IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Issues and Challenges of Cyber Crime in India: An Ethical Perspective

Gobinda Bhattacharjee
Lecturer, Dept. of Philosophy,
Rabindranath Thakur Mahavidyalaya, Bishalgarh, Tripura, INDIA

Abstract

The present paper is an attempt to discuss issues and challenges of Cyber Crime in India from an ethical perspective. Ethics is a branch of philosophy which deals with what is considered to be right or wrong. The ethics centers and program devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. Cyber crime is emerging as a serious threat. Computer Technology is one of the important general purpose Technologies in today's age for several reasons. Today it is used in almost all the organizations, institutions, and people. Computer technology makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber crime'. The advancement of IT brings so many facilities to us; but also brings so many problems and challenges too and out of which Cyber Crime is a kind of offence which deals with the cyber world which includes computer security, information security, and mobile security too. The increasing number of crimes in the field of Information Technology brings a big attraction to Cyber Crime to everyone.

***Keywords**: Ethics, Cyber Crime, Issues and Challenges in India, Computer Security*

1. Introduction

Ethics is a branch of philosophy which deals with what is considered to be right or wrong. The ethics centers and program devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. Cyber crime is emerging as a serious threat. Cyber crime 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.

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

2. Objective

The main aim and objective of this study includes but not limited to as follows:

- To know basic about Cyber Crime and its characteristics;
- To know basic about the challenges and facet of Cyber Crime;
- To learn basic about the issues related to Cyber Crime briefly;
- To know basic about the Cyber Crime related act in the Indian context.

3. Classification of Cyber Crime

Data Interception: An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream.

Data Modification: Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it.

Data Theft: Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate

Network Crime: Network interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data. Network Sabotage 'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of. It could be the above alone, or a combination of things. But if Verizon is using the help the children, hindering first responders line then they might be using network problems as an excuse to get the federal government to intervene in the interest of public safety. Of course if the federal government forces these people back to work what is the purpose of unions and strikes anyway.

Access Crime: Unauthorized Access "Unauthorized Access" is an insider‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality. Virus Dissemination Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.

4. Reasons behind the Cyber Crime

There are many reasons why cyber-criminals are doing cyber-crime; chief among them are mentioned below:

- For the sake of recognition.
- For the sake of quick money.
- To fight a cause one thinks he believes in.
- Low marginal cost of online activity due to global reach.
- Catching by law and enforcement agency is less effective and more expensive.
- New opportunity to do legal acts using technical architecture.
- No concrete regulatory measure.
- Lack of reporting and standards
- Difficulty in identification
- Limited media coverage.
- Corporate cyber crimes are done collectively and not by individual persons.

5. Challenges of Cyber Crime

Endless discussion is there regarding the pros and cons of cyber crime. There are many challenges in front of us to fight against the cyber crime. Some of them here are discussed below:

- Lack of awareness and the culture of cyber security, at individual as well as organizational level.
- Lack of trained and qualified manpower to implement the counter measures.
- No e-mail account policy especially for the defense forces, police and the security agency personnel.
- Cyber attacks have come not only from terrorists but also from neighboring countries contrary to our National interests.
- The minimum necessary eligibility to join the police doesn’t include any knowledge of computers sector so that they are almost illiterate to cyber-crime.
- The speed of cyber technology changes always beats the progress of govt. sector so that they are not able to identify the origin of these cyber-crimes.
- Promotion of Research & Development in ICTs is not up to the mark.
- Security forces and Law enforcement personnel are not equipped to address high-tech crimes.
- Present protocols are not self sufficient, which identifies the investigative responsibility for crimes that stretch internationally.
- Budgets for security purpose by the government especially for the training of law enforcement, security personnel’s and investigators in ICT are less as compare to other crimes.

6. Way to Reduce Cyber Crime

There are so many actions available to reducing Cyber Crime and cyber offence and out of which followings are important such as

Legal Action: as far as legal action is concerned, the following actions may be helpful to reduce Cyber Crime and important to take into

- Electronic Communications Privacy Act of 1986.
- Federal Privacy Act of 1974.
- Indian IT Act.
- Communications Act of 1934 updated 1996.
- Computer Fraud and Abuse Act of 1984.
- Computer Security Act of 1996.
- Economic Espionage Act of 1996.
- Health Insurance Portability and Accountability Act of 1996.
- Personal Data Privacy and Security Act of 2007.
- Data Accountability and Trust Act.

- Identify Theft Prevention Act.
- Data security Act of 2007

Awareness Building: Awareness building is most important to reduce Cyber Crime and IT crime; thus following things are essential to follow

- Creating changes in the password of the computing devices such as computers, search and networking systems, changes of the password of other services such as email, social networking site, and other service based site registered by the applicant or user.
- Reduction in use of email in cyber café and other places and computing devices.
- Open and communicating with the unknown computer and similar device.

Technological Backup:

- Use of Anti Virus software and system in the computer system or when network or telecommunication Systems.
- Use of internet safety tools, appropriate time and as per machine requirement.
- Use of Good firewall and sophisticated Network Designing.
- Keep off the Blue tooth and other RF devices.

7. Findings

- IT Crime and Electronic Crime are synonymous with Cyber Crime and using rapidly for breaking foolproof systems.
- Still, many people are not aware of the strategy to use „switch off‟ Cyber Crime.
- Cyber Crime is increasing both in manual form and as well as online form.
- Today Cyber Crime includes apart from the computer and such devices are TV, ATM, Mobile Phone, I-Pod and so on.

8. Conclusion

IT is one of the important and helpful tools nowadays. The new world of information society with global networks and cyberspace will inevitably generate a wide variety of social, political, and ethical problems. Many problems related to human relationships and the communities become apparent, when most human activities are carried on in cyberspace. Some basic ethical issues on the use of IT on global networks consist of personal privacy, data access rights, and harmful actions on the Internet. Though it has so many problems and drawbacks in many classes out of which Cyber Crime is most important and on the other hand, E-Crime and its world emerging. Reduction in Cyber Crime is only possible when user will be much more aware of the aspects of Cyber Crime and when they enrich their knowledge towards a reduction in cyber and electronic crime. The advancement of IT brings so many facilities to us; but also brings so many problems and challenges too and out of which Cyber Crime is a kind of offence which deals with the cyber world which includes computer security, information security, and mobile security too. The increasing number of crimes in the field of Information Technology brings a big attraction to Cyber Crime to everyone.

Ethical standards also include those that enjoin virtues of honesty, compassion, and loyalty. And, ethical standards include standards relating to rights, such as the right to life, the right to freedom from injury, the right to choose, the right to privacy, and right to freedom of speech and expression. Such standards are adequate standards of ethics because they are supported by consistent and well-founded reasons. Ethics refers to the study and development of personal ethical standards, as well as community ethics, in terms of behavior, feelings, laws, and social habits and norms which can deviate from more universal ethical standards.

References

- ACM, 1992, ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, USA, October 1992.
- Kubo, Takeaki, 1999, Internet Revolution & Japanese IT Industry, Symposium on Development of Information Industry in the Asia-Pacific Region, 5-8 October 1999, Srilanka, page 21-93.
- Martin, S.B. (1998). Information technology, employment, and the information sector: Trends in information employment 1970–1995. Journal of the American Society for Information Science, 49(12), 1053–1069.
- Saracevic, T. (1996). Relevance reconsidered. Information science: Integration in perspectives. In Proceedings of the Second Conference on Conceptions of Library and Information Science (pp. 201– 218), Copenhagen, Denmark: Royal School of Library and Information Science.
- Saracevic, T. (1975). Relevance: A review of and a framework for the thinking on the notion in information science. Journal of the American Society of Information Science, 26(6), 321–343.
- Stephan, Karl D, 2002, Is Engineering Ethics Optional?, IEEE Technology and Society, Volume 20, Number 4, page 6-12.