Vol.03,Issue02,Dec.2014

INTERNATIONAL JOURNAL OF RESEARCH PEDAGOGY AND TECHNOLOGY IN EDUCATION AND MOVEMENT SCIENCES (IJEMS)

ISSN: 2319-3050

INVESTIGATION OF CYBER CRIMES

Parveen Sadotra

Teaching Assistant, Govt. Degree College R S Pura, J&K, India

ABSTRACT

Over few 3 decades, international society especially across the industrially developed world has experienced phenomenal technological transformation. The ubiquity of digital technology and its easy integration with human activities has brought a great advantage for us. But at the same time diverse new activities have also emerged in association with technological revolution which we can call cybercrime. Many old techniques of crimes are now being aided through the use of computer and internet. The study of this research work is focused on various types of cyber crimes using various different tricks and techniques along with discussion of various methodologies to investigate cybercrimes. Legal framework of cybercrime also discussed in the paper also all the limitations that are present in our legislation being mentioned. Research findings of the cyber crime investigations are summarized. All the remedial actions and preventive measures are given in the suggestion section.

Keywords: *Casey Model, Cyber Crime, Cyber Criminal, Cyberspace, DFRWS, ICT, Investigation, IPC, IT Act,2000, Models.*

INTRODUCTION:

Internet, a great invention, has revolutionized our lives on this earth. Globalization of economies, and changes in political and social scenario, has supported an increasing use of the Internet and other information and communication technologies. All this has raised a whole range of questions relating to privacy and the protection of personal data and finance. There are questions concerning data protection principles, use of personal data in the police sector, and the investigation of cybercrime. Many issues related to data retention, increasing trend towards authentication of ICT (Information and communication technology) users, relationship between service providers and law enforcement and others have also come up. Countries that are involved in developing cyber crime legislation must have the knowledge of relevant privacy and data protection issues. We witness an emerging adaptation of "conventional" crime to cyber crime

because the phenomena of the digitization, convergence of technologies and globalization of ICT. Old and traditional methods of investigations fail to meet the demands of these changes; so some special procedures are required to be developed for such crimes.

The question is what measures governments and police authorities can take to overcome, control and manage this development in a way so that the present privacy rights are preserved. It has to be seen that to what extent are authorities have freedom to use a data which is and decide about the sources from where it can be taken. Data is publically available data from the Internet and other public sources, but much of the data acquired for carrying out public tasks, is available in databases maintained by government. A major concern is if criminal investigators are allowed to use the data in the same way other governmental authorities use these sources.

Due to the international nature of crimes, international co-ordinate investigations and the use of personal data must be made possible, but with a sharp vigil has to be kept on their limitations in the interest of human rights, especially the protection of the privacy of individuals and consider the evolution of availability of data.

The key questions that crop up here are:

- How can the conflict between privacy protection and criminal investigation be regulated at the levels that are acceptable and
- What changes to the present regulatory framework are required?

LEGAL FRAME WORK FOR CYBER CRIME IN INDIA:

The Information Technology Act 2000 also known as ITA-2000, or the IT Act, is an Act of the Indian Parliament (No 21 of 2000) notified on October 17, 2000.

The United Nations General Assembly by resolution A/RES/51/162, dated the 30 January 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce. Following the UN Resolution India passed the Information Technology Act 2000 in May 2000, which came into force on October 17, 2000. The Information Technology Act 2000 has been substantially amended through the Information Technology (Amendment) Act

2008 which was passed by the two houses of the Indian Parliament on December 23, and 24, 2008. It got the Presidential assent on February 5, 2009 and came into force on October 27, 2009. The amended Act has provided additional focus on information security. It has added several new sections on offences including cyber terrorism and data protection. A set of Rules related to sensitive personal information and reasonable security practices (mentioned in section 43A of the ITAA, 2008) was notified in April 2011. [1]

Provisions in Indian IT Act 2000:

Information technology Act 2000 consisted of 94 sections segregated into 13 chapters. Four schedules form part of the Act. In the 2008 version of the Act, there are 124 sections (excluding 5 sections that have been omitted from the earlier version) and 14 chapters. Schedule I and II have been replaced. Schedules III and IV are deleted.

Information Technology Act 2000 addressed the following issues:

1. Legal recognition of electronic documents
2. Legal Recognition of digital signatures
3. Offenses and contraventions
4. Justice dispensation systems for cybercrimes

Cyber law- The term Cyber law describes the legal issues concerned with the use of communications technology, particularly "cyberspace", i.e. the Internet. It is not much distinct field of law in the way that property or contract are, as it intersects many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In actual practice, cyber law is an attempt to apply laws designed for the physical world to human activities happening on the Internet. In India Information Technology Act [Amend.] 2008 is known as the Cyber law. It has a separate chapter XI entitled Offences" in which different cyber crimes have been declared as penal offences that are punishable with imprisonment and fine.

CYBER CRIME AND TYPES OF CYBER CRIME IN INDIA:

Activities done with a criminal intention in cyber space is called Cyber Crime. These can be of three categories

- Those against individuals.
- Against Business and Non-business organizations.
- Crime against government.

Let us have a look at the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves changing the face of a conventional crime by using computer. Some examples are: [3]

1. Financial Claims
2. Cyber Pornography
3. Sale of illegal articles
4. Online gambling
5. Intellectual Property Crimes
6. E-Mail spoofing
7. Forgery
8. Cyber Defamation
9. Cyber Stalking
10. Hacking
11. Unauthorized access to computer system or network
12. Stealing information contained in electronic from
13. E-Mail bombing
14. Data diddling
15. Salami attacks
16. Denial of Service
17. Virus & worm
18. Logic bombs
19. Trojan horse
20. Internet Time Theft
21. Physically damaging a computer system. [3]

AIMS AND OBJECTIVES OF THE RESEARCH WORK:

The method adopted for this research is known as doctrinal method. Bare Act, books, websites, cases, articles and journals have been consulted for conducting the research which are attained from Library and resources from the World Wide Web.

Objectives of this research work are:-

To raise awareness about the risks, vulnerabilities and protection requirements, especially for new technologies

- To provide the latest methods for investigation and prevention
- To evaluate the effectiveness and legal implications of new techniques, legislation, policies, and software that are used to the fight cybercrime
- Develop various solutions by integrating skills from whole range of diverse fields as computer science, criminal justice and law

HYPOTHESIS AND LIMITATIONS:

A good model of cybercrime investigations is important, as it is instrumental in providing an abstract reference framework, independent of any particular technology or organizational environment, for the discussion of techniques and technology for supporting the work of investigators. It can provide a basis for common terminology to support discussion and sharing of skills. The model can be used to help develop and apply methodologies to new emerging technologies and become the area of investigations. Furthermore, the model can be used in a proactive way to recognize opportunities useful for the development and implementation of technology to assist the investigators in their work, and to provide an infrastructure for the capturing and analysis of requirements for investigative tools, specifically for advanced automated analytical tools. At present, there is a shortage of general models that particularly target at cybercrime investigations. The available models only focus on part of the investigative process (only dealing with collecting, analyzing and presenting evidence) but a complete and general model must include other aspects so that it becomes comprehensive.

Such a model is helpful not just in enforcement of law. It can also prove advantageous for IT managers, security practitioners, and auditors. These people are increasingly in the position of having to carry out investigations because of the rising incidence not only of cybercrime, but of breaches of the policies and guidelines of company (e.g. the abuse of Internet connections in the workplace).

This paper brings an extended model of cybercrime investigations which shows the activities during the investigative process and the major information flows in that process, an important aspect of developing supporting tools. Present models from the literature are elaborated and compared to the new model. Notice that the model that is described here is wider than those dealing only with processing of digital evidence; this model tries to explain the entire cybercrime investigative process to the maximum extent including the digital evidence processing activities.

Existing Models- There are many models for investigation in the literature. Brief explanations of the most important ones are given below. These models mainly restrict themselves to the investigation of the crime scene and the evidence, and so are less extensive in their scope than the model to be described afterwards.

Lee's Model of Scientific Crime Scene Investigation Lee has brought forward the scientific crime scene investigation as a process. His model deals only with investigation of crime scene, not with the full investigative process. Four steps have been identified within the process.

1. Recognition
2. Identification
3. Individualization
4. Reconstruction

This model stresses that the investigation of a crime scene must be systematic and methodical. It is mainly targeted at investigations using physical evidence, but it will be seen below that many sides of it reflect in forensic examination of electronic scenes. The major shortcoming of this

model is that it points out only the forensic part of an investigation and issues such as the exchange of information with other investigators are not brought about. [16]

The Proposed Model- Given that a number of models already exist, so let us see that what can be the motivation for presenting yet another one. The present models do not cover each and every side of cybercrime investigation; they concentrate mainly on the processing of digital evidence. Although useful, they are not general enough to describe fully the investigative process in a way which will help in developing new investigative tools and techniques. A comprehensive model can provide a common reference framework for discussion and for the development of terminology. It can be useful in the development of tools, techniques, training and the certification/accreditation of investigators and tools. It can also give a unified basis for case studies/lessons learned materials to be shared among investigators, and for developing standards, conformance testing, and investigative best practices.

The largest chasm in the presently existing models is that they are unable to explicitly identify the information flows in investigations. For example, Reith et al. (2002) themselves have noted the absence of any explicit mention of the chain of custody in their model. This is a major anomaly when one considers the different laws, practices, languages, and so on which must be handled in a correct manner within real investigations. It is important to recognize and explain these information flows so that protection and technological support can be brought out for them. For instance by using trusted public key infrastructures and time stamping to recognize investigators and authenticate evidence.

Another concern with the existing models is that they have tended to focus on the middle part of the process of investigation, i.e. the collection and examination of the evidence. However, the beginning and later stages must be taken into consideration if a comprehensive model is to be brought forth, and in particular if all the relevant information flows through an investigation are to be identified.

The proposed model is shown in Figure below: -

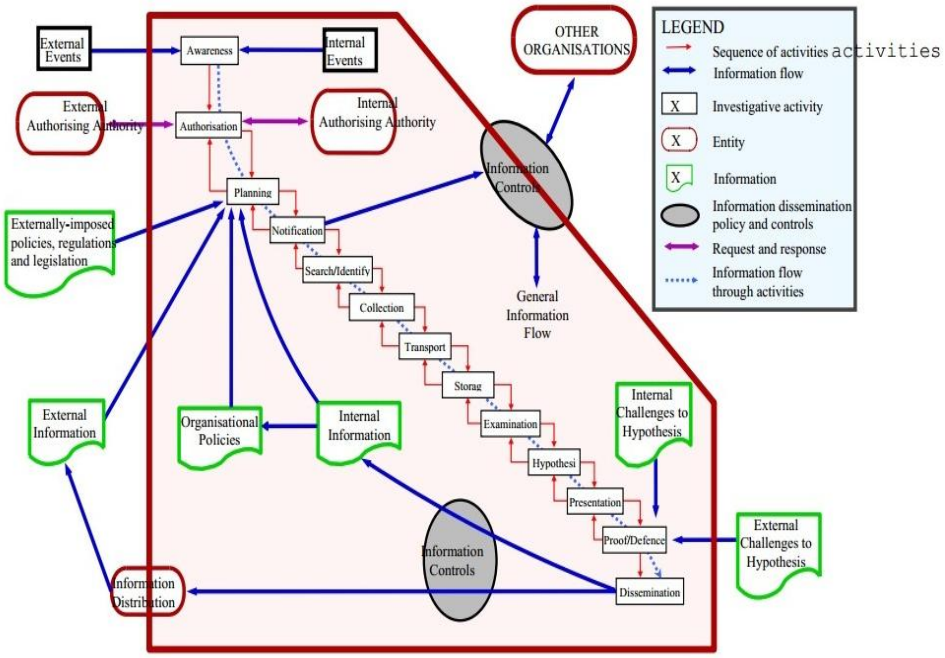

Figure 1. The proposed model of cybercrime investigations.

.

The activities in an investigation

1. Awareness
2. Authorization
3. Planning
4. Notification
5. Search for and identify evidence
6. Collection of evidence
7. Transport of evidence
8. Storage of evidence
9. Examination of evidence
10. Hypothesis

11. Presentation of hypothesis
12. Proof/Defense of hypothesis
13. Dissemination of information

FINDINGS IN RESEARCH:

In cyberspace, bytes replace bullets when there is cyber crime. Concluding from the above study, the cases which are high in number are hacking and obscene publication under IT act 2000 and under IPC cases are many cases of forgery. Hacking is the thing which we need more focus because most of data requires security. Next work will focus on the solutions of preventing data from unauthorized attacks.

Internet was developed for improved communication and research. As the technology advanced of technology and as there is expansion of internet every area, it is not only easier to access but it also provides a pathway to commit illegal acts easily without much effort only by sitting on a system.

Some have minds that are of criminal nature, they tend to use internet as an instrument of crime which is now known as cyber crime committed in cyber space. Cyber crime is now a major issue in all the countries to handle because most of data these days is being transferred online even governmental data also. This Cyber crime denotes to describe any criminal activity in which computer or computer network are taken as tool or target of criminal activity meant to deny service attack. Conventional crime is also included in it where computers are used. Cyber crime mainly consists of unauthorized access to Data and data alteration, data destruction, theft of funds or intellectual property. Due to these online criminal activities cyberspace has become the most unsafe place to do any business. Word cyber space was first used by William Gibson, in his book, Necromancer, written in 1984. Cyberspace can be used to describe a virtual world of computers where there is involvement of internet, where there is an interaction of individuals, businesses are conducted, transactions are done, and graphics are developed.

CONCLUSION:

The ICT Trends of India 2013 show that India has been unsuccessful in enacting a strong and stringent Cyber Law in India. On the contrary, the Information Technology Act 2008 (IT Act 2008) has made India a safe haven for cyber criminals, say cyber law experts of India. The problem seems to be multi- faceted in nature. Firstly, the cyber law of India contained in the IT Act, 2000 is highly deficient in many aspects. Thus, there is an absence of proper legal enablement of ICT systems in India. Secondly, there is a shortage of cyber law training to the police, lawyers, judges, etc in India. Thirdly, capabilities showing cyber security and cyber forensics are not found in India. Fourthly, the ICT strategies and policies of India are lacking and require an urgent overhauling. Fifthly, the Government of India has not been bothered about the ICT reforms in India. This results in a fall in ranking of India in the areas of e-readiness, e-governance, etc. While International communities like European Union, ITU, NATO, Department of Homeland Security, etc emphasize on an enhanced cyber security and tougher cyber laws, India seems to be moving on the wrong side of weaker regulatory and legal regime. Praveen Dalal, Managing Partner of Perry4Law and the leading Techno-Legal Expert of India sent an open letter to the Government of India including the Prime Minister of India,

'President of India, Supreme Court of India, Ministry of Parliamentary Affairs, etc and brought to their attention the growing menace of cyber crimes in India. At last, somebody in the government has shown some concern regarding the growing menace of cyber crimes in India. However, the task is difficult since we do not have trained lawyers, judges and police officers in India in respect of Cybercrimes. However, at least a step has been taken in the right direction by the law minister of India'.

Police in India are trying to become cyber crime savvy and are recruiting people who are trained in this area. The speed of the investigation however can be faster, judicial sensitivity and knowledge has to improve. Focus has to be made on educating the Police and district judiciary. IT Institutions can also play an integral role in this area. We need to sensitize our lawyers and judges towards the trends of the system. Since the law enforcement agencies find it comfortable

to handle the cases under IPC, IT Act cases are not getting reported and when reported are not handled with under the IT Act. A lengthy and an intensive process of learning is required.

A whole new range of initiatives of cyber forensics were initiated and cyber law procedures resulted out of it. This is an area where one has to learn every day since we all are aliens in this area. We need to be looking for solutions faster than the problems. We have to move faster than the criminals. The real concern is finding the ways to prevent cyber crime. The challenges in cyber crime cases include finding evidence that is expected to stand scrutiny in a foreign court.

For this India should get cooperation internationally with specialized agencies of different countries. Police has to make certain that they have captured exactly what was there at the scene of crime and the same should be analyzed and reported in the court based on this evidence. It has to maintain the chain of custody. The danger is not from the intelligence of criminals but from our ignorance of common man and security agencies and the willingness to fight against it.

Criminal Justice systems all over the world, must also remember that because of certain built in difficulties in the recognition of the real cyber criminal, cyber law must be applied so as to distinguish between the innocent and the deviant. A limit has to be exercised on the general tendency to follow the principle of deterrence as a response to increasing rate cyber crime, without being sensitive to the rights of those who are accused. Our law makers and the criminal law system must remember the basic difference between an accused and a convict. There is only a marginal difference between the requirement to ensure that no innocent is punished and the need to punish the cyber criminal.

Thus lastly, there were two research questions which were raised by the researcher for the purpose of the project. The first one is the effectiveness of Information Technology Act, 2000 and if it is efficient enough for controlling the recent developments in Cyber Crimes in India. The Hypothesis for the question was „No" and it has been proved.

The second research question was, if the recent proposed amendment to the Information Technology Act, 2000 would be an answer the contemporary complications in the cyber crime arena in India. The hypothesis for the same was „No" and to conclude the researcher has proved it.

References

<http://en.wikipedia.org/wiki/Information_Technology_Act_2000>

<www.cyberlawsindia.net/lawyering.html>

<www.cyberlawclinic.org/cybercrime.htm>

<Book Securing Information and communication system>

<https://utica.edu/academic/institutes/ecii/publications/articles/>

<https://groups.yahoo.com/neo/groups/soel07/conversations/topics/21>

<http://whizkids007.blogspot.in/2009/10/cyber-stalking.html>

<Times of India, "Now, a phishing email in the name of RBI", 14 May14, 2013>

<The Hindu, "a new squatting case registered under ACPA", February 13th, 2013>

<http://ijecs.in/issue/v2-i8/41%20ijecs>

<http://www.supremecourtofindia.nic.in/scr/2011_v1_pii.pdf>

<http://www.ncrb.gov.in>

<http://articles.economictimes.indiatimes.com/2012-12-07/news/35670501_1_cyber-crimes-crime-data-ncrb>

<http://exclusivetechnologyconsulting.com/ITSecurity.html>