Analysing Issues of Cyber Threats in Nigeria

Boniface K. Alese, Aderonke F. Thompson, Korede V. Owa, Otasowie Iyare., Olufemi T. Adebayo

Abstract—**This paper examines the pattern of cyber threats and information security in line with the Nigerian approach to meeting these challenges in the 21st century. Investigation was carried out on the level of awareness and compliance with the existing cyber security policies among the cyberspace users. The level of enforcement of these policies or measures by cybercafé administrators and government security agencies is also considered. The research employed primarily qualitative methods in the design and analysis. A questionnaire was designed and used in the study. Data obtained from the survey through the questionnaires administered were subjected to analysis using the Statistical Package for Social Sciences (SPSS). The results of the analysis suggest the major group of the populace that are mostly active in committing cybercrime.**

Index Terms: Cybercrime, Cyber Space, Security Agencies, Chitest, Information Security

I. INTRODUCTION

Information Technology (IT) revolution has had impacts in almost every area of human endeavour. From business, industry, government to nonprofit organizations, IT 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 other related cybercrimes. This research, therefore, discusses the following fundamental questions. What are:

a. modern challenges posed by cyber threats?
b. channels through which these challenges occur?
c. modern challenges posed by cyber threats?
d. channels through which these challenges occur?
e. existing mechanisms to curb the trend?
f. efficiency of our information security?
g. the possibilities of modern technique to tackle cyber threats?
h. role of the government in this matter?

Computers are either used as tools or target of the crime. The fundamental nature of computing would contribute in no small measure to the scope and magnitude of this crime.

Manuscript received August 29, 2013; revised on October 11, 2013
B.K. Alese is with the Federal University of Technology, Akure, Nigeria, e-mail: bkalese@futa.edu.ng , +2348034540465
A.F. Thompson is with the Federal University of Technology, Akure, Nigeria, e-mail: afthompson@futa.edu.ng, +2348034897857
K.V. Owa is with the Rufus-Giwa Polytechnic, Owo Nigeria, e-mail: korede.owa@gmail.com, +2348033738090
O. Iyare is with the Federal University of Technology, Akure, Nigeria, e-mail: oiyare@futa.edu.ng, +2347033513174
O.T is with the Federal University of Technology, Akure, Nigeria, e-mail: otadebayo@futa.edu.ng , +2348065793988.

Cyber space is dynamic and changes often at a rapid pace. Moore's laws prediction is observed: as computer increases sophistication in power capacity and communication speed, it also increases the criminal opportunity for motivated offenders as well as the availability of suitable targets. Moreover, the worldwide computer network (Internet) has transformed computer crime from a local problem to an international security issue.

II. LITERATURE REVIEW

Cyber threat can broadly be defined as criminal activities involving an IT infrastructure.

Cyber threats in Nigeria started late 1990s, and have continued to escalate in variation and frequency. Efforts to fight cyber threats have involved a growing number of participants including governments, non-governments, public sectors, and non-profit organizations.

[1] addresses cybercrime from its technical beginnings, through the law enforcement role of pursuit and apprehension, to the final legal issue of prosecution. [2] addresses computer crime investigations and forensics by examining the factors used in determining whether or not a given computer crime is "solvable." The author explores the allocation of effort and resources in pursuing computer crime based on the probability of ultimately solving the crime. [2] views computer crime investigation as a case by case approach as opposed to presenting a cohesive model for understanding cybercrime investigation from a more strategic perspective.

[3] addresses some key concepts to be aware of when examining the process of cyber investigations, such as the tactics of traditional crime and how they apply to computer crime. The author also discusses the necessity of outsourcing investigations to the private sector, as the ability to cooperate with private companies affects both the investigation process as well as outcome (success). In the same vein, [4] points out another critical factor in computer crime investigations: international cooperation. Many western countries may be at the forefront of computer crime forensics and investigations, but other nations may not, and cooperation with them is a critical and on-going challenge.

[5] draws attention to the concern of adequately securing government and military systems as well as addressing vulnerabilities in critical infrastructures in the United States by scrutinizing the context of policy planning and international relations. [6] examination of the concept of cyber warfare delves deeply into the vulnerabilities and political considerations of this new form of conflict. Specifically, the author underscores the dangers related to

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

cyber warfare and outlines future threats and cyber warfare strategies (prevention or defense).

Threat is categorized into four different forms: attack through email, spam associated threats, malware and phishing. Malware threat was further described to reduce system network. Hence, on the case of threats to email, this disallows employees to have access to the original data of the organization. Phishing threats on the other hand, are inform of hacking of vital information especially hacking of credit card information or account information. In attempting exposure reduction to common security threats, the top managers must carry out risk assessment of both internal and external threats to know and identify where risks may come from [7].

An organization is prone to threat if appropriate precautions are not put in place and lack of a strong information system increases the cost of an organization while trying to manage information in an unstructured manner. Moreover, with Federal Financial Institutes Examinations Council (FFIEC) in Nigeria, there are information security breaches. The need to have cyber/information security legislations that comply with ISO 27001 requirements as well as reduces the threat of successful information security breaches and inspires confidence in investors and users cannot be overemphasized [7]. Hence, compliance with international standards afford the organization the assessment and verification opportunities.

In addition, Nigerian Banks compliance with BSI 200th 27000th series is dedicated to ISMS –related documents. In this series, additional standards would soon appear on ISMS guidance, auditing, reviewing and metrics as defined by the ISO JTC1/SC27 roadmap. ISO is a set of standards and methods used as reference for specialists where documents could be identified that are valuable resources for people dealing with ISS. The advent of ISO 27001 (ISO 17799 now change to ISO 27001), brought about an ISM code of practice that helps organizations take information security seriously. It stipulates wide range of security issues such as system policy, system organization compliance, physical control, system organization and so on [7] argues that there is a new information security legislations enacted in Europe and North America that would make it mandatory for organizations to implement adequate information security controls commensurate to the risks that may accrue to systems within their environments.

Information Security policy (ISP) is an important instrument used in ISM to demonstrate the need for and scope of information security [8]. It stipulates the policies, procedures and structure to be followed in the organization. Practically, ISP expresses top management commitment towards protecting the information assets. There are many international standards that explain the procedures and controls that should be conducted into ISP. Adopting these international standards gives ISP an integral role in the success of ISM.

a) Theories

[1] addressed the issue of cybercrime, but did not delve into case management or the over-arching strategy of computer crime investigation. In [5], attention was drawn to the concern of adequately securing government and military systems as well as addressing vulnerabilities in critical infrastructures in the United States by scrutinizing the context of policy planning and international relations. [6] examination of the concept of warefare delves deeply into the vulnerabilities and political considerations of this new form of conflict. In this regard, several of the existing literatures do not address the current state of cyber crime investigations processes and how law enforcement and national security agencies work to effectively address cyber threats globally. In addition, there has been inadequate infrastructure in information security system to combat cyber threats and its challenges in the 21st century.

a) Social Theories

From a social scientific point of view, security theories on providing and implementing protection against breaches and information system misuse have evolved. These theories focus on user security awareness, motivation, deterrents, technology and training [9]. Researchers have theorized that user perception of risks and choices based on those perceptions can influence system security. The situational characteristics theory proponents argued that situations within a system usage domain can impact on ethics and user behaviour [10]. [11] proposed the Human Firewall theory stating that those user actions can undo technical security measures. He advocated that organizations must sensitize and educate users and evaluate their compliance with security policies and procedures. The theory of least possible privilege as proposed by [12] suggests psychological profiling of potential new users, while [13] argues that new users are more vulnerable to security breaches when using information systems (IS). [14] theorizes about defensive information warfare and proposes that security policy training and awareness will better equip users against threats. [15] theorized about using social psychology as a tool to improve user security conduct. The importance of the interest of senior management and integrating security issues as part of the corporate asset protection model was highlighted by [16]. [17] also modeled an Information System security awareness program to address end-users, IT personnel and management executives.

[18] theorized about using values, perceptions and behaviour to change user attitude about security, while [19] argues that ignorance and incompetence about the consequence of security policy abuse is a serious problem among users. [20] proposed a theory that uses rewards and penalties to influence attitudes toward security in information systems.

[21] theorized that the nature of the technology with respect to the user's goals and intentions significantly influence security features and usage in IS systems. They went further to propose the use of training, punishment, and

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

reporting security as a motivation for creating security awareness among users.

[22] adopted a socio cultural approach to information security and posited that the cultural theory can be used to enhance security at different cultural layers-namely, corporate policies, top management, and individuals. [23] used human morality as a force that can impact on security. [24] argued for a theory that uses a holistic IS security architecture to incorporate infrastructure, policies, standards, awareness and compliance. He however, concentrated on awareness training at the expense of all the other components.

a) *Routine Activity Theory*

This theory proposes that three situations facilitate the occurrence of crime. Proponents argue that such events must happen at the same time and in the same space. The three situations are the existence of a suitable target, lack of security, and a motivated offender for the crime to occur [25]. The assessment of the situation determines whether or not a crime takes place.

b) *Technology Theory*

The response of technology to cybercrime centers on the use of computer security theories to design and evolve solutions that provide authentication, integrity, verification, nonrepudiation and validation. These theories and models rely on the use of cryptography, steganography, network protocols, and software engineering process/models to develop systems that offer some form of protection for users and the information infrastructure.

Cyber crime thrives on the web today because the internet did not inculcate in its protocols from the onset a mechanism that allows a host to selectively refuse messages [26]. This implies that a benign host that desires to receive some particular messages must read all messages addressed to it. In essence, a malfunctioning or malicious host has the capacity to send many unwanted messages. This problem is exacerbated by the ubiquitous nature of the web and remains the Achilles heel of the issue of web security today. Although all the theories discussed above are related to cyber crime, we are inclined to adapt routine activity theory to this study because the theory captured the philosophical assumptions upon which this study is based.

c) Space Transition Theory

Proponents of space transition theory argue that behavior of people in cyber space tends to bring out their compliance and noncompliance behavior both in the physical and in cyber space. This theory does not explain physical crime but cyber crime and how people move and behave from one space to the other.

This entails persons with repressed criminal behavior (in the physical space) having a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space, due to their status and position. It also implies that the status of persons in physical space does not transit to cyber space. [27], for instance, argues that the individual behavior repressed in physical space is not repressed in cyber space.

III. RESEARCH MATERIALS AND METHODS

a) Methods

Questionnaires were distributed to 100 cybercafé administrators in Akure Metropolis, the Nigerian Police Force and the Judiciary in order to ascertain the level of awareness of the existing cyber security policies or measures and the level of enforcement of these policies by the cybercafé administrators and government security agencies.

The research on cyber threats and information security employs primarily qualitative methods in research design and analysis. The questionnaire consisted of two sections:

Section A measured the socio demographic variables of establishment. It includes items like name, location, year of operation, principal area of operation and so on.

Section B for the cyber café administrators measured the level of awareness and compliance of cyber security laws and policies of government agencies. While section B for the Nigerian Police Force measured the effectiveness of enforcement of cyber laws and policies and the judiciary measured the level of conviction and prosecution of cyber crime and other internet related offenders.

b) Procedure

The researcher approached and sought the permission of Assistant Commissioner of Police, State Criminal Investigation Department (SCID), Ondo State Command, Ekiti State Command and Osun State Command to administer the questionnaire to the department. Permission was granted after two weeks. The judiciary was also approached for permission which was granted in a week. Questionnaires were also administered to cybercafé administrator. The questionnaire administration spanned four weeks and were scored, coded, and analysed with the Statistical Package for the Social Sciences (SPSS).

c) Statistical Analysis

CHITEST returns the value from the chi-squared (x^2) distribution for the statistic and the appropriate degrees of freedom.

CHITEST(actual_range,expected_range)

Actual_range is the range of data that contains observations to test against expected values.

Expected_range is the range of data that contains the ratio of the product of row totals and column totals to the grand total.

The x^2 test first calculates a x^2 statistic using the formula:

$$\chi^2 = \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{\left(A_{ij} - E_{ij}\right)^2}{E_{ij}} \qquad (1)$$

where:

A_{ij} = actual frequency in the i-th row, j-th column

E_{ij} = expected frequency in the i-th row, j-th column

r = number or rows

c = number of columns

3.1.3 Factors/Indices in the Questionnaire

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Some major factors or indices in the questionnaire are:

- ✓ Are there adequate laws to fight cyber crime in Nigeria?
- ✓ Is the judiciary lifting-up to expectation in terms of cyber crime?
- ✓ Out of every five-offendants prosecuted, how many are convicted?
- ✓ How many of such cases are reported between the last six months?
- ✓ Who are the catgories of individuals that are charged with cyber crime?
- ✓ As technology improves and innovations changes, do reported cases take the same trend?
- ✓ Are there departments that handle cyber crime offenses?
- ✓ Is there an awareness mechanism of sensitizing the public?
- ✓ How often do you train and re-train your personnel?
- ✓ Are there cyber security measures put in place to combat cyber crime?

IV. RESULTS AND DISCUSSION

The data collected from the questionnaire and interviews with their analysis are presented in this section.

The main item of the questionnaire requested the respondents (50) to indicate the approximate age of their customers. Fig I shows the age distribution of the customers of the cafes according to the internet café administrators.

From the Fig I, the approximate age between 18 to 30 years constituted about 88 percent of their customers whilst the remaining 12 percent is shared among the ages of 31-35 and above 35 years. The age distribution suggests that, most of the people who patronize these cafes are young men and were likely to form a majority of perpetrators of the crime. The researchers at the time of administering the questionnaire observed that more adolescent boys below the age of fifteen patronize their services, but in answering the questionnaires, the café administrators tend to have reported a lesser number. In corroborating these findings with the Judiciary response, it was confirmed, that the majority of cyber crime suspects are the youth aged between 21-35 totaling 85 percent of cyber crime suspects.

The question: To what extent are Akure cyber space users aware of the cyber security laws or policies of any government agencies charge with the responsibility of formulating or implementing cyber security laws or policies?

The data obtained from the responses of all cyber café users in order to test their level of awareness of cyber security laws or policies shows that 80% of the respondents are aware of cyber security laws or policies. Chi-Square was used to analyze the distribution of this percentage. The result of this analysis is shown in Table I and II.

From table I, the calculated Chi-Square value is 1.600. Using degree of freedom (df) of 1, the Chi-Square distribution table was used to get the table value using confidence interval of 0.050 and the corresponding table value is 3.835. The calculated Chi-Square value is less than the table value, which emphasized that the customers awareness of cyber security laws or policies of government agencies affect their level of compliance.

From table IV, 50% of the cyber café administrators agreed that most of the cyber space users overlook the cyber security measures being used in the cyber café.

The responses to the various questions in the questionnaire show that the level of awareness of Nigerian Cyber crime Working Group (NCWG) and Directorate for Cyber security (DfC) or any of their policy by the cyberspace users in Akure, Ondo State, Nigeria is very high since only 20% out of the respondents claimed not to have heard of such government bodies. Also, 90% of the cyber café administrators stated that they cannot force cyberspace users to comply with their measures since the business is no more lucrative as it was in the years back and they are not encouraged by the way the law enforcement agencies handled victims of previous raids. Are there adequate laws to fight cyber crime and other internet related offenses in Nigeria?

The data obtained from the responses of the Nigerian Police Force and the judiciary shows that 80% of the respondents are of the opinion that there have not been adequate laws to combat cybercrimes and other internet related offenses in Nigeria. Chi-Square was used to analyze the distribution of this percentage. The result of this analysis is shown in Tables V and VI.

From table V, the calculated Chi-Square value is 1.800. Using degree of freedom (df) of 1, the Chi-Square distribution table was used to get the table value using confidence interval of 0.050 and the corresponding table value is 3.835. Having shown that the calculated Chi-Square value is less than the table value, this emphasized that the available laws to fight cyber crime and other internet related offenses affects the level of conviction, therefore the laws are not adequate enough to prosecute offendants.

V. CONCLUSION

Cyber crime is common to both developed and developing countries. Its impact appears to be worse in developing countries where the technology and law enforcement expertise are inadequate. This shared challenge tends to be reflected in Nigeria. The limited options for the Police, legal and financial institutions to address cyber crime call for a multi-stakeholder analysis at the national level.

Concerning practice and policy implications, the research provides the basis for a concerted effort on the part of individual citizens and corporate bodies, to report cyber crime cases and demand that government put in place laws, policies and technologies to curb cyber crime. As with other forms of ITs, since these laws are critical, there is the need to gain political support. This could be from the government, or political parties, interest groups, private sector advocates, thus key stakeholders who can push for these legislation and rules.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The government should empower the Police force by providing the needed training and technical resources required to discharge their duties effectively. The Central Bank of Nigeria which regulates Commercial Banking operations must develop a reporting scheme on all the identity of all recipients of foreign remittances to it or other agencies of the state so as to create a database that can be reviewed regularly and used for investigating suspicious foreign remittances.

Internet service providers operating in the country should also be mandated to report suspicious traffic going through their networks. Since cyber crime is a global problem, the need also arise for law enforcement agents in Nigeria to collaborate in the area of information sharing, infrastructure and personnel with other African Countries and major international security agencies such as the Federal Bureau of Investigation and INTERPOL (International Police) to crack-down on cyber criminals.

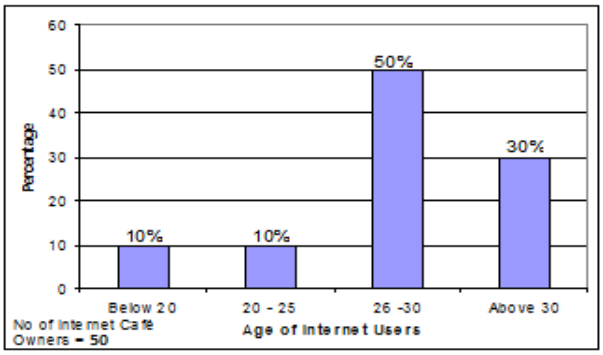

Fig 1: Perceived Age Distribution of Internet Users

Table I: Customers awareness

Customers awareness

	Observed N	Expected N	Residual
No	15	5.0	-2.0
Yes	35	5.0	2.0
Total	50		

Table II: Chi-Square of table I

Test Statistics

	Customers awareness
Chi-Square[a]	1.600
df	1
Asymp. Sig.	.206

a. 0 cells (.0%) have expected frequencies le
5. The minimum expected cell frequency i

Table III: Administrator's responses to security measures available in cyber café

Paper Notice	Scrolling marquee on PC	Disabling of Office Application	None
40%	10%	20%	30%

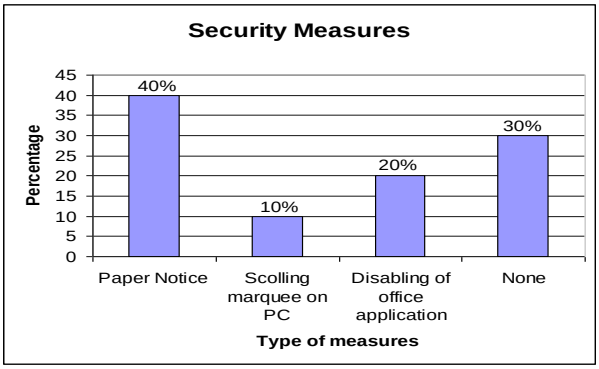

Fig 2: Type of Security Measures

Table IV: Administrator's responses to various Yes/No questions

Questions	Yes	No	Not Sure
Do your customers comply with your cyber security measure(s)?	20	5	25
Have you had a course to report a customer to a security agency?	20	30	0
Will you be willing to hand over any erring customer to the appropriate security agency?	40	0	10

Table V: Adequate Laws

do we have adequate laws to fight cyber crime

	Observed N	Expected N	Residual
No	20	2.5	1.5
Yes	5	2.5	-1.5
Total	25		

Table VI: Chi-Square of table V

Test Statistics

	do we have adequate laws to fight cyber crime
Chi-Square[a]	1.800
df	1
Asymp. Sig.	.180

a. 2 cells (100.0%) have expected frequencies less than 5. The minimum expected cell frequency is 2.5.

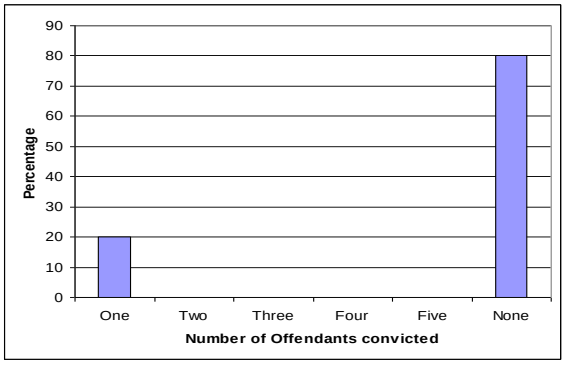

Fig 3: Perceived Number of Offendants Convicted

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

REFERENCES

[1] Reyes, Anthony. Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors. Rockland: Syngress, 2007.
[2] Mendell, Ronald. Investigating Computer Crime in the 21st Century. Springfield: Charles C. Thomas, 2004.
[3] Hinduja, Sameer. "Computer Crime Investigations in the United States: Leveraging knowledge from the Past to Address the Future." International Journal of Cyber Criminology. 1.1 (2007)
[4] Sussmann, Michael. "The Critical Challenges From International High-tech and Computer-related Crime at the Millennium." Duke Journal of Comparative & International Law. 9:451-490, 1999.
[5] Cavelty, Myriam. Cyber-Security and Threat Politics. New York: Routledge, 2008.
[6] Carr, Jeffrey. Cyber Warfare. Sebastopol: O'Reilly, 2010.
[7] Akinsuyi (2009). The drawing of Information Security Legislations, What Nigerian Corporations Can Do to Prepare.
[8] Hone Karin & J.H.P Eloff, (2002). Information security policy what do international information security standards say? Department of Computer Science, and Afrikaans University.
[9] Kajava, J, Varonen, R (2000). Information security education: From the end-user perspective to public administration applications, Verwaltungsinformatik 2000. mdv Halle (Saale), Germany.
[10] Perry, W. (1985). Management strategies for computer security, ButterworthHeinemann Newton, MA, USA.
[11] Wood CC (2002) The Human Firewall Manifesto. Computer Security Journal 18(1): 15- 18.
[12] Beatson JG (1991) Security - a personnel issue. The importance of personnel attitudes and security education. Proceedings of the Sixth IFIP International Conference on Computer Security.
[13] Bray TJ (2002) Security actions during reduction in workforce efforts: what to do when downsizing. Information system security 11(1): 11-15.
[14] Denning DE (1999) Information Warfare and Security. ACM Press, USA
[15] Kabay ME (2002) Using Social Psychology to Implement Security Policies. In: Bosworth S & Kabay ME (eds) Computer Security Handbook, 4th edition. John Wiley & Sons, Inc., USA,32.1-32.16.
[16] Kovacich GL & Halibozek EP (2003) The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program. Butterworth-Heinemann, USA.
[17] Vroom, C. and R. v. Solms (2002). A Practical Approach to Information Security Awareness in the Organization. Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, Kluwer, B.V.
[18] DeLone, W. and McLean, E. (1992). Information System Success: The Quest for the Dependent Variable, Information Systems Research, 3, 1, 60-95
[19] Murray, B. (1991). Running corporate and national security awareness programmes.
[20] Parker, D.B (1981). Managers Guide to Computer Security. Prentice Hall, Virginia.
[21] Sasse A, Brostoff S & Weirich D (2001) Transforming the 'weakest link' a humancomputer interaction approach to usable and effective security. BT technology, Journal 19(3): 122- 131.
[22] Schlienger T & Teufel S (2002) IS security Culture: The Socio-Cultural Dimension in IS security Management. Proceedings of IFIP TC 11.
[23] Siponen, M.T., Oinas-Kukkonen, H.(2007), "A review of information security issues and respective research contributions,". The Database for Advances in Information Systems, 38(1), pp. 60-81.
[24] Tudor JK (2001) IS security Architecture, An Integrated Approach to Security in the. Auerbach Publications, USA.
[25] Cohen, L. and Felson M. (1979). Social Change and Crime Rate Trends : A Routine Activity Approach », American Sociological Review, 44 (4), 1979, pp. 588-608.
[26] Crocker, D.(1982) Standard for the format of ARPA Internet text messages. http://www.rfc-editor.org/info/rfc822.
[27] Jaishankar K., (2008), Space Transition Theory of Cyber Crimes, Crimes of the Internet, Pearson, ISBN-13:978-0-13- 231886-0 pp.283-299.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)