Vandana Publications
IJEMR

Volume-7, Issue-2, March-April 2017
International Journal of Engineering and Management Research
Page Number: 48-51

Cyber Crimes Becoming Threat to Cyber Security

Dr. Latika Kharb

ABSTRACT

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the internet, cyber space and the worldwide web. The growing danger from crimes committed against computers, or against information on computers by persons involved in the profession of crimes, has become a major issue in India. For an effective application, the existing laws must be constantly reviewed and modified accordingly to face the challenges coming from the cyber world. In this paper, we've discussed the cyber crimes as one of the challenges for cyber laws and it also discussed about the cyber crimes that have continued to grow as one of the threats to the users of the cyber society. We've also discussed the laws in cyber space and their need along with the IT Act-2000. Some more viewpoints presented in the paper include: the legal drawbacks with regards to cyber crimes being solved in India, and the need for new legalizations. The main emphasis of the paper revolves around the challenges faced by cyber laws in regulating cyber crimes.

Keywords**—** Cyber crimes, cyber laws, cyber society, IT Act-2000

I. INTRODUCTION

The rapid change occurring in the present era of information technology includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element. Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and different activities [1]. Cyber laws help in maintaining a trustworthy environment for cyber society by applying rules of law in criminal investigations. Cyber crime is a criminal activity committed on the internet and is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money. Cyber laws are meant to set some rules and guidelines that make the cyber activities legalized. One of the major challenges laws have been facing has been in the cyber space crimes as cyber technology changes have been so rapid that it has become a difficult issue for law enforcement agencies to keep up with this rapid change.

II. CYBERCRIMES IN CYBER SPACE

The growing danger from crimes committed against computers, or against information on computers, has become a major issue in the India. Cyber crime is a broad term that describes everything from electronic cracking to denial of service attacks that cause e-commerce sites to lose money. The Encyclopedia Britannica defines cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology [2]. Cyber crimes are harmful acts committed from or against a computer or network. Some other cyber crimes include:

- Using one's own programming abilities as also various programs with malicious intent to gain unauthorized access to a computer or network are very serious crimes.
- Creation and dissemination of harmful computer program which do irreparable damage to computer systems is another kind of cyber crime.
- Software piracy is also another distinct kind of cyber crime in which many people online distribute illegal and unauthorized pirated copies of software.

Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the IT Act 2000. Cyber crimes in the cyber society can be basically divided into 3 major categories [3]:

2.1. Cyber crime against Persons
2.2. Cyber Crimes against Property
2.3. Cyber Crimes against Government

2.1. Cyber crime against Persons

Cyber crimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer like email. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important cyber crimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one cyber crime which threatens the growth of the younger generation. Harassment can be sexual, racial, religious, or other and persons perpetuating such harassment are also guilty of cyber crimes.

2.2. Cyber Crimes against Property

The second category of cyber-crimes is that of cyber crimes against all forms of property. These crimes include computer vandalism i.e. destruction of others' property, and transmission of harmful program.

2.3. Cyber Crimes against Government

The third category of cyber-crimes relate to cyber crimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the international governments and also to terrorize the citizens of a country. Cyber crime occurs when an individual "cracks" into a government or military maintained website. During the investigation of the Red Fort shootout in Dec. 2000, the accused Ashfaq Ahmed of this terrorist group revealed that the militants are making extensive use of the internet to communicate with the operatives and the sympathizers and also using the medium for intra-bank transfer of funds" [3].

III. NEED FOR CYBER LAWS AGAINST CYBER CRIME

It is common that many systems operators do not share information when they are victimized by crackers. They don't contact law enforcement officers when their computer systems are invaded, instead prefer to fix the damage and take action to keep crackers from gaining access again. Computer crime poses a real threat and as the cases of cyber crime grow, there is a growing need to prevent them. Cyberspace belongs to everyone; so there should be some kind of electronic surveillance i.e. investigators to track down/ monitor the hacker/cracker as he breaks into a victim's computer system. The basic laws governing real-time electronic surveillance in criminal investigations must also apply in this context like the search warrants to be obtained to gain access to the premises where the cracker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime. To overcome the security flaws, we've some suggestions for cyber society [4]:

- Protect your databases and place the database behind a second interface on your firewall, with tight access rules.
- Avoid giving out any information about yourself in a chat room. Children should never arrange face-to-face meetings or send their photographs online.
- Use the latest anti-virus software, operating systems, web browsers and email programs and put in a firewall and develop your content off line. Use a security program that gives you control over cookies that send information back to Web sites.
- Make sure web servers running your public site are physically separate and individually protected from your internal corporate network.
- Send credit card information only to secure sites.
- Back up your web site after every update, so you can re-launch it immediately in case of a malicious defacement.

Internet provides anonymity: this is one of the reasons why criminals try to get away easily when caught and also give them a chance to commit the crime again. Therefore, we users should be careful and if we find anything suspicious in e-mails or if the system is hacked, it should be immediately reported to the police officials who investigate cyber-crimes rather than trying to fix the problem by ourselves.

IV. TECHNOLOGY CHALLENGES IN CYBER CRIME

In the present era of advancements in technology, law enforcement agencies must provide their computer crime investigators with the technology required to conduct complex computer investigations. Besides access to technology, law enforcement agencies must also be given Forensic Computer support as many computer crimes leave "footprints" on the computer as well as on the internet [5]. Most of the prosecutors also lack the specialization to focus on the prosecution of criminals who use computer-based and Internet system as a means of committing crimes. Moreover, the prosecutors must have enough knowledge of computer-based and Internet investigations if they have to handle these crimes effectively. Law enforcement must seek ways to keep the drawbacks from overshadowing the computer age. Cyber crimes have to be tackled effectively not only by the law officials but also by the cyber society by co-operating with the law.

V. THE IT ACT 2000: THE FIRST CYBER LAW

The Parliament of India passed its first Cyber law, the Information Technology Act in 2000 i.e. IT Act-2000. It not only provides the legal infrastructure for E-commerce in India but also at the same time, gives powers to the police to enter and search, without any warrant, any public place for the purpose of nabbing cyber-criminals and preventing cyber crime [7]. The IT Act 2000 gives the legal framework so that information is not denied legal effect, solely on the ground that it is in the form of electronic records. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the IT Act 2000. On the contrary, it has a separate chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine. The offences covered under Chapter XI of the Indian Information Technology Act 2000 include [6]:

(i) Tampering with the computer source code or computer source documents

(ii) Hacking

(iii) Publishing or transmitting any information in the electronic form which is lascivious or which appeals to the prurient interest.

(iv) Failure to decrypt information if it's necessary in the interest of the sovereignty or integrity of India.

(v) Securing access or attempting to secure access to a protected system.

(vi) Mis -Representation while obtaining, any license to act as a Certifying Authority or a digital signature certificate.

(vii) Breach of confidentiality and privacy

(viii) Publication of digital signature certificates which are false in certain particulars

(ix) Publication of digital signature certificates for fraudulent purposes.

VI. DRAWBACKS OF CYBER LAWS AGAINST CYBER CRIMES

Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space. India is the 12th nation in the world that has cyber legislation. The cyber laws of the country could not be regarded as sufficient and secure enough to provide a strong platform to the country's e-commerce industry for which they were meant [7]. However, it is important to note that existing laws do not help in solving cyber crimes efficiently. There are many drawbacks which prevent cyber crimes from being solved in India:

- Most people in India prefer not to report cyber crimes to the law enforcement agencies because they fear it might invite a lot of harassment.
- Awareness of cyber crime is extremely low. Awareness of people about cyber crime is still very low and so we need to take many steps to alert the legal scenario.
- Law enforcement agencies in the country are not well equipped and knowledgeable enough about cyber crime.
- An immense need for training the law enforcement agencies: very few cities have cyber crime cells *viz*. under the IT Act, the relevant officer entitled to investigate a cyber crime is a Deputy Superintendent of Police (DSP), but most of the DSP's are not well equipped to fight cyber crime.
- There is also a lack of dedicated cyber crime courts in the country where expertise in cyber crime can be utilized.
- The Law enforcement agencies have been facing tremendous problems while trying to cope with the challenges of emerging cyber crimes.

VII. IMPROVEMENTS REQUIRED IN CYBER LAWS

The law enforcement agencies have been facing tremendous problems while trying to cope with the challenges of emerging cyber crime within the ambit of the Indian Penal Code [8], even if a liberal interpretation of it is taken. As far as the issue of solving cyber crime goes, the credit lies with the law enforcement agencies. There is a need for some new and distinct laws on cyber crime and appropriate changes should also be made in the Indian Penal Code and the IT Act. However, cyber law is indeed helpful in addressing some cyber crimes but in the areas where the law does not cover cyber crimes which have already emerged, the law is of no assistance or help whatsoever. Moreover, there is a need for dedicated, continuous, updated training of the law enforcement agencies. While Indian laws are well-intentioned, there is a general perception among the population that one can get away with any crime due to various flaws in the execution. It is important to know that existing laws are not well equipped enough to deal with cyber crimes as they do not possess the latest tools. People need to be encouraged to report the matter to the law enforcement agencies with full confidence and trust and without the fear of being harassed. Further, the law enforcement agencies dealing with cyber crime need to come up with an extremely friendly image.

VIII. CONCLUSION

Cyber crime that has become a great threat to the cyber society, has to be tackled efficiently not only by the law officials but also by the cyber society. The IT Act 2000 has developed great assistance to the cyber law prosecutors to put the cyber criminals behind the bars. Being co-operative with the law, the problem could be solved to a great extent i.e. if the law enforcement agencies dealing with cyber crimes have been extremely cooperative with cyber society. To conclude, in order to deal with the problem of cyber crimes along with better legal implementations, a need for some new laws along with a pro-active approach by the law enforcement agencies still exists.

REFERENCES

[1] Latika Kharb, Balwant Rai, Pradeep Tomar, “New Vision of Computer Forensic Science: Need of Cyber Crime Law”, The Internet Journal of Law, Healthcare and Ethics, 2007. Volume 4, Number 2. ISSN: 1528-8250.
[2] Curtis P A., Cowell L. ” Cyber Crime”: “The Next Challenge” in seminar at School of Law Enforcement Supervision in November 12, 2000
[3] Maya Babu, Mysore Grahakara Parishat, ”What Is Cybercrime?”, in Star Of Mysore, Online magazine, October 11, 2004
[4] Gopika Vaidya-Kapoor , “Byte by Byte” in Net Guide, Online magazine, February 18, 2003
[5] National ICT Security and Emergency Response Centre (NISER) “Is Cyber Crime reigning on a no Man’s land”.
[6] www. economictimes.indiatimes.com
[7] Vijayashankar N. “The role of Cyber Laws in E-Governance” Paper presented at the Seminar in Chennai on September 16, 2000
[8] www.cyberlaws.org