International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-9, Issue-4)

Research Article | **April 2019**

Cybercrime: Responding Sensibly in the Age of Uncertainty

Akpan, Abasiama G.
Department of Computer Science, Evangel University, Akaeze – Nigeria
gakpan76@gmail.com

Eneji, Samuel E.
Department of Computer Science, Federal College of Education, Obudu – Nigeria
borngreat969@gmail.com

Abstract: ***Cybercrime is now threatening the very existence of Information Technology critical infrastructure, the greatest human innovation after the industrial revolution. 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. This paper has proposed several recommendations including the fact that the National Orientation Agency should shift focus to national re-orientation of the psyche of the whole population and particularly the youths in post-primary and tertiary institutions and to parents, towards raising crop of children with strong religious training, belief and trust in God as well as the infusion of religious training in the curriculum of our educational system at all levels. Cyber-security awareness training should now constitute part of the school curriculum. Government-Private sector partnership should be formed to develop appropriate strategies towards cyber crime monitoring, control and prevention. This is the responsibility of all citizens - government, private sector and individuals. The paper contends that if action is not taken urgently, Nigeria will head towards self-destruct and the African continent may turn out to become a desolate colony!***

Key Words: Cyberspace, Cybercrime, Biometric, Computer crime, Cyber security.

I. BACKGROUND TO THE STUDY

"Cybercrime", for the purpose of this paper, can be described as computer viruses/malware, online credit card fraud, online hacking, online harassment, online identity theft, online scams (i.e., fraudulent lotteries/employment opportunities), online sexual predation and online phishing. Thus, Freeware, software, hardware, social networking sites and absolutely everything that involves an internet cable, a PC as well as a mobile phone could be a potential agent for fraud, violence, crime and severe losses. Cybercrime has to do with criminality committed in the internet with the aid of computers or criminal activity conducted via the Internet.

Cybersecurity encompasses industry and government defense strategies adopted to curb cyber-criminality in the super highway. Cybercrime has dwarfed the expectations of e-commerce as a potential tool to improve Africa's national GDP, job creation and elimination of mass poverty. E-commerce, which is totally dependent on viable internet connectivity, has been violently attacked to the extent that e-commerce has virtually come to a halt because of the activities of cybercriminals. The activities of these evil agents have been described as the worst threat to the most formidable human innovation after the Industrial Revolution. It is indeed a colossal economic catastrophe for the developing nationals of Africa. This singular act by these agents of the devil has painted Nigeria black in the eyes of the international community to the extent that electronic transactions from Nigeria are no longer respected by merchants from other parts of the world.

II. LITERATURE REVIEW

2.0 The Nature of Crime in the Cyberspace

The primary types of cybercrimes are data, network, access, and other crimes [31, 32]. Cybercrimes under the title of data crimes include data interception, data modification, and data theft. Data interception is the interception of data in transmission [33]. Data modification is the alteration, destruction, or erasure of data [34]. Data theft is the taking or copying of data, regardless of whether it is protected by other laws such as US copyright and privacy laws, Health Insurance Portability and Accountability Act (HIPAA), and the Gramm Leach-Bliley Act (GLBA) (Electronic Privacy Information Center, 2004 [35,36].

Cybercrimes include access crimes such as unauthorized access and virus dissemination. Unauthorized access is the hacking or destruction of a network or system [42]

2.1 Top 10 Nations Perpetrating and Complaining Of Cybercrime

Below are two maps showing countries perpetrating cybercrime and those complaining of the menace as provided by IC3 2006 Internet Crime Report. January 1, 2006 – December 31, 2006 by the National White Collar Crime Center and the Federal Bureau of Investigation, 2007. A cursory look at the two maps shows that the USA ranked no. 1 for both perpetration and complaint scoring 60.9% for perpetration and 90.7% for complaint. This is an interesting scenario. This is not surprising though because the US is the heaviest user of IT and the cyberspace.

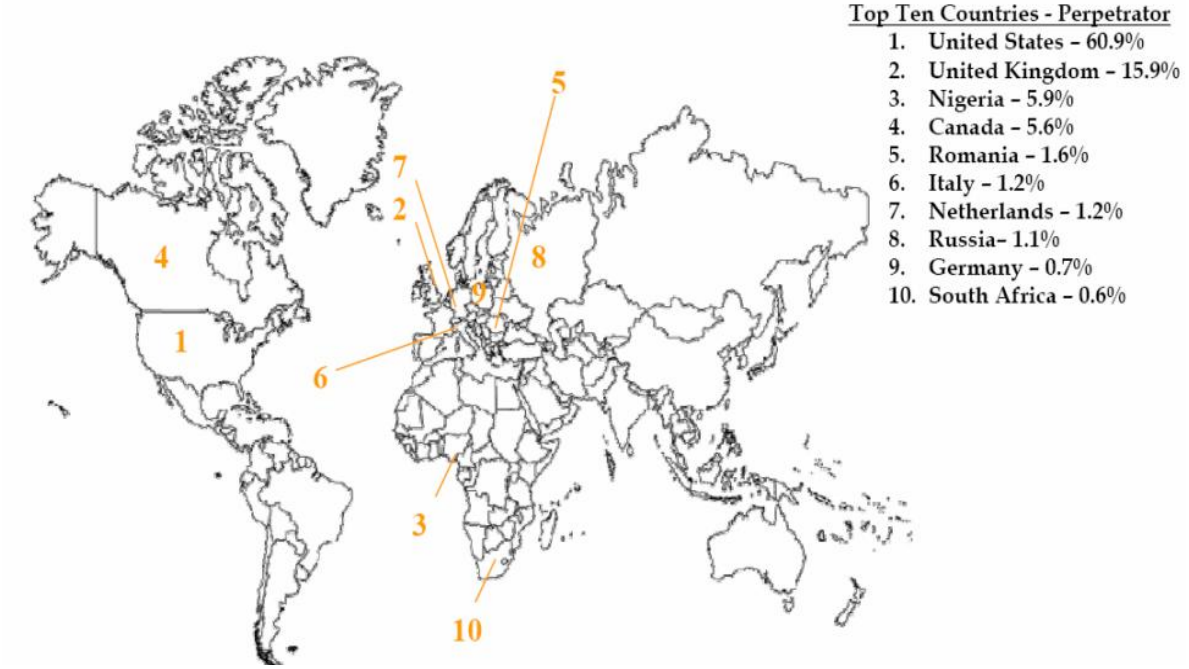

Figure 1: Map of Top 10 Countries by Count Perpetrators (Number is Rank) Note. Adapted from The IC3 2006 Internet Crime Report. January 1, 2006 – December 31, 2006 by the National White Collar Crime Center and the Federal Bureau of Investigation, 2007. [30]

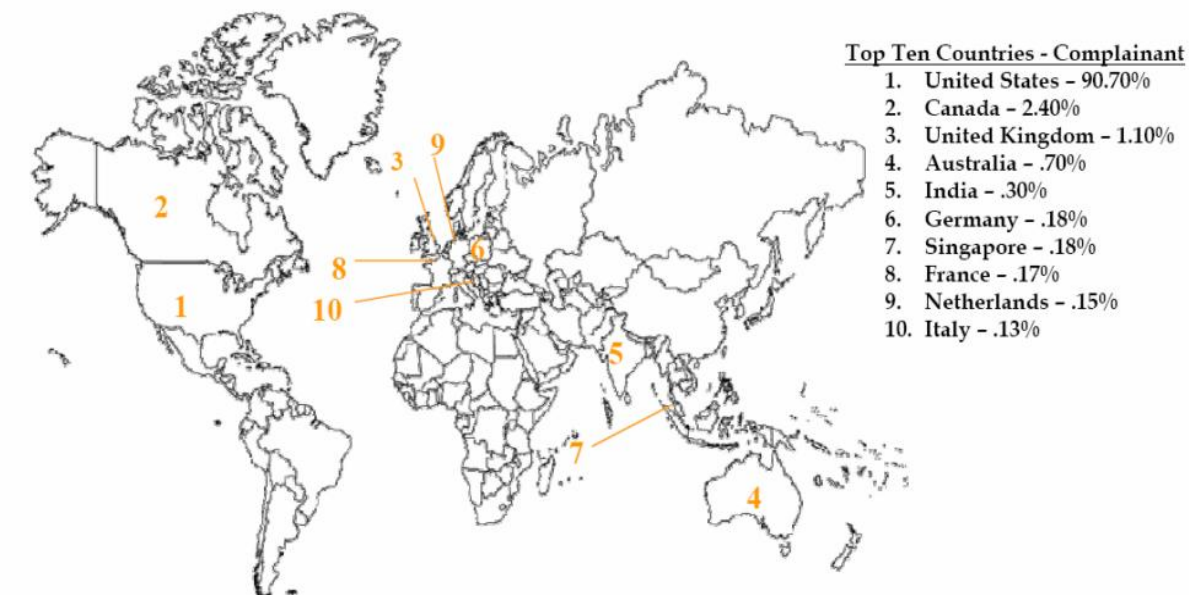

Figure 2. Map: Top 10 Countries by Count: Individual Complainants (Number is Rank) Note. Adapted from The IC3 2006 Internet Crime Report. January 1, 2006 – December [30]

2.2 Corporate Security Concerns

Denis [30] had reported in her work on Cybercrime's Impact on the Work Place that the top three computer security concerns, as reported by respondents, were:

(a) Embezzlement 30% (92), (b) intrusion or breach of computer systems 22% (67), and (c) computer viruses and denial of service attacks 11% (33). These top three computer security concerns reflect the thinking of 63% of the organizations reporting. Figure 2 depicts in ranking order all the variables identified.

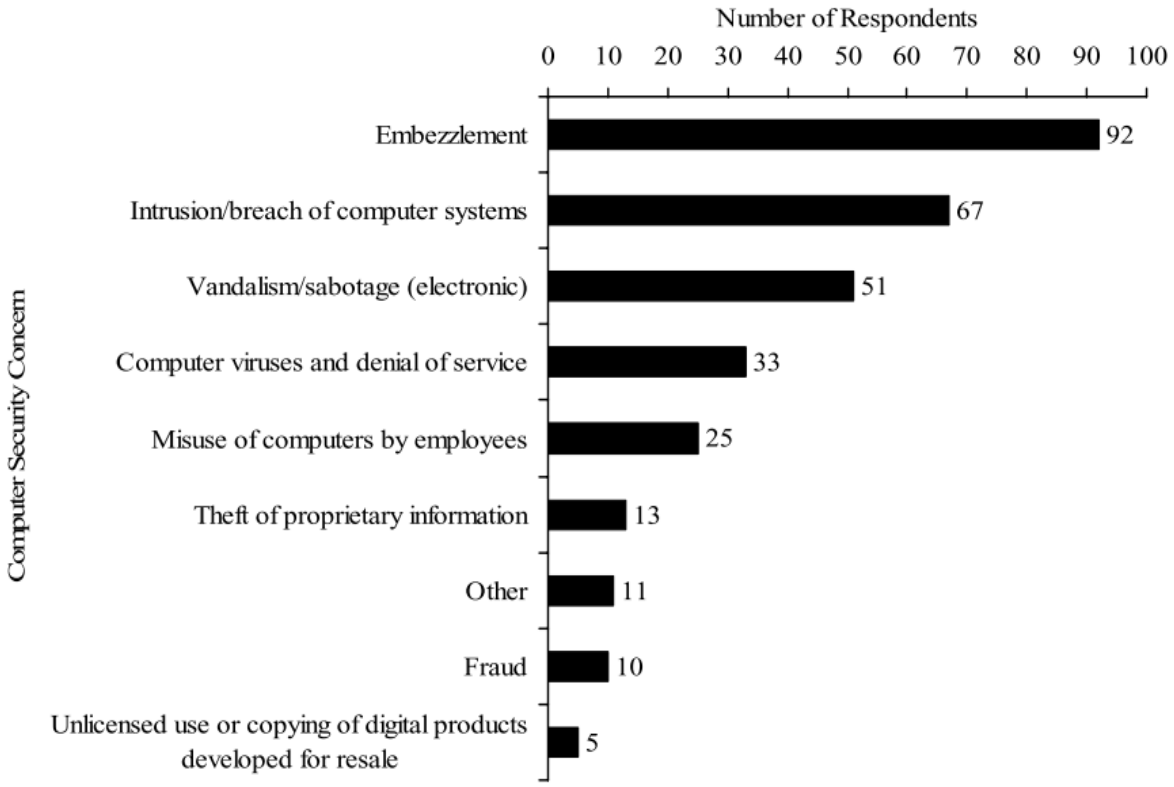

Figure 3. Ranking of computer security concerns by organizations.

2.3 Summary of Cybercrime Classification

The above descriptive discussion on the types of cybercrime can be summarized thus:

- **Hacking**: This is a term used to describe illegal intrusion into a computer system without the permission of the computer owner or user for purposes of stealing valuable information of market value.
- **Denial of Service Attack**: A criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.
- **Virus Dissemination**: This involves sending malicious software that attaches itself to other software. Good examples of these include: virus, worms, Trojan horse, Time bomb, Logic Bomb, Rabbit and Bacterium etc.
- **Software Piracy:** This involves the theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. This can be done in many ways such as via End user copying, Hard disk loading, counterfeiting, illegal downloads from the internet.
- **Pornography:** Pornographic tactics is used by many advertisers to encourage customer's access their website. Publishing, transmission of any material in electronic form which is lascivious or appeals to the prurient interest (nude people having live sex) is an offence is a serious crime in American Law (Section 67 of I.T. Act 2000). This has been included in the Information Technology Bill and the Cybercrime Act undergoing final reading in the Nigeria's National Assembly. It is a very powerful predator as it is used as a tool to lure victims.
- **IRC Crime**: IRC means Internet Relay Chat. IRC servers have chat rooms in which people from anywhere in the world can come together and chat with each other. Criminals use it for meeting conspirators. Hackers use it for discussing their strategies and sharing information on techniques. Pedophiles use chat rooms to lure young children. Cyber Stalking is used to harass a woman via her telephone number which may be given to others as if she wants to befriend men.
- **Credit Card Fraud:** If your electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating as the credit card owner. These criminals can use Credit card skimmer or writer to make fake credit cards with your information and use it to withdraw your money from your accounts.
- **Net Extortion**: This involves copying the company's confidential data in order to extort huge sum of money from the firm.
- **Phishing:** Deployed to pull out confidential information from the bank or financial institutions account holders by deceptive means.

Table 1: Countries with phishing sites (Source:eBay)

Countries	Number of Phishing Sites
Korea	87
China	75
India	25
Thailand	25
Japan	9
Chinese Taipei	18
Australia	4
Hong Kong	5
Malaysia	3
Singapore	2

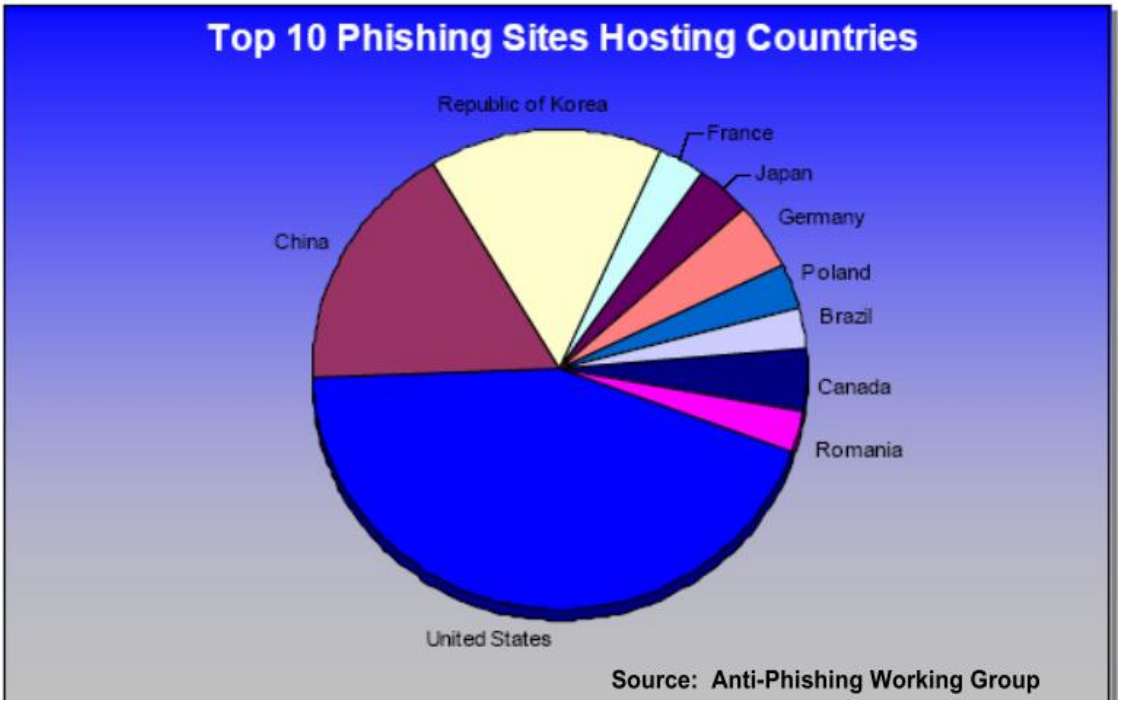

Figure 4: Ten Top Phishing Sites Hosting Countries

- **Spoofing:** This involves getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network.
- **Cyber Stalking:** In this technique, the criminal follows the victim by sending emails, entering the chat room frequently in order to catch his victim.
- **Cyber Defamation:** This involves the criminal sending emails containing defamatory statements to all concerned of the victim or posts the defamatory matters on a website. This is usually the style deployed by disgruntled employees against their boss, ex-boy and girl friends against each order or divorced wife against their ex-husbands.
- **Threatening:** Criminals may send threatening email or contact you in a chat room. This is the tactics adopted by disgruntled enemies against their boss, friend or official.
- **Salami Attack:** In this technique, the criminal makes insignificant changes in a manner that would make his action unnoticeable. For example small amount like N0.20 can be deducted from every N100 of your salary per month from the account of all the customer of a bank and deposited in his private account. Since the deductions

are very small, it is unlikely to be noticed by any bank Custer and accordingly reported. If he does for a long time unnoticed, he will make millions without running into the hands of the law.

- **Sale of Narcotics:** Web sites abound which offer sale and shipment of contraband drugs. They use Stenography for hiding the messages.
- **Nigeria's own 419:** This is a scam which starts with a bulk mailing or bulk faxing of a bunch of identical letters to businessmen, professionals and other persons who tend to be wealthy. The greedy ones will fall prey to such dubious business proposal and they will be heavily duped.
- ***seller frauds* is another distinct type of cyber crime** such as account take over via phishing, fake Escrow sites, non-performance transactions (fake listing), fraudulent misrepresentation**.**

2.4 Demography and characteristics of Cybercriminals

According to recent study by ChiChao Lai et.al [29] the demographic characteristics of cybercriminals is revealing as well as disturbing and calls for concerted effort by all to avoid an impending catastrophe. The report findings show that **81.1%** were **male**; **45.5%** had some senior high school; **63.1%** acted independently; ***23.7%** were* **currently enrolled students;** and **29.1%** were in the **18-23 age bracket**, which was the majority group. For those enrolled student cybercrime suspects, the findings show ***that the percentage of junior high school and senior high school student suspects constituted 69.0% (2002), 76.1% (2003) and 62.7% (2004)*** of cybercrime suspects in their respective years. The high rate shows that the number of currently enrolled students suspected of involvement in cybercrime is cause for concern**.** The following group of people are easily fall prey or perpetrate cyber-criminality:

- ***Disgruntled employees***
- ***Teenagers***
- ***Political Hacktivist***
- ***Professional Hackers***
- ***Business Rival***
- ***Ex-boy or Girl friend***
- ***Divorced Husband or Wife***
- ***Political enemies***

The victims are **gullible**, **desperados** and **greedy people, unskilled** and **inexperienced** and perhaps **unlucky people** too can fall victim**.**

2.5 Security Measures in Place: Industry Security Initiatives For The Cyberspace:

- *Firewalls, Antivirus, Anti-Malware, Pass-Wording, Encryption, Biometric Authentication Systems, Intrusion Detection and prevention Systems, etc.*

III. METHODOLOGY

3.1 Some Tested Palliative solutions in place

If correctly installed, the following technologies can help to block attacks: (These will be explained further in the following pages).

- **Firewalls** are hardware or software devices that block certain network traffic according to their security policy.
- **Software solutions** exist to identify and remove malware and to help manage spam email. Many must be paid for but free versions are also available.
- **Authentication** involves determining that a particular user is authorized to use a particular computer. This can include simple mechanisms such as passwords, to more complex methods using biometric technology.
- **Hardware cryptography** uses computer chips with cryptographic capabilities intended to protect against arrange of security threats.
- **Patches** are programs designed by software manufacturers to fix software security flaws. Patching is often installed automatically. This reduces end-user participation and increases ease of use

3.1.1 Biometric Authentication Systems (BAS)

According to Osuagwu [4] BAS refers to a brand new technology to reliably indicate whether people are actually who they say they are using traits unique to them. These traits include fingerprint patterns, the arrangement of tissue in the eye's iris, and the timbre of a person's voice.

Table 2 Factors Used To Authenticate An Individual

Source: FFIEC Guidance for Authentication in an Internet Banking Environment

Factors Used To Authenticate An Individual	
Something a person knows	Commonly a password or PIN. If the user types in the correct password or pin, access is granted.
Something a person has	Most commonly a physical device, referred to as a token. Tokens include self-contained devices that must be physically connected to a computer, or devices that have a small screen where an OTP is displayed, which the user must enter into an interface to be authenticated by the backend server.
Something a person is	Most commonly a physical character, such as a fingerprint, voice pattern, hand geometry, or pattern of veins in the user's eye. This type of authentication is referred to as biometrics and often requires the installation of specific hardware on the system to be accessed.

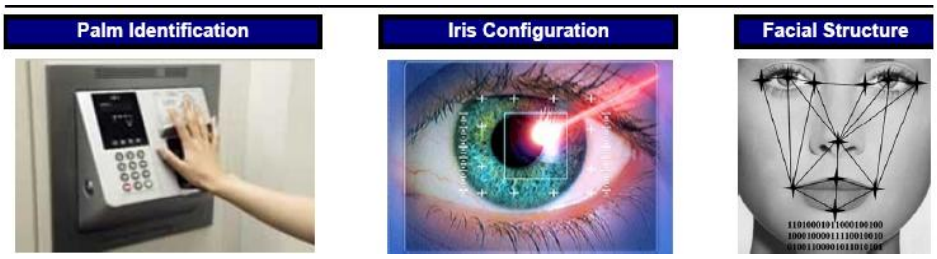

Figure 5: Samples of Biometric Authentication Technologies

Businesses, schools, and apartment buildings are using vascular recognition for physical access control. Large organizations are also beginning to deploy the technology to manage access to their information technology infrastructure. Vein pattern recognition has been adopted to screen passengers at South Korea's International Airport and to control access to the tarmac at several Canadian airports. Vascular recognition already has won wide acceptance in banking. More than a dozen Japanese banks and credit unions have made hundreds of ATMs featuring vascular sensors available for everyday use. In the vascular recognition systems developed by Fujitsu and TechSphere after inserting a banking card in a cash machine, the user is prompted to hold a hand near an infrared light source. The light source is paired with a charge-coupled device similar to the one used in standard digital photography.

Variants of BAS

a. **Finger Prints**: This technique of biometric authentication have been used to secure commercial transactions since the days of ancient Babylon, where fingerprints have been found among the ruins on clay scale attached to business documents. Each fingerprint contains global features, which can be seen with the naked eye, and local features, also called minutia points, the tiny unique characteristics of fingerprint ridges. Fingerprint scanners can be attached to USB ports as an external peripheral or they can be embedded within device.
b. **Iris Scans**: This technique analyze vein pattern and has the potential to be more accurate than fingerprints because the iris has about 260 degrees of freedom with regard to its vein patterns. Using an iris scanner requires aligning the eye with a coloured LED inside the camera, then moving the person's head forward or back until the LED changes colour, signaling that the distance is correct for proper imaging. The system then makes the scan, analyzes the image, and stores the template.
c. **Biometric Sensors**: This is the new proposal for enhancement of the existing BAS systems posited by Jain and Pankanti [16,17]. This new techniques uses fingerprint sensors and a combination of other BAS techniques could be incorporated. It is going to be economical, protect privacy, and guarantee the validity of all kinds of credit card transactions, including ones that take place at a store, over the telephone, or with an Internet-based retailer. By preventing identity thieves from entering the transaction look, credit card companies could quickly recoup their infrastructure investments and save businesses, consumers, and themselves billions of dollars annually.
d. **Smart Cards:** A smart card is another example of an authentication method. The size of a credit card, a smart card contains a microprocessor that enables it to store and process data. To be used, a smart card must be inserted into a compatible reader attached to either a computer or some type of electronic reading device. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her pass-code (second

factor) to complete the authentication process. Smart cards are difficult to duplicate and have demonstrated to be tamper resistant, creating a relatively secure vehicle for storing sensitive data and credentials.

Figure.6: Examples of Smart Cards

Source: Versatile Card Technology, Inc

Figure 7: PIN PADS

3.1.2 Intrusion detection system in the market place

Intrusion detection (ID) is a type of security management system for computers and networks. An **intrusion detection system** (IDS) is a device or software application that monitors network and/or **system** activities for malicious activities or policy violations and produces reports to a Management Station. It s used to determine if a computer network or server has experienced an unauthorized intrusion. Intrusions are the activities that violate the security policy of system. Intrusion Detection is the process used to identify intrusions IDS inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. There are several ways to categorize an IDS:

- **misuse detection** vs. **anomaly detection**: in misuse detection, the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network??s traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.
- **network-based** vs. **host-based systems**: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall??s simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.
- **passive system** vs. **reactive system**: in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

From the above taxonomy IDS can summarily be classified thus:

- Host-based IDSs
  - Get audit data from host audit trails.
  - Detect attacks against a single host

- Distributed IDSs
  - Gather audit data from multiple host and possibly the network that connects the hosts
  - Detect attacks involving multiple hosts
- Network-Based IDSs
  - Use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services
  - Detect attacks from network.

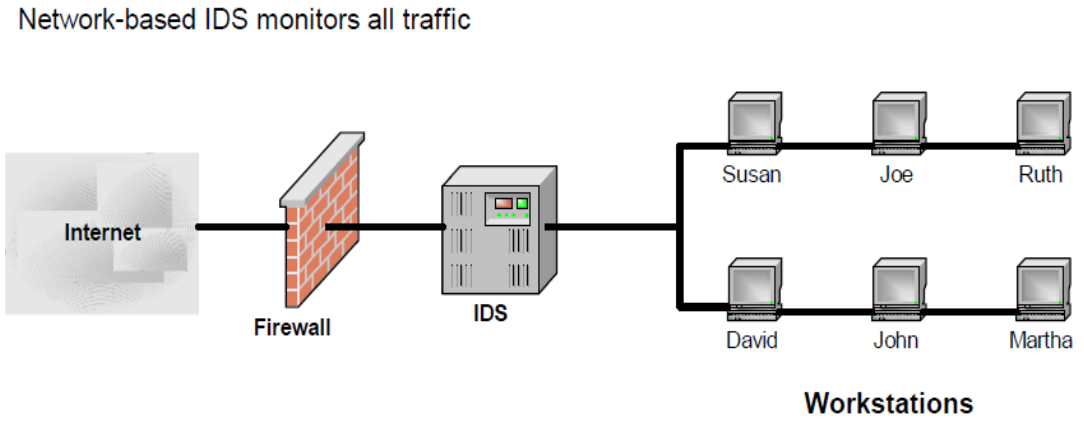

Figure.8: Example of Network-based IDS monitoring [27]

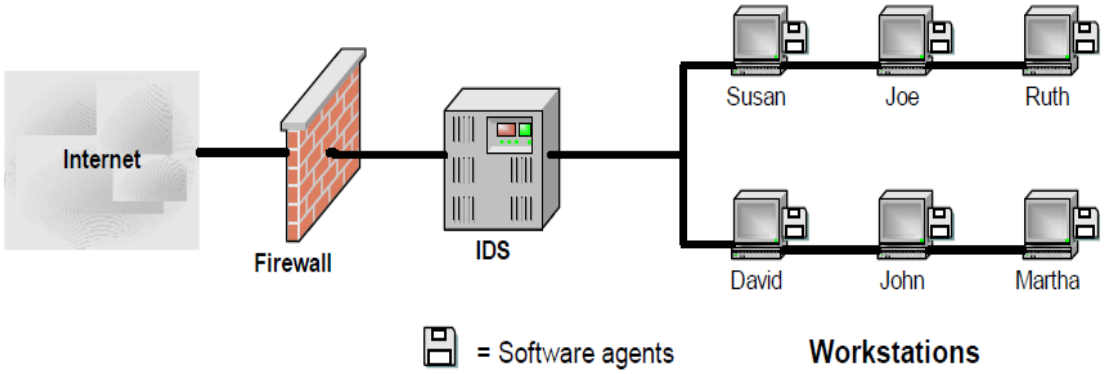

Figure 9: Software Agent Requirement in IDS monitoring [27]

- Misuse detection
  - Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities.
- Anomaly detection
  - Detect any action that significantly deviates from the normal behavior

3.1.3 Intrusion Detection Techniques

1. Define and extract the features of behavior in system
2. Define and extract the Rules of Intrusion
3. Apply the rules to detect the intrusion

3.1.4 Intrusion Prevention Systems

An Intrusion Prevention System is a module added to a base Intrusion Detection System. This module provides the ability to perform specific tasks automatically. An IT administrator can define the actions to be taken by the IPS when the attack severity reaches a pre-determined threshold. This allows an IT administrator to specify that any attack event at the denial of service (DoS) level or greater will result in the source IP address being filtered. The filter duration can be set from 15 minutes to permanently.

The advantages to Intrusion Prevention Systems are numerous:

- An attacker's ability to attack the target network can be automatically blocked any time 24x7.
- The filter duration can be specified so the attacker's IP address is not permanently blocked.
- Real-time email notification can be sent to the IT administrator.
- The attacker's Upstream Network Provider can be notified immediately when an attack occurs.

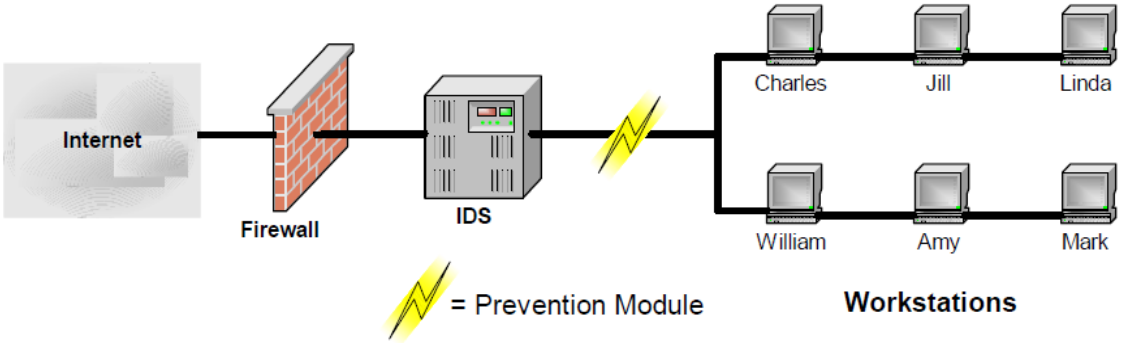

Figure 10: Example of Intrusion Prevention System. IPS disconnects attackers automatically [27]

Network Detection Zones

Intrusion Detection/Prevention Systems are placed in different types of network environments. For simplicity sake, we have identified three types of network detection zones as shown below. Each network detection zone has unique characteristics and the IDS must be able to adapt to each zone.

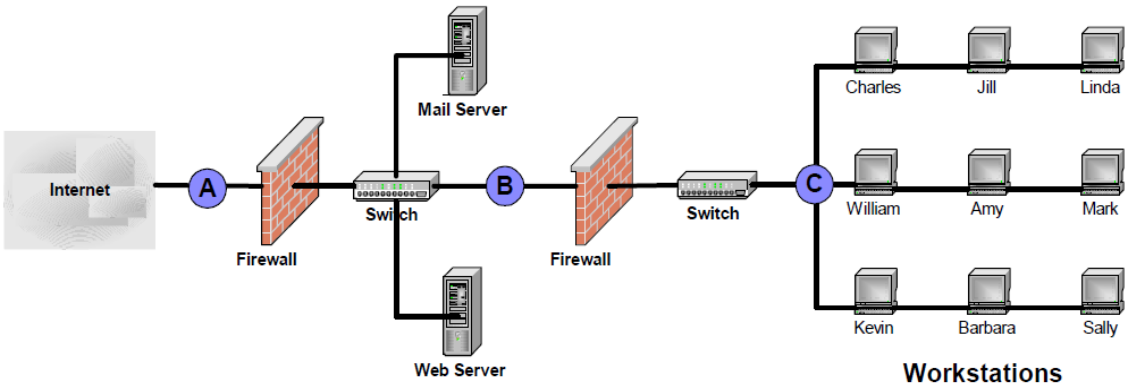

Figure 11: Network Detection Zones [27]

Zone A

This zone is in front of the main firewall. The main characteristic of this zone is the number of attacks logged. Frequent port scanning attempts, worm attacks and other network attacks are found in this network detection zone. The IDS must have the following characteristics to operate in this zone:

- Employ firewall protection on the external interface
- Allow logging of all attacks while offering user selectable alert notification for critical attacks
- Trigger alerts originating from both internal and external networks

Zone B

This zone is behind the main firewall so the number of attacks is dramatically lower than those experienced in Zone A. When the IDS triggers in this zone the threat is more serious in nature. IPS threshold settings may be tightened to lower or more sensitive levels in this zone.

Zone C

In this network detection zone a properly configured IDS will see fewer alerts than Zone B. The IDS and IPS threshold settings may be tightened to the lowest levels in this zone.

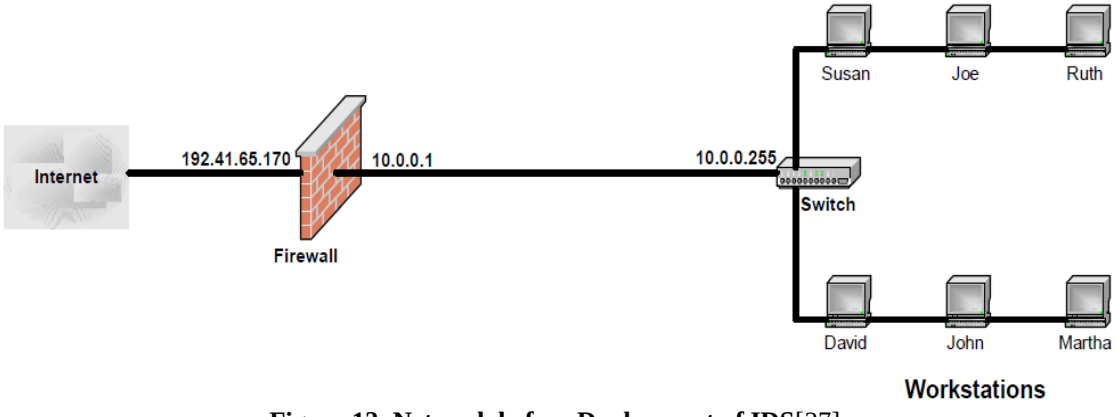

Figure 12: Network before Deployment of IDS[27]

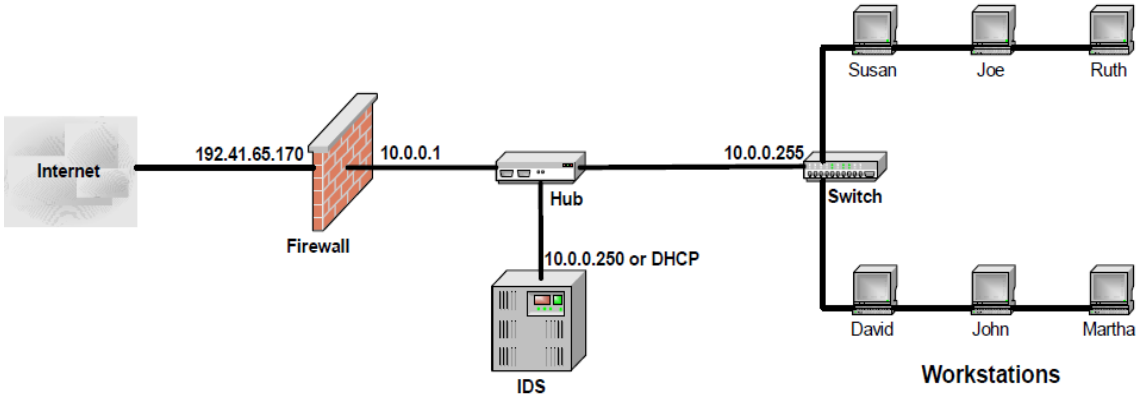

Figure.13: Network after deployment of IDS

3.2 Security Metrics Intrusion Detection Technology [27]

Security Metrics Intrusion Detection System is comprised of a number of subsystems or modules. Each of these components performs specific features. The following illustration shows the main components

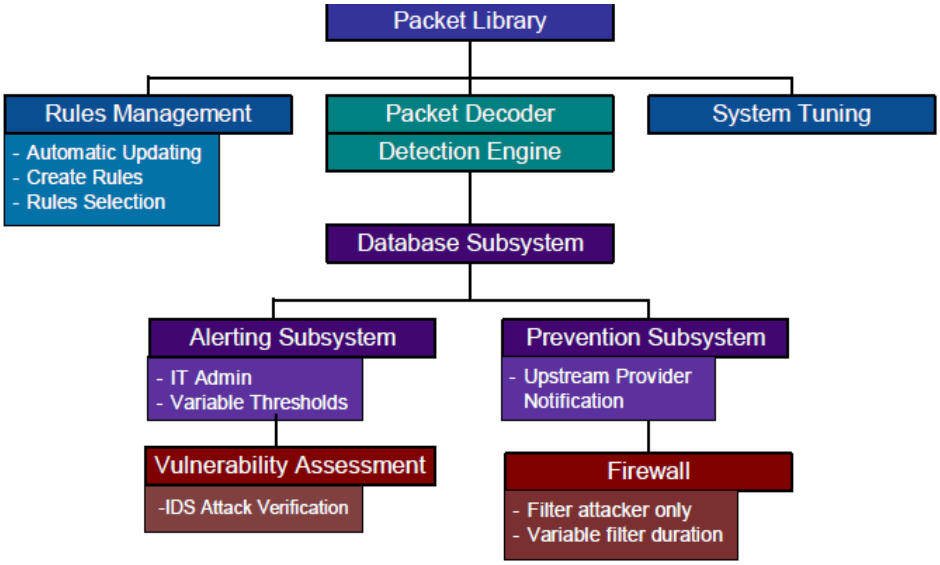

Figure 14: Security-Metrics Intrusion Detection Technology [27]

All the above measures are palliative. However, the most reliable authentication and integrity system today is the biometric frontiers.

IV. CONCLUSION

Cybercrime is real. The internet is the nervous centre of world economy. Cybercrime is conducted remotely and anonymously to take advantage of flaws in software code. Cybercrime has created major problems and has continued to increase at institutions of higher learning, the academia. The academia is emerging as a particularly vulnerable for internet crime. Organizations and individuals have suffered losses at the hands of cyber-criminals with only nine percent of such incidents reported to the security operatives. US organizations alone have estimated a loss of over $67 billion in 2005 [47]. Approximately nine out of every 10 US firms have experienced a cybercrime in [48]. In the lighting of the foregoing reports, I recommend as follows [49]:

1. There is need for consistent training of the Nigerian Police in Cybercrime Prevention and Forensic science for cyber crime policy and control.
2. Development of national community education and training targeted at school children and senior communities.
3. Establishment of a centralized national reporting centre such as the IC# (Internet Computer Crime Complaints Centre) in the US which is managed by the FBI which is online crime reporting centre and clearing house for cyber crime. The IC3 plays a pivotal role in detecting and reporting the identity of cyber criminals and proving information to victims of cyber crime.
4. Deployment of Biometrics and device fingerprinting supported by secure gateways and quality encryption. This strategy will assist in overcoming the anonymity of a good deal of internet activity and provide enhanced security.

5. There is urgent need to develop a single national database to gather and compile cybercrime data.
6. The National Assembly should consider enacting a legislation that encourages incident reporting while reducing the risks associated with reporting and provide policies that provide stronger sentences for those found guilty of committing a cybercrime.

REFERENCES

[1] Osuagwu O.E. (2007, 2008) ***Global Internet Terrorism & Fraud Pandemic: E-Commerce Bottlenecks and the Challenge of Computer Forensics,* M.S/PhD Dissertation, American Heritage University of Southern California, San Bernardino, California.**

[2] Osuagwu O.E. (2008) ***Software Engineering: A Pragmatic and Technical Perspective*,** Olliverson Industrial Publishing House, (OIPH) Owerri, Nigeria, pp.478-499

[3] Osuagwu O.E. (2008) ***Insight into the New Frontiers of Computer Forensics & Cyber-Criminality (with Case Studies),*** OIPH, Owerri, Nigeria.

[4] Osuagwu O.E. et.al. (2007) ***Blocking Credit Card Fraud via Biometric Authentication Systems,*** Proceedings of the International Conference of the Nigeria Computer Society, Concord Owerri June 2007

[5] U.S. Federal Trade Commission (FTC)

[6] A U.S. FTC survey released in September 2003

[7] www.Incardtechnologies.com

[8] **Computer crime,** October 2006 Number 271 Page 2

[9] 2002/03 British Crime Survey

[10] Osuagwu O.E. et.al. (2007) Blocking Credit Card Fraud via Biometric Authentication Systems, Proceedings of the International Conference of the Nigeria Computer Society, Concord Owerri June 2007

[11] http://www.webopedia.com/term/c/cyber_FORENSICS.htm http://www.iwar.org.uk/cip/resources/pcipb/cyberstrategy.htm "2003 Computer Crime and Security Survey," Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001, 2003.

[12] Ken Baiman (2006).

[13] Robbins, Judd,(20040) "***An Explanation of Computer Forensics***," National Forensics Center, 774 Mays Blvd. #10 143, Incline Village, NV 89451, 2004 [The Computer Forensics Expert Expert Witness Network, 472 Scenic Drive, Ashland,OR] (©2004, National Forensics Center. All rights reserved), 2001.

[14] Vacca, John R.(2002), ***The Essential Guide to Storage Area Networks***, Prentice Hall, New York, 2002

[15] Alfred C. Weaver (2006) ***Biometric authentication***, Computer Feb 2006.

[16] Anil K. Jain & Sharathchandra Pankanti (2006) ***A Touch of Money***, IEEE Spectrum July 2006.

[17] Willie D. Jones (2006) Blood ***Test – Vascular Patterns Provide New Means of Identification and Authentication***. IEEE Spectrum

[18] Federal Ministry of Justice (2004) IT Bill 2004

[19] Noblett, Michael G., Pollitt, Mark M., and presley, Lawrence A. (2002) Recovering and Examining computer Forensic Evidence, US. Department of Justice, Federal Bureau of Investigation, Forensic Science Communications, Vol. 2, No. 4 (www.Fbi.gov).

[20] Nelson, Bill, Phillips, Amelia, Enfinger, Frank, and Steward, Chris (2004), ***Guide to Computer Forensics and Investigations*** Thomson, Course Technology, Boston.

[21] New Technologies, Inc (Forensics-intl.com).

[22] Rude, Thomas, (2000) Guidance Seizure Methodology for Computer Forensics, http://www.crazy nights.com/seizure.html.

[23] Wolfe, Henry B., (2003). ***Computers and Security***, El Servier Science, Ltd., pp. 26-28 (www.sciencedirect.com).

[24] http://www.protegga.com/services.html.

[25] Osuagwu O.E., Anyanwu E. (2003) ***Management of Information Technology at Periods of Technological Discontinuity***, OIPH, Owerri, Nigeria, p.23.

[26] FIB Anthrax Report (2001)

[27] https://www.securitymetrics.com/docs/IDSWhitepaper.pdf

[28] Osuagwu O.E. Ogiemien T & Okide S (2010) *Deploying Forensics Science & Technology for Resolving National Cyber-Security Challenges, International Journal of Mathematics & Technology, Azibijan, Russia, August 2010.*

[29] ChiChao Lu, Wen Yuan Jen & Weiping Chang, Shihchieh Chou(2006), ***Journal of Computers,*** Vol. 1. No. 6, Sept. 2006, Academicy Publisher, USA.

[30] Denise Marcia Chatam (2007) The Study on Cybercrime's Impact in the Workplace, *Campus Technology, USA.* URL

[31] Whitney, S. (2004, December 1). ***Trend turns, more purchase coverage for cybercrime***. Best's Review, 105(8):90. Oldwick, NJ: A.M. Best Co. Inc.

[32] Williams, P. (2002). ***Organized crime and cybercrime: Implications for business***.Retrieved electronically October 15, 2007, from URL: http://www.cert.org/archive/pdf/cybercrimebusiness.pdf#search='FBI%20cyber%20crime%20profit'.

[33] Bigelow, B. V. (2005, February 3). ***Computer theft may put workers' data in danger***.Knight Ridder Tribune Business News. Washington, DC: Knight Ridder Tribune Information Services.

[34] ibid

[35] US copyright and privacy laws, Health Insurance Portability and Accountability Act (HIPAA), and the Gramm Leach-Bliley Act (GLBA) (Electronic Privacy Information Center, 2004

[36] McConnell, B. W. (2001, March 6). ***Hearing on cybercrime, Committee on Legal Affairs and Human Rights***, Parliamentary Assembly of the Council of Europe. Paris, France: McConnell International.

[37] ***United States Department of Health and Human Services***. (2003, May). Office for Civil Rights (OCR) Privacy Brief, Summary of the HIPAA Privacy Rule, HIPAA Compliance Assistance. Retrieved electronically December 29, 2006, from URL: http://www.hhs.gov/ocr/privacysummary.rtf.

[38] Bigelow, B. V. (2005, February 3). ***Computer theft may put workers' data in danger***.Knight Ridder Tribune Business News. Washington, DC: Knight Ridder Tribune Information Services

[39] Evans, M. P., and Furnell, S. M. (2000). ***Internet-based security incidents and the potential for false alarms***. Internet Research: Electronic Networking Applications and Policy, (10)3, pp. 238 – 245. Plymouth, UK: MCB University Press

[40] McNeil Solida, M. (2003, February 18). ***Ex-pension employee is charged***. Retrieved electronically December 28, 2006, from URL:http://www.carlbrizzi.com /news/display.php3?NewsID=71

[41] Barr, J. G. (2003, December). ***Monitoring employee computer usage.*** Retrieved electronically December 27, 2004, from URL: http://80www.faulkner.com.ezproxy.apollolibrary.com/products/securitymgt/docs/monitoring1203.htm.

[42] McConnell, B. W. (2001, March 6). ***Hearing on cybercrime, Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe***. Paris, France: McConnell International.

[43] United States Department of Justice. (2005, December 28). ***Man pleads guilty to infecting thousands of computers using worm program then launching them in denial of service attacks.*** Retrieved electronically April 17, 2006, from URL: http://www.cybercrime.gov/clarkPlea.htm.

[44] ibid

[45] McConnell, B. W. (2001, March 6). ***Hearing on cybercrime, Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe***. Paris, France: McConnell International

[46] White, G. A., & Kern, R. W. (2006, February 28). ***Cleveland, Ohio man sentenced to prison for bank fraud and conspiracy***. Retrieved electronically April 17, 2006, from URL: http://www.cybercrime.gov/flurySent.htm.

[47] Evers, J. (2006, January 19). ***Computer Crime Costs $67 Billion, FBI Says***. Cnet News.com. Retrieved electronically September 30, 2006, from URL: http://news.com.com/Computer+crime+costs+67+billion%2C+FBI+says/21007349_3-6028946.html?tag=cd.top.\

[48] Citrano, V. (2006, January 20). ***Mueller's FBI puts computer crime losses at $32M.*** Retrieved electronically September 1, 2006, from URL:http://www.forbes.com/facesinthenews/2006/01/20/fbi-computer-securitycx_vc_0120autofacescan07.html?partner=vnu.

[49] Akpan AG et. al. (2018). Cybercrime and Cybersecurity: A Painted Scenario of a New Type of War. Journal of Scientific and Engineering Research, 2018, 5(10): 185 – 197. ISSN: 2394 – 2630. CODEN (USA): JSERBR. Retrieved from: www.jsaer.com.

