A Strategic Assessment of Cyber Security Strategies and Mitigation of Cybercrime in Nigeria

By

AKPAN, E. Ebenezer, *Ph.D, FCICN, AP, PPGDCA, PHDCDPM*
Corporate Institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State

Abstract

The study strategically examined cyber security strategies as a mitigation method of cybercrime in Nigeria. The population of this study consisted of all experts and post graduate students in computer science, computer engineering and security management studies in Nigeria. The study adopted descriptive survey research design while stratified random sampling technique was used in selecting the respondents. The instrument for data collection which was tagged "Cybercrime and Cyber Security Questionnaire (CCSQ)" was administered to the respondents and used for the study. The instrument was vetted by the researcher's supervisor who is an expert in the field before the reliability test was conducted which produced the reliability coefficient of 0.75 proving the instrument to be reliable for the study. Data collected were analyzed using descriptive analysis and chi-square analysis. From the results of the data analysis, it was observed and concluded that there are many cases of cybercrimes in Nigeria and Nigeria has begun to do something to strengthen cyber security for the good of the country. It was therefore recommended that government should create dedicated national and regional cybercrime units to deal with forensic retrieval of computer-based evidence.

KEY WORDS: Strategic Assessment, Cybercrime, Cyber Security, Mitigation and Nigeria.

Introduction

Our society is highly digitized. On a typical day, people use various information technology (IT) applications on the web. With the digitization of society, crime has also digitized. On the one hand, there are new offenses, such as hacking databases and taking down websites or networks. On the other hand, there are traditional forms of crime in which IT plays an increasingly important role in its realization, examples are internet fraud and cyber stalking. Digitization has consequences for the entire spectrum of crime and raises all sorts. According to Moore (2005), cybercrime, or computer oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Warren, Kruse, Jay and Heiser (2002) assert that cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".

Halder and Jaishankar (2011) opine that cybercrime may threaten a person or a nation's security and financial health. Steve (2016) observed and reported that issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child

grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

According to Gordon (2006), these crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have, which explains how unprepared the society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. Criminal activity on the Internet is wide-ranging and can include an assortment of offenses such as illegal interception, copyright violation, stalking, money laundering, extortion, fraud and resource theft involving the illegal use of computers (Broadhurst and Choo, 2011).

A common method of automated cybercrime at present is the use of spam and malicious websites with the goal of compromising computers (Alazab, Layton, Broadhurst and Bouhours, 2013). Ostensibly the Internet has made certain crimes simpler to carry out: Identity theft is one such example in which personal information is misappropriated for crime. The Internet has made it easier to access vast amounts of personal information on individuals for the purposes of identity theft (Smith, 2010). As observed by Chabinsky (2010), the larger criminal enterprise comprises various cybercriminals with specialised functions one of which includes money mules specifically hired to visit banks to transfer proceeds from online fraud. In certain scenarios, stolen credit card details are used to order packages, by a cybercriminal, and sent to a money mule that subsequently ships the package to another destination, that is, to the money mule "herder" (Australian Institute of Criminology, 2007).

There are also cases of money mules that receive bank deposits and, after withdrawing a small cut, transfers the rest of the funds to another individual in the crime ring (Stone-Gross et al., 2013). In organised online fraud operations, cybercrime activity can often extend beyond the Internet and involve “unwitting and inexperienced” (Krebs, 2012) individuals with no requirement to access the Internet or the knowledge that they were involved in any sort of illegal activity. Cybercrime can manifest in different forms, and the pathway and means for offenders to engage in specific acts of cybercrime are diverse. Interaction between offenders can certainly take place exclusively online and so too the offender-victim engagement, however it should be underscored that cybercrime ultimately affects the “offline”, for example, banks and financial institutions, businesses, and day-to-day Internet users.

Cyber security on the other hand consists of technologies, processes and measures that are designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects entities, organisations and individuals from the deliberate exploitation of systems, networks and technologies (Michael and Tobby, 2015). Cyber security is effective without compromising the usability of systems and there is a robust continuity business plan to resume operations, if the cyber attack is successful. While rapid advancement and technological developments are constantly being recorded in the ICT sector, the volume and sophistication of cyber-attacks are also increasing, therefore serious attention must be given to the protection of personal or business information transmitted in the cyber space as this ultimately impacts on national security as well. There is therefore an increasing

awareness of the need to address cyber-security threats in Nigeria and Africa as a whole. This study therefore investigates strategic assessment of cyber crime and cyber security in Nigeria.

Statement of the Problem

Cases of cybercrime are becoming increasingly evident worldwide occurring irrespective of geographic and political borders. Cyber threats are now the most effective way to attack an organization or country and the fact is that those with malicious intent are finding ever more sophisticated ways of carrying out their activities. It is common for cybercrime offenders to initiate attacks from one country that target those in another. The cross border nature of cybercrime is frequently exploited by cybercriminals from safe havens, and thus underlines the need for cross-national and international responses to combat cybercrime. In the case of Nigeria, cybercrime is a growing risk across the society ranging from hacking and internet fraud to various online scams and phishing activities which involves phishing through emails, instant messaging and other forms of Internet communication that attempt to trick victims into revealing personal private information. This has threatened the cyber security in the country; hence this study seeks to strategically assess cyber crime and cyber security in Nigeria.

Objectives

The main objective of the study was to carry out strategic assessment of cybercrime and cyber security in Nigeria, while the specific objectives are as follows:

1. To examine the effects of cybercrimes in Nigeria
2. To find out the extent to which cyber security strategies have helped in reducing cybercrimes in Nigeria.

Research Questions

The following research questions will be answered:

1. What are the effects of Cybercrimes in Nigeria?
2. To what extent have cyber security strategies helped in reducing cybercrimes in Nigeria?

Research Hypothesis

The hypothesis below will be tested:

1. There is no significant difference in the perception of people as regards the effects of cyber security strategies on the reduction of cybercrimes in Nigeria.

Significance of the Study

This study is of great importance to the security services in their battle to fight cyber crime in the nation. It will expose them to various cyber crime activies and hence bring awareness on threats. The result of this study will be beneficial to the public, in that they will be aware of cyber terrorism and know how to avoid it.

This study will be of value to the government in that they will know how to effectively combat this menace because of cyber-attacks in the country by maintaining citizen-to-government communications, protect sensitive information as well as safeguard national security. This study will be of value to the policy makers and regulators such that they will gain

insight on cyber crimes. This will influence policy makers formulating informed policies concerning the overall cyber security of the country.

This study will also provide basis for reference in future research. The scholars, researchers, students, security service will find this study valuable as they will gain knowledge and carry out further security studies on the topic.

LITERATURE REVIEW

Concept of Cyber Crime

According to Smith, Grabosky and Urbas (2004), cybercrime includes events committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. Cyber crimes are broadly categorized into three categories, namely crime against individual, property and government (Gordon and Sarah, 2006). Each category can use a variety of methods and the methods used vary from one criminal to another:

Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Law enforcement agencies take this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

Property: Susan and Brenner (2010) assert that just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

According to Bowker (2012), when any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location (Denning, 1999). In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection.

Yahoo Attack: Also called 419, it is characterized by using e-mail addresses obtained from the Internet access points, using e-mail address harvesting applications (web spiders or e-mail extractor). These tools can automatically retrieve e-mail addresses from web pages and send messages to unsuspecting victims defrauding them of their cash.

Credit Card or ATM Fraud: Credit card or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction or when withdrawing money using ATM card. The hackers can abuse this card by impersonating the credit card holder.

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history (Kshetri, 2010).

Ransomware: This is one of the detestable malware-based attacks. Ransomware enters your computer network and encrypts your files using public-key encryption, and unlike other malware this encryption key remains on the hacker's server. Attacked users are then asked to pay huge ransoms to receive this private key (Choo, 2007).

DDoS attacks: DDoS attacks are used to make an online service unavailable and bring it down, by bombarding or overwhelming it with traffic from multiple locations and sources. Large networks of infected computers, called Botnets are developed by planting malware on the victim computers. The idea is normally to draw attention to the DDOS attack, and allow the hacker to hack into a system. Extortion and blackmail could be the other motivations (Barford & Yegneswaran, 2007).

Botnets: Botnets are networks of compromised computers, controlled by remote attackers in order to perform such illicit tasks as sending spam or attacking other computers. Computer Bots can also be used act like malware and carry out malicious tasks. Then can be used to assemble a network of computers and then compromise them (Yar, 2005).

Spam and Phishing: Spamming and phishing are two very common forms of cybercrimes. Spam is basically unwanted emails and messages. They use Spambots. Phishing is a method where cyber criminals offer a bait so that you take it and give out the information they want. The bait can be in form of a business proposal, announcement of a lottery to which you never subscribed, and anything that promises you money for nothing or a small favor.

Cyber Stalking: The fraudster follows the victim by distributing mails and entering the chat rooms frequently.

Concept of Cyber Security

The International Telecommunications Union [ITU] defines Cyber security as "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."

Basically, Ravi (2003) asserts that cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across the world. The ITU also notes that the three broad security objectives are ensuring Availability; Integrity (which may include authenticity and non-repudiation), and Confidentiality. While these are the bedrock of a secure network, achieving these three objectives is no mean feat as it requires the integration of various functions such as robust systems engineering and configuration management; effective cyber security or information assurance policy and comprehensive training of personnel. 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 - the internet (Steffani, 2006). Cyber Security can also be described as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (Thilla, 2012).

Functions of a Cyber Security Center:

Ideally, a Cyber Security Center should strive to ensure a secure and resilient cyber and communications infrastructure that supports national/ regional security, a vibrant economy, and the health and safety of all citizens. To achieve this, a Cyber Security Center ought to:

- Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the Nation;
- Pursue whole-of-nation operational integration by broadening and deepening engagement with its partners through information sharing to manage threats, vulnerabilities, and incidents.
- Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.
- Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security.
- Protect the privacy and constitutional rights of the citizens in the conduct of its mission.

Effects of Cybercrime in Nigeria

Cybercrime affects all areas of society from the private to the public sector, ranging from home users, small to large businesses, and government. As of 2015, the total number of Internet users worldwide is over 3.2 billion (Internet Live Stats, 2015). This statistic is likely to grow with the ubiquity of mobile technologies allowing people to access the Internet from any location. Kuhn (1962) observed that the internet now permeates all areas of culture and has radically altered the way we live our lives. People are ever more embracing technology due in part to the release of new technological devices and decreasing cost of computers. Communication now commonly takes place exclusively in an online environment and has changed the nature of how people interact socially on all levels.

According to Easttom (2010), becoming the victim of cyber crime can have long-lasting effects on your life. One common technique scammers employ is phishing, sending false emails

purporting to come from a bank or other financial institution requesting personal information. If you hand over this information, it can allow the criminal to access your bank and credit accounts, as well as open new accounts and destroy your credit rating. This type of damage can take months or even years to fix. Fafinski, (2009) asserts that the overall monetary losses from cyber crime can be immense. According to a 2012 report by Symantec, more than 1.5 million people fall victim to some sort of cyber crime every day, ranging from simple password theft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cyber crime worldwide every year. As consumers get wise to traditional avenues of attack, cyber criminals have developed new techniques involving mobile devices and social networks to keep their illicit gains flowing.

Hacking often results in a loss of data due to personal, organizational, business or governmental files being deleted or changed. Customer information and order information can be stolen and deleted, or a leak of top secret information could cause real-world security issues. Sometimes, these hackers even post information from these governmental organizations online, which could in theory cause unrest between countries. Grabosky (2006) asserts that when hackers gain access to your computer, they can see everything. Since much of the personal, professional and financial parts of our lives have moved online, one risk losing much more than money or information. Because of the Internet, privacy is limited, usually by choice. A hacker with access to your email, social networking accounts and personal photos can very quickly destroy that privacy.

According to Jaishankar (2011), the cyber crime of piracy has had major effects on the entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of naira per year. In response, copyright holders have lobbied for stricter laws against intellectual property theft.

Combating Cyber Crimes and Preventive Measures in Nigeria

Combating cybercrime is a particular challenge for countries lacking cybercrime-specific legislation and policy instruments (Broadhurst, 2006). It is considered common for countries with Internet access to be affected by the cybercrime problem at some level. It is advised that people should not give out their credit card details online and also regulate the way they click on ads and share personal information online. Shafic and Adamu (2011) assert that in order to combat cyber crimes in Nigeria, the police should have a Central Computer Crime Response Wing to act as an agency that advises the state and other investigative agencies on how to coordinate computer crime investigation.

Ribadu (2011) proposed that the country should set up National Computer Crime Resource Centre, a body, which will comprise of experts and professionals to establish rules, regulations and standards and authentication of each citizens' records to easily trace fraudsters. Forensics commission should be established, which will be responsible for the training of forensics personnel/law enforcement agencies so as to decipher fraudsters and scammers easily. Above all, Brenner (2011) is of the view that a comprehensive law to combat computer and cyber related crimes should be promulgated to fight this deadly phenomenon.

Strategies for Effective Cyber Security Operations against prevalence of cyber crime in Nigeria

Nigeria like most other country recognizes the importance of cyber security and is actively involved in the implementation of the Global Cyber Security Agenda and has taken concrete steps to secure its cyber space. In December, 2014, Nigeria published its National Cyber Security Strategy which clearly mapped out Nigeria's National Cyber Security Vision and the strategies for achieving this vision. Furthermore, in May, 2015 the President of the Federal Republic of Nigeria signed into law the Nigeria Cybercrime (Prohibition, Prevention, etc.) Act. The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria in order to eradicate cybercrime challenges in the country, (Michael, D. and Tobby, 2015). The Act also ensures the protection of critical national information infrastructure, and promotes Cyber Security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. The Nigeria National Computer Emergency Response Team (ngCERT) Operations Center was also officially commissioned in May, 2015 by the National Security Adviser. The MITRE Corporation in its 2014 publication suggested ten strategies for effective Cyber security operation centers regardless of their size, offered capabilities or type of constituency served. These strategies include the following:

1. Consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance under one organization: the CSOC.
2. Achieve balance between size and visibility/agility, so that the CSOC can execute its mission effectively.
3. Give the CSOC the authority to do its job through effective organizational placement and appropriate policies and procedures.
4. Focus on a few activities that the CSOC practices well and avoid the ones it cannot or should not do.
5. Favor staff quality over quantity, employing professionals who are passionate about their jobs, provide a balance of soft and hard skills, and pursue opportunities for growth.

METHODS

Research Design

A descriptive survey design was used for this study. In this type of design the researcher assesses and describes the extent and the effect of the concerned variables used for the study.

Area of the Study

The research area for this study was Nigeria.

Population of the Study

The population of this study comprised all experts and post graduate students in computer science, computer engineering and security management studies.

Sample and Sampling Techniques

A stratified random sampling technique was used to draw the 300 respondents and used for the study.

Instrumentation

The main instrument used in this study was questionnaire titled "Cybercrime and Cyber Security Questionnaire" (CCSQ). The questionnaire was made up two sections, (sections A and B). Section A was used to collect information on personal data of the respondents while section B of the questionnaire was made up of two variables such as cyber security strategies and cybercrimes. The obtained data was coded statistically before the statistical analysis of the data.

Validation of the Instrument

The instrument passed through face and content validated by the experts in test and measurement in our university.

Reliability of the Instrument:

Cronbach Alpha technique was used to determine the level of reliability of the instrument. In the trial test, a total of 30 respondents who did not form part of the main study were randomly selected from one of the state not used for the study. The reliability coefficient, obtained was (0.75) and considered high enough to justify the use of the instrument.

Procedure for Collecting Data

A letter of introduction was written by the researcher. This letter was to introduce the researcher to the heads of the organizations for understanding and assistance. The questionnaire were issued and retrieved 3 days latter from each respondent. The exercise took about one week.

Method of Data Analysis

The researcher subjected the data generated for this study to appropriate statistical techniques such as descriptive analysis and chi-square analysis. The test for significance was done at 0.05 alpha levels.

RESULTS AND DISCUSSIONS

Research Question One

The research question sought to find out the effect of Cybercrimes in Nigeria. In order to answer the question, percentage analysis was used. (See table 1)

Table 1

Percentage analysis of the effects of Cybercrimes in Nigeria.

Effects of Cybercrime	FREQ	%	Ranking
Financial Losses	91	30.33**	1st
Loss of Information	33	11	5th
Decreased Privacy	45	15	3rd
Damaged Reputation	21	7	6th

Economic Data	60	20	2nd
Direct Costs	39	13	4th
Secondary Attacks	11	3.67*	7th
Total	**300**	**100%**	

** The highest percentage frequency
* The least percentage frequency
SOURCE: Field survey

From the result of the above table 1, it was observed that the most frequent effect of cybercrime in Nigeria was financial loss (30.33%), while secondary attack (3.67%) was the least prevalent effect.

Research Question 2

The research question sought to find out the extent to which cyber security strategies have helped in reducing cybercrime in Nigeria. In order to answer the question, percentage analysis was used, (see table 2).

Table 2

Percentage analysis of the extent to which cyber security strategies have helped in reducing cybercrime in Nigeria

Cyber Security Strategies	**Freq**	**Percentage**
VERY HIGH EXTENT	84	28
HIGH EXTENT	145	48.33**
LOW EXTENT	37	12.33
VERY LOW EXTENT	34	11.33*
TOTAL	**300**	**100%**

** The highest percentage frequency

* The least percentage frequency

SOURCE: Field survey

From the result of the above table 2, it was observed that the highest percentage (48.33%) of the respondents attested that the extent to which cyber security strategies help in reducing cybercrime in Nigeria is of high extent, while the lowest percentage (11.33%) affirmed very low extent as regards cyber security strategies contribution to reduction of cybercrime in Nigeria.

Hypothesis 1

The Null hypothesis states that there is no significant difference in the perception of people as regards the effects of cyber security strategies on the reduction of cybercrimes in Nigeria. To test the hypothesis, chi-Square analysis was performed on the data (see table 3)

Table 3

Chi-square analysis of the difference in the perception of people as regards the effects of cyber security Strategies on the reduction of cybercrimes in Nigeria.

Extent of effects	Observed Frequency	Expected Frequency	X^2
VERY HIGH EXTENT	84	75	
HIGH EXTENT	145	75	
LOW EXTENT	37	75	108.08*
VERY LOW EXTENT	34	75	
TOTAL	**300**	**300**	

***Significant at 0.05 level; df = 3; Critical = 7.82**

Table 3 shows the calculated X^2-value as (108.08). This value was tested for significance by comparing it with the critical X^2-value (7.82) at 0.05 levels with 3 degree of freedom. The calculated X^2-value (108.08) was greater than the critical X^2-value (7.83). Hence, the result was significant. The result therefore means that there is significant difference in the perception of people as regards the effects of cyber security Strategies on the reduction of cybercrimes in Nigeria. The result was in agreement with the research findings of (Michael, and Tobby, 2015) who said that the Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria in order to eradicate cybercrime challenges in the country. The significance of the result caused the null hypotheses to be rejected while the alternative one was accepted.

Conclusions

Based on the findings of the research work, it has been concluded that there are many cases of cybercrimes in Nigeria. Besides, the country, Nigeria has begun to do something to strengthen cyber security for the good of Nigeria. With the application cyber security in Nigeria the issue of cyber crimes has been reduced.

Recommendations

Based on the findings of the research work, it is recommended that:

1. Government should create dedicated national and regional cybercrime units to deal with forensic retrieval of computer-based evidence.

2. The Cross Domain Solution should be adopted in organizations which offer a way to keep all information confidential by using safe and secure domains that cannot be tracked or accessed.
3. The country should set up a National Computer Crime Resource Centre, a body, which will comprise of experts and professionals to establish rules, regulations and standards of authentication of each citizen.
4. Individuals should not let out their personal bank and other secured details on a public site. Secondly, while logging into your bank, ensure the communication is secured.

REFERENCES

Alazab, D., Layton, C., Broadhurst, F. & Bouhours, C. (2013) Zero-day malware detection based on supervised learning algorithms of api call signatures. *Paper presented at the Proceedings of the Ninth Australasian Data Mining Conference-Volume 121.*

Australian Institute of Criminology (AIC). (2007) Money mules, High Tech Crime Brief No 16. Available on: http://www.aic. gov.au/publications/current%20series/htcb/1-20/htcb016.aspx [Date accessed 01.08.2011.].

Barford, M. & Yegneswaran, D. (2007). Influence of data discretization on efficiency of Bayesian classifier for authorship attribution. *Procedia Computer Science*, *35,* 1112-1121.

Bowker, A. *(2012).* The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st entury. *Springfield: Thomas.* ISBN 9780398087289.

Brenner, S. (2011) *Law in an Era of Smart Technology,* Oxford: Oxford University Press

Broadhurst. L. O. & Choo. M., (2006). Broadhurst, R., and Chang, Lennon Y.C. (2013) "Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds), *Asian Handbook of Criminology* (pp. 49–64). New York: Springer (ISBN 978-1-4614-5217-1)

Chabinsky, S. R. (2010). Cybersecurity strategy: A primer for policy makers and those on the front line. *Journal of National Security Law and Policy, 4*(1), 27–40.

Choo, H. (2007). The Influences of Compiler Optimization on Binary Files Similarity Detection. *Paper presented at the 2013 the International Conference on Education Technology and Information System (ICETIS 2007)*.

Denni, S M. (1999). "War is War? The utility of cyberspace operations in the contemporary operational environment" *(PDF). Center for Strategic Leadership. Archived from* the original *(PDF)*

Easttom, C. (2010) *Computer Crime Investigation and the Law*

Fafinski, S. (2009) *Computer Misuse: Response, regulation and the law* Cullompton: Willan

Gordon. S. (2006). "On the definition and classification of cybercrime" *(PDF).* Retrieved January 14, 2018.

Grabosky, P. (2006) *Electronic Crime,* New Jersey: Prentice Hall

Halder, D. & Jaishankar, K. (2011) *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

Internet Live Stats, (2015) Internet Users by Country 2015, www.internetlivestats.com/ internet-users-by-country

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal behavior*.

Krebs, B. (2012) Did the Mirai Botnet Really Take Liberia Offline?, *KrebsOnSecurity* https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/, last accessed on January 2, 2017.

Kshetri, D. (2010) *Kshetri, Nir.* Diffusion and Effects of Cyber Crime in Developing Countries.

Kuhn, H. (1999) Cybersecurity Strategy. Retrieved September 13, 2002 from http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecuritystrategy. pdf.

Michael, D. & Tobby, A. (2015) Multiple Execution Paths for Malware Analysis. *Paper presented at the IEEE Symposium on Security and Privacy*.

Moore, R. (2005) *Cyber crime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing.

Ravi. S, (2003) Study of Latest Emerging Trends on Cyber Security and its challenges to Society. *International Journal of Scientific & Engineering Research*, Volume 3, Issue 6, June -2012 1 ISSN 2229-5518 IJSER © 2012

Ribadu, G. (2011) Combating the Menace of Cyber crime. *International Journal of Computer Science and Mobile Computing*, *3(6)*, 980 – 991.

Shafic, F. & Adamu, D. (2011) *Asymmetric cyber-warfare between Israel and Hezbollah*: *The web as a new strategic battlefield.* Proceedings of the ACM WebSci'11, June 14–17 2011, Koblenz, Germany. Retrieved March 22, 2011, from http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf.

Smith, D. (2010*). Cybercrime: law enforcement, security and surveillance in the information age. Routledge, London, J. Soc. Policy* 30(1):300.

Smith, R. G., Grabosky, P. & Urbas, G. (2004). *Cyber Criminals on Trial. Cambridge (UK):* Cambridge UP.

Steffani. A. B. (2006). *The Impact of Information Security in Academic Institutions on Public Safety and Security*: Assessing the Impact and Developing Solutions for Policy and Practice.

Steve, M. *(2016).* Cyber Crime Costs Projected To Reach $2 Trillion by 2019. *Forbes. Retrieved September 22, 2016.*

Susan, W. & Brenner, D. (2010) *Cybercrime:* Criminal Threats from Cyberspace, ABC-CLIO, 2010, pp. 91

Thilla, R. (2012) Associate Lecturer, School of Law, University of Western Sydney, The Society of Digital Information and Wireless Communications (SDIWC), *International Journal of Cyber-Security and Digital Forensics* (IJCSDF) 1(3): 232-240 (ISSN: 2305-0012)

Warren, G., Kruse, D., Jay, G. & Heiser, F. (2002). *Computer forensics: incident response essentials. Addison-Wesley. p. 392.* ISBN 0-201-70719-5.

Yar, M. (2005) *Cybercrime and Society,* London: Sage.