International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

Cyber Crimes in India: An Overview

Parvinder
Research Scholar, Faculty of Law, MDU, Rohtak

ABSTRACT
Every crime has its impact specifically on society, nation and the world to the great extent. By the surveillance of cybercrime and its phenomenon it is exposed that similar to former crimes it has badly affected social life of humans. To understand the influence of cybercrime, it is necessary to look into the impact of two things computer technology and internet on people as cybercrime is no doubt originating out of these. There are inherent challenges to the field of IT security and services through individuals and critical infrastructure. Socially, people are now more open to communicate and interrelate with others compared to past which widen the objectives from the personal relations to the professional ones. Today, there is no single reason for the people to interact through internet but thousands. The advantage behind this mediator is its collaborating and speedy communication which is lacked in other medium of communications.
Keywords: IT act, IPC, Cybercrimes, Internet users.

INTRODUCTION

The present study has been undertaken to touch some aspects, effect and prospects of this cyber technology with special reference to threat poses of Cyber crime by India. Efforts have been made to analyze legal framework available for its control in India. To start with, it is, therefore, necessary to demarcate the dimensions of word 'crime'. Thus it is beyond doubt that 'crime' is a relative phenomenon, universal in nature and essentially all societies from ancient to modern have been evidently demonstrating its presence. Each society have been providing its own description of criminal behavior and conduct made punishable by express will of the political community ruling over the society and it was always influence by religious-social-political economical values prevailing in the given society. Thus from time immemorial the behavior that attracts 'penal liability' influenced and characterized by overall outcome of these standards. Parenthetically, just as concept of crime [has undergone] change with the growth of Information Technology so the categories of criminals who engage in such crimes. So far Indian society is concerned, particularly during ancient period, the definition of crime flagged by religious interpretation. The period was known for complete ominance of religion. All political and social activities in general and 'Crime' in particular, considered to be happened due to the presence of super-natural power. The Demonological theory of crime causation was an outcome of this period.

Medieval period had evidenced the eras of renaissance and restoration, which delivered new, and a fresh look to 'crime'. The concepts like utilitarian, positive approach, analytical thinking, principles of natural justice, and thoughts of lessie faire, hedonistic philosophy, and pain and pleasure theory were outcome of this period which helped to open new horizons for the study of crime. Latter period paved the way for scientific & industrial revolution and rational way of interpretation dominated the thinking.

WHAT IS CYBER CRIME

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are

used to enable the illicit activity. The Cyber crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds.[1]

TYPES OF CYBER CRIME

Some major types of the cyber crime are followed as under:

Email spoofing: This technique is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source. These tactics are usually used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.[2]

Spamming: Email spam which is otherwise called as junk email. It is unsought mass message sent through email. The uses of spam have become popular in the mid 1990s and it is a problem faced by most email users now a days. Recipient's email addresses are obtained by spam bots, which are automated programs that crawls the internet in search of email addresses. The spammers use spam bots to create email distribution lists. With the expectation of receiving a few number of respond a spammer typically sends an email to millions of email addresses.

Cyber defamation: Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space.[3] The purpose of making defamatory statement is to bring down the reputation of the individual.

IRC Crime (Internet Relay Chat): IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other.

- Cyber Criminals basically uses it for meeting.
- Hacker uses it for discussing their techniques.
- Paedophiles use it to allure small children.

A few reasons behind IRC Crime:

- Chat to win ones confidence and later starts to harass sexually, and then blackmail people for ransom, and if the victim denied paying the amount, criminal starts threatening to upload victim's nude photographs or video on the internet.
- A few are paedophiles, they harass children for their own benefits.
- A few uses IRC by offering fake jobs and sometime fake lottery and earns money.[4]

Phishing: In this type of crimes or fraud the attackers tries to gain information such as login information or account's information by masquerading as a reputable individual or entity in various communication channels or in email.

CYBER LAWS IN INDIA

In INDIA information technology act 2000 deals with the cybercrime activities /problems. It act 2000 has both positive and negative aspects as well. Therefore amendment is done in Rajya Sabha on Dec 23rd of 2008.this act was renamed as information technology(Amendment) act 2008 and referred as ITAA 2008.

[1] Sumanjit Das And Tapaswini Nayak, Impact Of Cyber Crime: Issues And Challenges, International Journal Of Engineering Sciences & Emerging Technologies, October 2013.
[2] http:/researchsecurity.techtarget.com
[3] www.helplinelaw.com
[4] www.ccasociaty.com

CONCLUSION

Roots of cybercrime are lies in technology and critical infrastructure. Number of internet users is continuously increasing and with this growth risk of several types of crimes is also amplified. Cybercrimes are varying in its nature due to enhancement in technologies. Despite the fact that there is no agreed definition of the cybercrime, cybercrime is unavoidable. Few classifications of such crimes may look like the traditional crimes however many of them are recognized as different kinds of crime and to be handled in a different way. Technology-based crimes have been developing with the passage of every day and they need to be solved with utmost priority. These crimes never restricted to computers but other electronic devices are made like financial transaction machines, tale-communication equipments etc. Due to diversified nature it is difficult to identify the cyber security problems which lead to unawareness on security issues. The proliferation in registering the cybercrimes under various sections of IT act and IPC shows the severity of such cyber threats however most of the cases were still unreported because of various reasons. Considering this scenario security and awareness training model towards public security will be developed in preliminary phase. In next phase of the research a tool will be designed with the implementation of multilayer security algorithm.

REFERENCES

1. Cybercrime system requirements in India: Most necessary thing in India, [Online], Available: http://www.cyberlawsindia.net/requires.html
2. A comparative analysis of cybersecurity initiatives worldwide, international telecommunication union, Geneva, 28 June -1 July 2005.
3. IT Infrastructure in India, [Online], Available: http://business.mapsofindia.com/
4. Industry & Sectors, [Online], Available: http://indiainbusiness.nic.in
5. Lum Wai Seng, Dave Junia, Berenice Wong, Yeo Kai Zhen, Mabel, Tan Chien Ying, Jolin, Woo Nicholas. (2012) 'Responsibility of National Security and the Indian Government: A Case Study on Cyber Terrorism in India', National University of Singapore.
6. e-Infrastructure, [Online], Available: http://deity.gov.in
7. Pillai, (2008). 'Govt. framing norms for social infrastructure in SEZs', The Economic Times, [Online], Available: http://articles.economictimes.indiatimes.com
8. Sanjay K Singh, 'Information Technology in India: Present Status and Future Prospects for Economic Development'