Addressing issue of Cyber Crimes in India: An Analysis

Dr. Deevanshu Shrivastava
Assistant Professor (SG)
JLU School Of Law, Jagran Lakecity University,
Bhopal, Madhya Pradesh India

For a warrior, nothing is higher than a war against evil. The warrior confronted with such a war should be pleased, Arjuna, for it comes as an open gate to heaven. But if you do not participate in this battle against evil, you will incur sin, violating your Dharma and your honour.

- Bhagavad-Gita 2.31

The word cyber and its relative dot.com are probably the most commonly used terminologies of the modern era. In the information age the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of trans-national crimes known as “cyber crimes”. Cyber crimes have virtually no boundaries and may affect every country in the world. They may be defined as “any crime with the help of computer and telecommunication technology”, with the purpose of influencing the functioning of computer or the computer systems. The extent of loss involved worldwide of cyber crimes is tremendous as it is estimated that about 500 million people who use the Internet can be affected by the emergence of cyber crimes. Cyber crimes are a very serious threat for the times to come and pose one of the most difficult challenges before the law enforcement machinery. Most cyber crimes do not involve violence but rather greed, pride, or play on some character weakness of the victims. It is difficult to identify the culprit, as the Net can be a vicious web of deceit and can be accessed from any part of the globe. For these reasons, cyber crimes are considered as “white-collar crimes". To understand cyber crime as a significantly new phenomenon, with potentially profoundly new consequences, it is necessary to recognize it as a constituent aspect of the wider political, social and economic reconstructing currently effecting countries worldwide. This new technology not only provides opportunities for the profitable development of an international information market but has also raised the specter of new criminal activities to exploit them. The very technology that enables multinationals to do business more effectively and challenge the individual controls and regulations of nation states, also offers the prospect of globally organized criminal networks. Moreover the free flow of uncensored information on electronic networks and web- sites is as attractive to insurgents and extremist groups as it is to dissidents proclaiming their human rights. Just as crimes have changed with the growth of information technology so have the categories of criminals who engage in such crimes. There are three basic categories of criminals who engage in such crimes, ranging from hackers, information merchants and mercenaries, to terrorists, extremists and deviants.

I. The Vast Range of Cyber Crimes Hacking:

It is the most common type of Cyber crime being committed across the world. Hacking has been defined in section 66 of The Information Technology Act, 2000 as follows "whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking".

Punishment for hacking under the above mentioned section is imprisonment for three years or fine which may extend Upto two lakh rupees or both. A Hacker is a person who breaks in or trespasses a computer system. Hackers are of different types ranging from code hackers to crackers to cyber punks to freaks. Some hackers just enjoy cracking systems and gaining access to them as an ordinary pastime; they do not desire to commit any further crime. Whether this it would constitute a crime is a matter of fact. At most such a crime could be equated with criminal trespass.

II. Security Related Cyber Crimes:

With the growth of the internet, network security has become a major concern. Private confidential information has become available to the public. Confidential information can reside in two states on the network. It can reside on the physical stored media, such as hard drive or memory or it can reside in the transit across the physical network wire in the form of packets. These two information states provide opportunities for attacks from users on the internal network, as well as users on the Internet.

III. Network Packet Sniffers

Network computers communicate serially where large information pieces are broken into smaller ones. The information stream would be broken into smaller pieces even if networks communicated in parallel. These smaller pieces are called network packets. Since these network packets are not encrypted they can be processed and understood by any application that can pick them off the network and process them. A network protocol specifies how packets are identified and labeled which enables a computer to determine whether a packet is intended for it. The specifications for network protocols such as TCP/IP are widely published. A third party can easily interpret the network packets and develop a packet sniffer. A packet sniffer is a software application that uses a network adapter card in a promiscuous mode (a mode in which the network adapter card sends all packets received by the physical network wire to an application for processing) to capture all network packets that are sent !across a local network. A packet sniffer can provide its users with meaningful and often sensitive information such as user account names and passwords.

IV. IP SPOOFING

An IP attack occurs when an attacker outside the network pretends to be a trusted computer either by using an IP address that is within its range or by using an external IP address that you trust and to which you wish to provide access to specified resources on your network. Normally, an IP spoofing attack is limited to the injection of data or commands into an existing stream of data passed between client and server application or a peer to peer network connection.

V. PASSWORD ATTACKS

Password attacks can be implemented using several different methods like the brute force attacks, Trojan horse programmes. IP spoofing can yield user accounts and passwords. Password attacks usually refer to repeated attempts to identify a user password or account. These repeated attempts are called brute force attacks.

VI. DISTRIBUTION OF SENSITIVE INTERNAL INFORMATION TO EXTERNAL SOURCES:

At the core of these security breaches is the distribution of sensitive information to competitors or others who use it to the owners' disadvantage. While an outside intruder can use password and IP spoofing attacks to copy information, an internal user could place sensitive information on an external computer or share a drive on the network with other users

VII. MAN-IN-THE-MIDDLE-ATTACKS

This attack requires that the attacker have access to network packets that come across the networks. The possible use of such attack are theft of information, hijacking an ongoing session to gain access to your internal network resources, traffic analysis to drive information about one's own network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions.

VIII. FRAUD ON THE INTERNET

This is a form of white collar crime. Internet fraud is a common type of crime whose growth has been proportionate to the growth of internet itself. The internet provides companies and individuals with the opportunity of marketing their products on the net. It is easy for people with fraudulent intention to make their messages look real and credible. There are innumerable scams and frauds most of them relating to investment schemes and have been described in detail below as follows:

- **Online investment newsletters**

Many newsletters on the internet provide the investors with free advice recommending stocks where they should invest. Sometimes these recommendations are totally bogus and cause loss to the investors.

- **Bulletin boards**

This is a forum for sharing investor information and often fraud is perpetrated in this zone causing loss of millions who bank on them.

- **E-mail scams**

Since junk mail (E mail which contains useless material) is easy to create, fraudsters often find it easy to spread bogus investment schemes or spread false information about a company.

- **Credit card fraud**

With the electronic commerce rapidly becoming a major force in national economies it offers rich pickings for criminals prepared to undertake fraudulent activities. In U.S.A. the ten most frequent fraud reports involve undelivered and online services; damaged, defective, misrepresented or undelivered merchandise; auction sales; pyramid schemes and multilevel marketing and of the most predominant among them is credit card fraud.

Something like half a billion dollars is lost to consumers in card fraud alone. Publishing of false digital signature .According to section 73 of the I.T. Act 2000, if a person knows that a digital

signature certificate is erroneous in certain particulars and still goes ahead and publishes it, is guilty of having contravened the Act. He is punishable with imprisonment for a term that may extend to two years or with fine of a lakh rupees or with both.

Making available digital signature for fraudulent purpose

This is an offence punishable under section 74 of the above mentioned act, with imprisonment for a term that may extend to two years or with fine of two lakh rupees or with both.

IX. Alteration and Destruction of Digital Information

The corruption and destruction of digital information is the single largest menace facing the world of computers. This is introduced by a human agent with the help of various programmes which have been described in detail below as follows:

Virus Just as a virus can infect the human immunity system there exist programs, which, can destroy or hamper computer systems. A computer virus is a programme designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programmes like word processor or spreadsheets or they attach themselves to the boot sector of a disk. When an infected file is activated or when the computer is started from an infected disk, the virus itself is also executed.

X. Pornography on the Net

The growth of technology has flip side to it causing multiple problems in everyday life. Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly called is widespread. Almost 50% of the web sites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-Roms. The new technology is not merely an extension of the existing forms like text, photographs and images. Apart from still pictures and images, full motion video clips and complete movies are also available. Another great disadvantage with a media like this is its easy availability and accessibility to children who can now log on to pornographic web-sites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present. Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the internet.

The Information and Technology Act 2000 makes the publishing of information which is obscene in electronic form punishable as under:

" Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent Conviction, with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees."

This new law will operate upon anyone who is within its jurisdictional net. Any one within the country or the area of operation of the law who is carrying on a business of cyber porn will be liable under section 67 of the above mentioned Act. Apart from this, a multi-layered governance programme should be ushered in. This will mainly include a mixture of national and international legislations and self imposed regulations by internet service providers and users like parents for their children, hotlines and special organizations to report pornographic content. In this way the balance between the freedom of the individual and the greatest good of the society can be maintained.

XI. Cryptography, Privacy and National Security Concerns:

The Internet has provided its users with a new forum to express their views and concerns on a worldwide platform. As a necessary corollary to the freedom to communicate and speak is the fact that this must be allowed with as little State interference as possible; in other words, in the absence of State intrusion. This immediately raises the controversial issue of the right to privacy. It can be considered a logical corollary to the freedom of speech and expression. At the same time it is common knowledge that liberty cannot thrive without certain restrictions put on them so that each individual in society can be best protected. The practice of encryption and its study which is known as cryptography provides individuals with means of communication that no third party can understand unless specifically permitted by the communicators themselves. It would therefore seem that this practice is a legitimate utilization of the right to freedom of speech and expression and the right to have a private conversation without intrusion.

XII. Breach of Confidentiality and Privacy Under The Information And Technology Act 2000

According to section 72 of the above mentioned Act, if a person has secured access to any electronic record, book, register correspondence, information, document or other material without the consent of the person concerned and discloses the same to any other person then he shall be punishable with imprisonment upto two years, or with fine which may extend to one lakh rupees, or with both.

XIII. Encryption and Cryptography

Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. This therefore has the effect of ensuring total privacy even in open networks like the internet. Encryption involves the use of secret codes and ciphers to communicate information electronically from one person to another in such a way that the only person so communicating, would know to use the codes and ciphers. The field of cryptography on the other hand deals with the study of secret codes and ciphers and the innovations that occur in the field. It is also defined as the art and the science of keeping messages secure. Thus while encryption is the actual process, cryptography involves a study of the same and is of wider connotation.

XIV. The Right to Privacy and Encryption

It is usually agreed upon that in most democracies there do exist private and public spheres in every citizen’s life and that these two spheres are distinct and have to be treated as such. Although the line of distinction is blurred and continues to be the subject of much debate especially with regard to certain subjects such as pornography or the use of narcotics, it is generally agreed that the liberal democratic state has no power to interfere with the private aspect of its citizen's lives. There is a common misconception that the right to privacy is merely a weapon to ensure confidentiality in human affairs. This however does not present the complete picture. It must be remembered that the right to confidentiality arises only after information regarding human transaction or affairs have reached third parties. It may be said that privacy involves the right to control one's personal information and the ability to determine it and how that information should be used and obtained. This principle has sometimes been referred to as the right to "informational self-determination". This principle becomes all the more relevant with the onset of the internet and e-commerce. The volume and the varying nature of the transaction carried out on the net are such that the right to privacy must extend at least to a limited extent. At the same time, the very same factors, volume and the nature of transactions also raise the issue of security concerns as to the political, social and economic health of the country. Encryption of the details of our personal transactions would certainly assure us of greater degree of privacy but may also encroach upon the domain of national security concerns and two ends may be said to be in conflict.

XV. RESTRICTIONS ON CRYPTOGRAPHY IN INDIA

The use of the cryptography and encryption in India is a relatively new phenomenon. The use of this technology for the purposes of communication has begun only over the last 15-20 years in India. According to a recent report in India there are very few companies involved in the development of cryptography. Further, cryptography remains within the domain of the defense sector. It is only as late as 1995 that India introduced a list of items that required licensing before export. The list only included encryption software for telemetry systems in specific and did not relate to encryption software in general. The Information and Technology Act 2000 seeks to introduce some sort of control over the use of encryption for communication in India.

XVI. CONCLUSION

The internet is analogous to the high seas. No one owns it, yet people of all nationalities use it. It would perhaps be ideal if unification of internet laws could be so achieved so as to minimize the discrepancies in application of such laws. This is vital considering the growth of commercial activities on the internet. Changes need to be made to the existing Information and Technology Act 2000 in order to combat the numerous problems caused by the internet.

There is one spectacle grander than the sea, which is the sky, there is one spectacle grander than the sky, that is the interior soul

–Victor Hugo