ORIGINAL RESEARCH PAPER

Law

CYBER CRIMES IN INDIA

KEY WORDS:

Dr. R. M. Dave

Head, Department of Human Rights and International Humanitarian Laws
Saurashtra University, Rajkot, Gujarat

The era of modernization where the working without internet almost handicaps the core functioning at every level. Cyber space also played necessary role in easy & better functioning of trade & commerce to the society. The concept of cyber crimes is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counter balanced by the sanction of the state.Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment." The hallmark of criminality is that, it is breach of the criminal law.Per Lord Akin "the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences". A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

Cyber Crime

Cyber Crimes are one of the fastest growing crimes in the world. It is noteworthy that first cyber crime took place in the year of 1820. It has gained momentum in India in the recent past. In the present era, whereas internet has gained important role in effective functioning of trade & commerce, it suffice basic as well as necessary requirements to Industrial units MNCs etc., also providing Modern Banking System. But theirs a class of people who misuses the same for their personal interest, and hampers the very objective of Cyber space as boon to the society. Thus in India Information Technology Act,2000 (IT act 2000) takes into consideration of such offences, but at certain instances it fails due to loop holes of law.

Reasons for increasing cases of cyber crimes

Professor HLA Hart in his work "The concept of law" has said "human beings are vulnerable so rule of law is required to protect them". Applying this to the cyber space we may say that computers are vulnerable so rule of law is required to protect them and safeguard them against the cyber crimes. The reason for the vulnerability of computer may be said to be:

(1) Capacity to store data in comparatively small space:

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it easier.

(2) Easy to access:

The problem encountered in guarding a computer system from the unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bombs, key loggers that can steal access codes, advanced voice recognition, retina images etc. that can fool biometric system and bypass firewalls can be utilized to get pas many a security system.

(3) Complex:

The computer work on operating systems and this operating system in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be lapse at any stage. The cyber criminal take advantage of these lacunas and penetrate into the computer system.

(4) Negligence:

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

(5) Loss of evidence:

Loss of evidence is a very common and obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

Who are Cyber Criminals?

The cyber criminals constitute of various groups / categories. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals.

(1) Children and adolescents between the age group of 6 - 18 years:

The simple reason for this type of delinquent behavioral pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reason may be psychological even.

(2) (a)Hackers:

These kinds of hackers are mostly organized together to fulfill certain objectives. The reason may be to fulfill their potential bias, fundamentalism etc. The Pakistanis are said to be one of the organized hackers in the world. They mainly target the Indian government sites with the purpose to fulfill their political objectives.

(b) Professional hackers / crackers:

Their work is motivated by the color of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

(3) Discontented employees:

This group includes those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employer.

Safeguards for using Internet and other technologies for preventing himself from victim of cybercrime are given as under:

(1) It's a good idea to always be vigilant when sharing personal information over the Internet. It's important to make sure you only share minimal, if any, personal information with people you do not know. Be conscientious of what information share even if you think you are being careful. Often criminals will talk with their victims for long periods of time, piecing together bits of personal information until they have a complete profile. People you associate with or meet online may not appear to be who they say they are, after all one never knows who is really sitting at the other end of a network connection.

(2) Do not ever enter passwords or personal information on links you received in email since emails can be spoofed and/or used to "phish" for information.
(3) By educating yourself on current illegal trends, you can better understand ways you can reduce the risk of becoming a target. Awareness is the strongest weapon you can obtain to protect yourself against cyber crime.
(4) It's also important you invest in installation of anti-virus, spy-ware and firewall software. There are many programs available that you can download for free, or you can purchase a proprietary one.
(5) To prevent cyber stalking avoid disclosing any information pertaining to oneself.
(6) Always use latest and update anti-virus software to guard against virus attacks.
(7) Another tip is to read privacy policies of any online entity you conduct business with. Be aware of what is done with your personal information once you do share it with a company.
(8) Always keep backup volumes so that one may not suffer data lose in case of virus contamination.

CONCLUSION

Thus it will be fair enough to say that, the efforts made by Indian government are not sufficient enough to curtail the rate of Cyber crime in India in cases of extraterritorial jurisdiction. Though it has provided with the provision to deal beyond the territorial limits but it has not given any framework for its execution. Unless there are concrete steps towards international co-operation in combating terrorism, it is not possible to deal with acts committed on internet by aliens. Thus it will be correct to say that such provisions are not effective and stand forth on paper has no role to play in legal regime.to curb cyber crimes, one is required to understand then in the perspective of technologies advancement and the ease with which they can be committed. The old adage of "AN EYE FOR AN EYE" would be equally applicable to reduce computer crimes. It should be "TECHNOLOGY FOR TECHNOLOGY". If one is committing a crime by using technology, one will be blocked to do so by employing technology. Law can merely supplant but cannot supplement the effort of determining of cyber criminal.

REFERENCES:

1. An introduction to Cyber Laws- Dr. R.K Chaubey
2. SV Joga Rao, Law of Cyber Crime & Information Technology law, Wadhva& co, Nagpur, First Edition 2004.
3. Guide to Cyber Laws- Rodney O. Ryder
4. N.C. Jain, Cyber Crime, Allahbad Law Agency, First Edition 2008.
5. Symantec Security Response- by Sarah Gordon
6. Dr. Marco Gercke, Lecturer at the University of Cologne, Germany, Expert for the Council of Europe- Cyber Terrorism
7. The Time of Indiawebsite-accessing-information-technology" target="_blank"> http://articles.timesofindia.indiatimes.com/mumbai/27979238_1_website-accessing-information-technology
8. Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks, Janet J. Prichard and Laurie E. MacDonald, Bryant University, Smithfield, RI, USA
9. SV Joga Rao, Law of Cyber Crime & Information Technology law, Wadhva& co, Nagpur, First Edition 2004
10. Information Technology Act, 2000