of cyber-crime is one that has been discussed by many people with various perspectives on the issue, most coming at it from different sides than the others. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States.[7] According to a publication in [20] which states that "the adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security". The publication further stated that since threats could originate anywhere around the globe, the challenges are inherently international in scope thus requires international cooperation, investigative assistance, and common substantive and procedural provisions". In line with the above, Professor Augustine Odinma states that "cyber-crime is any illegal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a computer, a phones, etc. The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks (DOS), malware (malicious code). the illegal act may be facilitated by computer network or devices with target independent of the computer network or device".[5] Relating cyber-crime to the military in a paper depicting his vested interest in the country's military well-being, Major General Umo outlines that cybercrime, cyber terrorism, cyber warfare, cyber security are one and the same thing. This is because, stealing or forgery directed at an individual or an organization is synonymous to waging war on the target of the crime.[4]

Statistically, Nigeria ranked 43 in EMEA and ranked third among ten nations that commits cyber-crime in the world.[5] As a corrective measure, the then President of Nigeria, Olusegun Obasanjo set up National Cyber security Initiative (NCI) in 2003. The Nigerian cybercrime working group (NCWG) is to meet the objectives of NCI but their effects did not match up to the rate of growth of cybercrime. Professor Oliver Osuagwu, relating cyber-crime to the collapse of the educational sector, points out that cybercrime is causing near total collapse of the education community, particularly in Nigeria, with over 90% of criminals coming from this sector. Wrong value system has been identified as key factor encouraging cybercrime in Nigeria and the desire to get rich quick without working for it. Cyber-crime is complex and committed mostly from remote locations making it difficult to police. The absence of enabling law makes policing even more difficult.[9]

As earlier stated, the internet has a capacity for more good than bad. This is

better explained by Mrs. R. Moses-Oke in [14] when she said "The oxymoronic nature of the Internet is one of its unforeseen attributes; at its inception, no one, perhaps, could have clearly foreseen that, and how, the Internet would someday become a veritable platform for globalized criminal activities. As has been copiously remarked, the benefits of the Internet have so often been tainted by its versatility for virtual criminal activities that have vastly devastating physical and social impacts". Many will agree that concerns are increasing as Nigeria is increasing its digitalization not only in the area of commerce and communications, but gradually into the area of electronic banking. In the past year, electronic banking and the cashless initiative have been in focus a lot. Amaka Eze in her article [12] for THISDAY live writes, "As the country integrates electronic payment system into its financial institution; a step that is expected to accelerate the nation's e-commerce growth, the negative impact of cybercrime on businesses, and the absence of appropriate laws to guarantee the legality of online transactions, continue to create fear in the mind of users and potential online users". Even as we talk about the rise and dangers of cyber-crime and breach in cyber security, there is need to focus on a way to reduce or completely eradicate its incidence in Nigeria. To restore the full glory of cyber security, those involved have to spend time to learn how cybercrime ring operates and then devise strategies to fight the menace. We cannot fight today's crime with yesterday's technology. It will always be a losing battle if security professionals are way behind the cyber criminals in terms of technological knowledge. It's not just about computing skills, but IT Security expertise.

Also discussed previously are the costs incurred by the government due to the rise of cyber-crime. As for measuring costs, the Detica report in [3] considered four categories: costs in anticipation of cybercrime, such as antivirus software, insurance and compliance; costs as a consequence of cybercrime, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise; costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies; indirect costs such as reputational damage to firms, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy. Having seen cybercrime from different perspectives, we would now discuss fully on cyber-crime and cyber-security, practical instances and solution mechanisms in the following sections. Much has already been done by the law enforcement agents, but cyber-crime is still perpetrated underground.

3. Overview of cyber-crime and cyber-security

As technology has developed so have also the definitions of cyberspace, cyber security and cybercrimes. It has been argued that since computer crime may involve all categories of crime, a definition must emphasize the particularity, the knowledge or the use of computer technology. Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber

environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[20] Cyber-security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risks. Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. Sophisticated cyber criminals and nation-states, among others, present risks to our economy and national security. Nigeria's economic vitality and national security depend on a vast array of interdependent and critical networks, systems, services, and resources known as cyberspace. Cyber-space has transformed the ways we communicate, travel, power our homes, run our economy, and obtains government services. Cyber-security is the body of technology, processes and practices designed to protect networks, computers, programs and data from attacks, damage, or authorized access. In the computing or cyber context, the word security simply implies Cyber-security.[19] Ensuring cyber-security requires coordinated efforts from both the citizens of the country and the country's information system. The threat posed by breaches in our cyber-security is advancing faster than we can keep up with it. It is not possible to concentrate efforts on only one aspect of the breach as it means negligence and allowance of growth for other aspects of the breach. This leads us to conclude that we have to attack cyber security breaches as a whole. What then are these breaches?

Cyber-crime refers to criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users.[6] Perhaps the most complete definition of Cyber-crime is as given [7] "A criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud".

3.1. Goals of Cyber Security

The following are the objectives of Cyber-security.

- To help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.
- To help individuals and institutions develop and nurture a culture of cyber security.
- To work collaboratively with public, private and international entities to secure cyberspace.
- To help understand the current trends in IT/cybercrime, and develop effective solutions.
- Availability.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality.

4. E-crimes those are peculiar to Nigeria

There is no doubt that e-crime is an image trauma for Nigeria. Cyber-crime is a source of concern and embarrassment for

the nation. The Internet creates unlimited opportunities for commercial, social, and educational activities. But as we can see with cyber-crime the Internet also introduces its own peculiar risks. The instances reported here ranges from fake lotteries to the biggest internet scams. Elekwe, a chubby-faced 28-year-old man made a fortune through the scam after two years of joblessness despite having diploma in computer science. He was lured to Lagos from Umuahia by the chief of a fraud gang in a business center. He has three sleek cars and two houses from his exploits. In July 2001, four Nigerians suspected to be operating a "419" scam on the internet to dupe unsuspecting foreign investors in Ghana were arrested by security agencies. Their activities are believed to have led to the loss of several millions of foreign currencies by prospective investors. Two young men were recently arrested after making an online purchase of two laptops advertised by a woman on her website under false claims. They were arrested at the point of delivery by government officials. Mike Amadi was sentenced to 16 years imprisonment for setting up a website that offered juicy but phony procurement contracts. The man impersonated the EFCC Chairman, but he was caught by an undercover agent posing as an Italian businessman. The biggest international scam of all was committed by Amaka Anajemba who was sentenced to 2½ years in prison. She was equally ordered to return $25.5 million of the $242 million she helped to steal from a Brazilian bank.

On recent internet scam case was reported on the Sunday PUNCH newspaper of July 16, 2006 involving a 24-year-old Yekini Labaika of Osun State origin in Nigeria and a 42-years-old nurse of American origin, by name Thumbelina Hinshaw, in search of a Muslim lover to marry. The young man deceived the victim by claiming to be an American Muslim by the name, Phillip Williams, working with an oil company in Nigeria and he promised to marry her. He devised dubious means to swindle $16,200 and lots of valuable materials from the victim. The scammer later was sentenced to a total of 19½ years having been found guilty of eight-counts against him. Incidences like these are on the increase. Several young men unabated are still carrying out these illegal acts successfully, ripping off credulous individuals and organizations.[8] Recently, a report indicated that Nigeria is losing about $80 million yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research and forecasting firm, based in South Africa, on behalf of Business Software Alliance of South Africa. The American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up to 90% in 2001. The Centre also ranked Nigerian cyber-crime impact per capita as being exceptionally high.[17]

Those involved are between 18-25 years mostly resident in the urban centers. The internet has help in modernizing fraudulent practices among the youths. Online fraud is seen as the popularly accepted means of economic sustenance by the youths involved. The corruption of the political leadership has enhanced the growth of internet crime subculture. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud.[1]

5. Categories of cyber crime

- Hacking: Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what u do on your computer and can also import files on your

computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

- Cyber-Theft: Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and shareholders. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring experienced cyber-criminal large cash resulting from very little effort
- Viruses and worms is a very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in soft wares or the operating system. Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples. Experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained.[16]
- Spamming– involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.
- Financial Fraud- These are commonly called “Phishing’ scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim’s bank.
- Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.
- Cyber harassment- is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.
- Cyber laundering- is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.
- Website Cloning: One recent trend in cyber-crime is the emergence of fake ‘copy-cat’ web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster’s personal database. The fraudster is then able to make use of this

information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

6. Emerging cyber tricks in Nigeria

- **Beneficiary of a Will Scam**: The criminal sends e-mail to claim that the victim is the named beneficiary in the will of an estranged relative and stands to inherit an estate worth millions.
- **Online Charity**: Another aspect of e-crime common in Nigeria is where fraudulent people host websites of charity organizations soliciting monetary donations and materials to these organizations that do not exist. Unfortunately, many unsuspecting people have been exploited through this means.
- **Next of Kin Scam**: Collection of money from various bank and transfer fees by tempting the victim to claim an inheritance of millions of dollars in a Nigerian bank belonging to a lost relative.
- **The "Winning Ticket in Lottery you Never Entered" Scam:** These scams lately include the State Department's green card lottery.
- **Bogus Cashier's Check**: The victim advertises an item for sale on the Internet, and is contacted
- **Computer/Internet Service Time Theft**: Whiz kids in Nigeria have developed means of connecting Cyber Cafes to Network of some ISPs in a way that will not be detected by the ISPs and thereby allow the Cafes to operate at no cost.
- **Lottery scam:** allowing users believe they are beneficiaries of an online lottery that is in fact a scam.[18]

7. Challenges of cybercrime

- Tunji Ogunleye, an ICT security consultant and a member of Nigeria Cyber Crime Working Group (NCWG) disclosed that the rate of e-crime in Nigeria has outgrown the rate of Internet usage in the country. He said Nigeria is the 56th out of 60 countries embracing Internet usage but third in the fraud attempt category. We are tempted to ask why there is such an upsurge of e-crime in Nigeria and what are the factors that made Nigerians so vulnerable to e-crime?
- **Domestic and international law enforcement**: A hostile party using an Internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.
- **Unemployment**: The spate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. The federal government has proposed a mass sack of government workers. Companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on ad-hoc decisions.
- **Poverty Rate**: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries.
- **Corruption**: Nigeria was ranked third among the most corrupt countries in the world. Until 1999, corruption was seen as a way of life in Nigeria.
- **Lack of Standards and National Central Control**: Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business. Foreign Direct Investment (FDI) and foreign outsourcing

are encouraging computer misuse and abuse.

- **Lack of Infrastructure**: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.
- **Lack of National Functional Databases**: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.
- **Proliferation of Cybercafés**: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.
- **Porous Nature of the Internet**: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

7.1. Complexities of Cybercrime

- The speed and power of modern information technology complicates the detection and investigation of computer crimes. For example, communications networks now span the globe and a small personal computer can easily connect to sites that are located in different hemispheres or continents. This raises very significant problems in terms of jurisdiction, availability of evidence, co-ordination of the investigation and the legal framework(s) that can be applied to criminal acts that occur in this context.
- New technologies create new concepts that have no legal equivalence or standing. Nevertheless, a virus utilizes the resources of the infected system without the owner's permission. Hence, even a benign virus may be variously interpreted as a system penetration, a piece of electronic graffiti or simply a nuisance prank. The major point however, is that the legal system and therefore the definition of computer crime itself is reactive and unable to encompass behaviors or acts that involve new computational concepts.
- Information has several unique and abstract properties - for example its capacity to still be in the owner's possession after it has been copied or stolen. The last decade has seen the legal system struggle with the implications of this in a computer based context. Clearly, conventional notions of copyright, patent rights and theft have been strained when applied to software and computer based information, basically because existing concepts of theft and break-in for example, relate to common notions of permanent deprivation or removal (theft) or physical damage (break-ins).
- A related property of digital information is the ease and extent to which it can be transformed and translated. That is, a piece of information (i.e., a program) can be represented in a huge variety of informational forms. It can be represented as program text (source code), executable code (binaries), or it can be transformed in a large number of ways - mathematically, by encryption, or by conversion to say a holographic image or a piece of music. As long as the method(s) of transformation are known, the music, image, or encrypted text can be translated back to its original form. Therefore, the informational form in which information exists may eventually have no legal status. Instead, some measure of its value or functionality as information itself may eventually determine its legal and commercial position.
- This malleability of information has implications in terms of system break-ins where information may not be destroyed (as in corrupted or erased) but is encrypted or made temporarily inaccessible. Such actions can hardly be classified as theft or even malicious damage.[11]

7.2. Effects of Cyber Crime

- Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.
- Loss of reputation: most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.
- Reduced productivity: this is due to awareness and more concentration being focused on preventing cybercrime and not productivity.
- Vulnerability of their Information and Communication Technology (ICT) systems and networks.

8. Solutions to cybercrime

- Education: Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.
- Establishment of Programs and IT Forums for Nigerian Youths: Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.
- Address Verification System: Address Verification System (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like United States) matches the address where the cardholder's billing statements are mailed.
- Interactive Voice Response (IVR) Terminals: This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.
- IP Address tracking: Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.
- Use of Video Surveillance Systems: The problem with this method is that attention has to be paid to human rights issues and legal privileges.
- Antivirus and Anti spyware Software: Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.
- Firewalls: A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.
- Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient.[20] A

number of cryptographic methods have been developed and some of them are still not cracked.

- Cyber Ethics and Cyber legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.[7]

9. Conclusion and recommendations

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. A combination of sound technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents will be a good start in the war against cyber criminals. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications. There is need to create a security-aware culture involving the public, the ISPs, cybercafés, government, security agencies and internet users. Also in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. Mishandling of enforcement can backfire.

References

1. Adebusuyi, A. (2008): *The Internet and Emergence of Yahooboys sub-Culture in Nigeria*, International Journal Of Cyber-Criminology, 0794-2891, Vol.2(2) 368-381, July-December
2. Amaka Eze, "Thisday Live"
3. Anderson, Ross, et al. (2012): *Measuring the cost of cybercrime*, 11th Workshop on the Economics of Information Security (June 2012), Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf
4. Augustine C. Odinma, MIEEE (2010): *Cybercrime & Cert: Issues & Probable Policies for Nigeria*, DBI Presentation, Nov 1-2.
5. Background Check International, *"Information Technology/Cyber Security Solutions"*
6. International Telecommunication Union, Retrieved from http://www.itu.int/en/Pages/default.aspx
7. Laura, A. (1995): *Cyber Crime and National Security: The Role of the Penal and Procedural Law"*,Research Fellow, Nigerian Institute of Advanced Legal Studies., Retrieved from http://nials-nigeria.org/pub/lauraani.pdf
8. Longe, O. B, Chiemeke, S. (2008): *Cyber Crime and Criminality In Nigeria – What Roles Are Internet Access Points In Playing?, European Journal Of Social Sciences – Volume 6, Number 4*
9. Major General G. G UMO (2010): *Cyber Threats: Implications For Nigeria's National Interest*, Retrieved from https://docs.google.com/file/d/0B9sby6N_v5O3M2FlNWIzZjgtMDRiOS00NjI1LThmMjItNmI0Nzg5NGVlNTM2/edit?num=50&sort=name&layout=list&pli=1
10. Mohsin, A. (2006): *Cyber Crimes And Solutions*, Retrieved from http://ezinearticles.com/?Cyber-Crimes-And-Solutions&id=204167
11. Okonigene, R. E., Adekanle, B. (2009): *Cybercrime In Nigeria*, Business Intelligence Journal, Retrieved from http://www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7.pdf
12. Oliver, E. O. (2010): *Being Lecture Delivered at DBI/George Mason University Conferenceon Cyber Security holding*, Department

of Information Management Technology Federal University of Technology, Owerri, 1-2 Nov.

13. Olumide, O. O., Victor, F. B. (2010): *E-Crime in Nigeria: Trends, Tricks, and Treatment*. The Pacific Journal of Science and Technology, Volume 11. Number 1. May 2010 (Spring)
14. Roseline, O. Moses-Òkè (2012): *Cyber Capacity Without Cyber Security: A Case Study Of Nigeria's National Policy For Information Technology (NPFIT)***,** The Journal Of Philosophy, Science & Law Volume 12, May 30, 2012, Retrieved from www.Miami.Edu/Ethics/Jpsl
15. Schaeffer, B. S., et al. (2009): *Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others*
16. Strassmann, P. A. (2009): *Cyber Security for the Department Of Defense*, Retrieved July 10, 2011 From http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf
17. *The Economic Times*. September 11, 2004. 1.
18. Thompson, D. (1989): *Police Powers-Where's the Evidence*, *Proceedings of the The Australian Computer Abuse Inaugural Conference*.
19. www.bbc.co.uk
20. www.whatis.com