CYBER CRIMES IN INDIA AND THE CHALLENGES AHEAD

Vivek Y. Dhupdale.[1]

I. Introduction:

Crime is not a new phenomenon. Only the means by which criminals are able to commit crimes has vastly changed in some respects thanks to the use of the Internet and computer system. As technology advances, so does the ways in which criminals are able to pull off their dreadful activities. With the help of the Internet technology, crimes can now be committed more anonymously and at a very quick speed. On the other hand, this same technology helps the law enforcement agencies catch perpetrators. Some of the most common and highly dangerous cyber crimes that are regularly committed with the help of the Internet technology are cyber terrorism, child pornography, fraud, sale and purchase of illegal guns or drugs, or other material that are protected by copyright law. These cyber crimes can be broken down into three main categories; viz., (a) hacking into someone's computer, take control over it and steal; (b) use of computers to store stolen passwords, credit card information, etc; and (c) the use of communication technology such as email through network to commit various crimes.

Cyber crimes are far more different from the conventional crimes. They are characterised by high technological innovation, anonymity, distance from the scene of crime, extent of its reach and most important, the unusual profile of the criminal, many times a juvenile.[2] In the words of Mittal and Mittal, "*Computer crimes and crimes committed through the Internet in particular are extremely challenging because of their sophistication and variance from crime in the ordinary sense*."[3] Internet is one of the fastest modes of communication and has spread its sphere, covering all possible shades of mankind. But as the saying goes, "every good side has a bad side too". The same is true with the computers and the Internet technologies too. The advent of the computer has been a boon to students, lawyers, businessmen, teachers, doctors, researchers and also to the criminals. Today we venture into the virtual world of cyber-space where our privacy does not exist at all. What you share, in good faith, can be exploited against you.[4] Crimes are no more confined to the physical space alone but have entered into the virtual cyberspace. Cyber crime is a criminal activity in which computers or computer

---

1 I/C Head, Department of Law, Shivaji University, Kolhapur, Maharashtra State (India).

2 Mittal S.K. & Mittal Raman, 2004, "*Legal Dimensions of Cyberspace*", Indian Law Institute, New Delhi, p.261.

3 Ibid, p. 260.

4 Sharma Vakul, 2002, "*Handbook of Cyber Laws*", Macmillan India Ltd., p.126.

networks are used as a tool, a target, or a place of criminal activity and includes every thing 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.[5] Cyber crime is the most dangerous of all the other types of crimes as it causes a huge amount of the loss which is evident from the number of cases coming before the criminal justice system. At the same time it is very easy to commit cyber crime by maintaining anonymity. This crime does not recognize any geographical boundaries which render the investigation, collection of evidence and prosecution of criminals extremely difficult. If these crimes are not curbed in time, there may cause a huge loss to the humanity at large in the near future.

II. Some Facts:

Cyber crimes are a new class of crimes rapidly increasing due to extensive use of internet and IT-enabled services.[6] However, there is so far no law that can be comprehensive on cyber crime though the Government of India has proposed major amendments to IT Act, 2000[7] (IT Act) by passing the Information Technology (Amendment) Bill, 2006[8]. It is estimated that in India 17 mega cities reported 118 cyber crime cases under IT Act, seven mega cities reported 180 cases under Indian Penal Code (IPC). Hence there was an increase of 32.6% in the total number of cases – from 89 in 2006 to 118 in 2007 – booked under the IT Act. According to a report released by the National Crimes Records Bureau, Bangalore tops the list with 40 cyber crimes; Pune falls second with 14 cases and Delhi with 10 cases.[9] IT Act is the only act which deals with cyber crimes at present. The primary objective of the IT Act is to create an enabling environment for commercial use of Information

---

5 D. Murali, "*Losses due to cyber crime can be as high as $40 billion"*, available at http://www.thehindubusinessline.com/mentor/2007/05/21/stories/2007052100681300.html.

6 Appeared in the Times of India, Bangalore Ed., 6/12/2008.

7 The draft of the bill was placed in the Parliament in December 1999 and passed in May 2000. After the assent of the President on June 9, 2000, the act was finally notified with effect from October 17, 2000 vide notification number G.S.R 788(E).

8 Information Technology Amendment Bill, 2006 was introduced in the Parliament. The Bill has been passed in the Parliament on December 23, 2008. It has been renamed as Information Technology (Amendment) Bill, 2008. It is awaiting assent of the President and formal notification. In the Indian context till a Bill is finally notified by the Executive, it remains a Bill only. Thus, till the government of India notifies it, the old Information Technology Act, 2000 would govern the Indian cyber law. IT amendment Bill was signed into an Act by the President of India on February 5 2009, through a Gazette Notification. Government of India is now in the process of framing the rules which are required under the amendments. On completion of this exercise, the date of effect of the amendments would be notified which will probably be completed by the end of April or early May 2009.

9 Ibid, n.1.

Technology. It performs the dual role of encouraging digital interaction as well as booking the 'net criminals'.[10] However, since the IT Act is still in its improving stage, certain omissions and commissions of criminals while using the Information Technology have not been incorporated. Therefore, all the cyber crime cases are essentially required to be filed both under IPC and IT Act depending upon the nature of the crime.[11]

III. Who Could be a Cyber Criminal?

Children and adolescents between the age group of 6–18 years have a tendency to know and explore things and sometimes to prove their unique qualities. Organised hackers have their own targets to achieve. Professional hackers or crackers are employed to hack the site of the rivals and get credible, reliable and valuable information.[12] Discontented employees are people including those who have been either sacked by their employer or are dissatisfied with their employer. Therefore to take revenge they may also resort to these kinds of criminal activities.

IV. Applicability of IT Act 2000 to Cyber Crimes:

When IT Act was drafted the focus was more on providing a legal framework of E-Commerce. The most urgent need of the day was to provide legal recognition for electronic documents and defining a means of authentication of the electronic documents.[13] At the same time, some offences were also sought to be added through Chapter XI of the Act. The IT Act provided[14] that investigations of offences under the Act shall be undertaken only by a Police Officer of the rank of Dy. S.P. and above (now as per amendment, by a police officer not below the rank of Inspector). These provisions made the administrators feel that the offences referred above needed to be handled separately therefore some special independent Cells and Police Stations were set up in order to investigate and prosecute offences under the IT Act 2000.[15] These Cells and Police Stations were called "*Cyber Crime Cells*" and "*Cyber Crime Police Stations*" and therefore the word

10 Trilokekar N.P., 2000, "*A Practical Guide to Information Technology Act, 2000*", Snow White Publications Pvt. Ltd., Mumbai, p.51.

11 Ibid.

12 There are some professional hackers (white hat hackers) like Richard Stallman who is one of the top Non-Criminal Hackers of all time. He has received extensive recognition for his work, including awards, fellowship and four honorary doctorates. S.Gade, "*Cyber Space*", Lawyers Update, Vol XV, Part 5, May 2009, at p.20. Some of the infamous hackers (criminal) are: The *Guy, Captain Zap and Dr. Diode, Joe Engressia – The Whistler, Kevin Mitnick – the star of the hackers, Kevin Poulson.* Supra n. 5, p 201-03.

13 Vijayashankar Na., 2007, 'Applicability of IT Act 2000 in Cyber Crimes', *Law of Information Technology & Its Emerging Trends*, p.27-31.

14 Through Section 78.

15 Ibid.

"*Cyber Crime*" was considered similar to the offences under the IT Act 2000. The "*Cyber Crime*" has not been defined anywhere in the IT Act 2000 (not even in the amended Act). It only delved with few instances of computer related crimes which are defined in Chapter XI of the Act as follows:

a. Illegal access, introduction of virus, denial of services, causing damage and manipulating computer accounts.[16]
b. Tampering, destroying and concealing computer code.[17]
c. Acts of hacking leading to wrongful loss or damage.[18]
d. Acts related to publishing, transmission or causing Publication of obscene/lascivious in nature.[19]

Crimes such as causing denial of service, introduction of virus etc. as mentioned under section 43 only amounte to payment of damages which may be upto one crore rupees of fine. Punishment by imprisonment provided under section 65 and 66 amounted to 3 years or fine up to two lakhs rupees or with both. Under section 67 the first time offenders can be punished up to 5 years of imprisonment and with a fine of up to one lakhs rupees. Subsequent offence may lead to punishment of 10 years of imprisonment and fine up to 2 lakhs of rupees, etc.

V. Some Analysis of the IT Amendment Act of 2008:[20]

This Amendment Act has managed to improve the provision of the main IT Act to some extent. The salient features of the Amendment Act are as follows:

1. It has created liability of any body corporate towards dealing with Sensitive Personal Data.[21]
2. Introduction of virus, manipulating accounts, denial of services etc made heavily punishable.[22]
3. Sending of threatening, irritating messages and also sending misleading information about the origin of the message electronically has been made punishable.[23]
4. The acts of fraudulently receiving and retaining any stolen computer resource or communication device have also been made

16 Section 43.
17 Section 65.
18 Section 66.
19 Section 67.
20 IT Act Amendment 2008 came into force after in Feb, 2009 after the assent of the President.
21 Amendment of Section 43 of IT Act 2000.
22 Amendment of Section 66.
23 Section 66 A, Phishing and Spam.

punishable.[24]

5. Dishonest use of somebody else's digital signature has been made punishable.[25]
6. Cheating using computer resource has been made punishable.[26]
7. Introduced the special provisions dealing with Cyber Terrorism[27] which include following criminal activities:
   a. Denial of service of resources in use by nation.
   b. Attempting to penetrate or access a computer resource without authorisation or exceeding authorised access has been made punishable.
   c. Introducing or causing to introduce any computer contaminant likely to cause death or injuries to person or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or
   d. knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

These acts have been made punishable with Imprisonment which may extend to imprisonment for life.

8. The publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act or conduct, any one who creates, facilitates or records these acts and images is punishable.[28]
9. Intermediaries have been made liable to retain any information

24 Insertion of a new Section 66 B.
25 Insertion of a new Section 66 C.
26 Insertion of a new Section 66 D.
27 Insertion of a new Section 66 F.
28 Insertion of a new Section 67 B.

in the format that Central government prescribes.[29]

10. Introduction of Surveillance, Interception and Monitoring in order to compact cyber terrorism.[30]
11. All cases which entail punishment of three years or more have been made cognizable.[31]
12. One major change has been that of inclusion of Inspectors as investigating officers for offences defined in this act.[32] Earlier these investigations were being done only by an officer of the rank of Deputy Superintendent of Police which was a serious limitation mainly because number of officers in this rank is limited.
13. Newly introduced section 66 E talks about acts of intentionally or knowingly capturing, publishing or transmitting the images of any private area of any person without his or her consent, under circumstances violating the privacy of that person are made heavily punishable under the Act.

VI. Jurisdiction - A Major Hurdle in Cyber Crime Detection:

In spite of the latest amendment IT Act, the question of jurisdiction still remains threatening. Since most of the cyber crimes are committed by the perpetrator sitting at a far distance from the scene of offence, it becomes extremely difficult for the law enforcers to detect the crime and nab the culprits. The main problem with the Internet Jurisdiction is the involvement of multiple parties in different corners of the world. Therefore, it is highly difficult to accurately locate and establish a place from where the offender resides or so as to where the cause of action for the offence has occurred. Thanks to the legislature that our IT Act extends to whole of India and also envisages any offence or contravention thereunder committed outside India by any person.[33] Hence, it provides for an extra-territorial jurisdiction on Indian Courts and empowers them to take cognizance of offences committed even outside India irrespective of the nationality of the culprit. But in case of foreign criminals belonging to foreign nationals, such offence must involve a computer, computer system on computer network which is located in India.[34]

VII. Cyber Crimes and the Indian Criminal Justice System – the Impact:

Cyber crime has made a significant impact on the criminal justice system prevalent throughout the world. The effects are seen even more as nations are constantly trying to provide faster and well-organised services to

29 Insertion of a new Section 67 C & 69 (4).
30 Section 69.
31 Section 77 B
32 Section 78.
33 Sec. 1(2).
34 See Sec.75 (2) of the Act.

its citizens with the help of cyber space *via* internet. Almost all crimes in the modern time involve the use of computers and other electronic media at some stage of the act being committed by the offenders. Realizing the effectiveness of computers and the Internet to succeed in committing conventional crimes, the criminals are using them as tools for committing such criminal offences. Therefore, a Cyber Crime Investigation Cell is now the need of the hour for any law enforcement agency to tackle not only cyber crimes but also investigate other traditional or conventional crimes as there is an increasing use of encryption, high-frequency encrypted voice or data links, steganography etc. by terrorists and members of organised crime cartels. Some of the instances are coming to light where computers and other electronic tools have been used as tools to facilitate the commission of conventional crimes. Some of the conventional crimes where cyber space and other electronic media have been used are: Organised Crime, Terrorism, and Cyber Crime.

VII. Challenging the Challenges:

Computer technology offers many advantages to law enforcement agencies. A computer fitted patrol car can help a traffic police officer to detect and then confront someone who has just stolen a vehicle. Another example is the face-recognition software. With the help of CCTVs (closed circuit televisions) in public places, the software is being used in several areas to match faces in the crowd on public streets with photographic databases of known criminals. However, as the use of computer technology for good purpose has increased, the criminals too have adapted the technology for their unlawful activities. Therefore, to fight against these cyber criminals the law enforcement agencies will have to enhance their high-technology capabilities, including investigative techniques, sophisticated equipments, high technical training, and personnel recruitment and retention programmes. Computer/cyber crime control requires cooperation between the investigating agencies, public and private sectors. The law enforcement units must earn confidence amongst the people.

Sometimes we often wonder how wired connected we are with each other. Almost everything in our life is connected to some kind of technology and its gadgets. But imagine what a hacker can do to our life. He can snap down all our connections and turn us into Stone Age[35] within minutes for hours together. This is what is called as the cyber war in the modern terminology. Therefore, to fight this war our criminal justice system must be alert.

Cyber crime is the new challenge for the Indian society, industry and the law enforcement and the entire criminal justice system as a whole. The

35 Appeared in the New Indian Express, 21/06/2008, p.8.

anonymous nature of the Internet makes it an attractive medium to commit crimes and frauds.[36] Cyber crime is not confined to any national boundary. Therefore, it becomes very difficult to control the extent of its criminal activity. Though cyber crimes are increasing day by day and has become a matter of concern, yet there is lack of awareness among the people in general. Many individuals do not take initiative to come and report these crimes either due to its lack of awareness or in their opinion; such crimes would not be given much significance. Moreover, even some organisations also hesitate in reporting such crimes as they are afraid of losing reputation in the market.

The present position shows that cyber crimes are likely to grow in extent and complexity as more and more people are accessing internet services for their various purposes. It is high time that industries, law enforcement agencies and supporting groups should come forward to empower and protect individuals and organisations from falling prey to these cyber crimes and other online crimes.

The Police personnel, the prosecutors and the lower judiciary need to be educated to fight cyber crimes. This can be effectively achieved by organizing periodic conferences, seminars and workshops, training programmemes, etc. In fact the CBI, the Bureau of Police Research and Development (BPR&D) and the National Police Academy (NPA), Hyderabad have already made significant contributions by preparing a training module to be administered to State police personnel and conducted several training programmemes. There is no information that any systematic effort has been made till now to impart training to prosecutors and judges, although there is evidence of their keenness to become knowledgeable.

VIII. Cyber Crime and the International Co-operation:

An International co-operation in fighting the menace of cyber crime is the need of the hour today as the cyber crime knows no boundaries. For example, a hacker in New York can break into a system in Mumbai without the aid of any extraordinary talent or equipment. What he needs is a personal computer and a network connection. There is a need to create awareness among the international community that a hacker should not be allowed to get away only because of legal inadequacies. Section 75 of the IT Act clearly lays down that its provisions shall also apply to "any offence or contravention committed outside India by any person, irrespective of his nationality", provided that such act involves a computer, a computer system or computer network located in India.[37] But the biggest problem in securing international co-operation

36 A N Roy, IPS Commissioner of Police, Mumbai Available at http://www.Indiacyberlab.in/know_more/copawards2005-message.htm.

37 Ibid.

is that some nations are trying to protect their own citizens once blame comes on them.[38] The procedure also involves a request by the court of one country to its counterpart in another. Collection of information in cyber matters requires searches and confiscation of delicate material that needs speedy and expert handling. Assistance in such areas is slow and half-hearted despite the best of relations between countries. The Lyon Group of high-level experts set up by the G-8 nations has also been active. At this group's instance, a network of contacts available round-the-clock has been established. The Interpol has now the operational responsibility for this network and the CBI has been identified as a contact point for the Indian subcontinent and its neighbourhood.

IX. Network Service Provider's Liability:

The Information Technology Act, 2000 (as amended) provides that the Network Service Providers (ISPs) not to be liable for any third party information made available by him, if, he proves that the offence was committed without his knowledge, or that he had exercised all due diligence to prevent the commissioning of such offence.[39] The reason behind this is that the ISPs have no control over the contents of websites that are accessed daily. Then the question is who is liable for the unlawful acts on the Internet. Is it the sender of the information, the service provider, the user or all of them together?[40] In the Church of Scientology case in the Netherlands,[41] the court decided that the information providers do nothing more than offer an opportunity to publish and that they are unable to exercise any control over, or even be aware of, what people say or are able to say on the internet. Another problem is that if the service providers try to constantly monitor all the sites on their servers, it may amount to undesirable form of censorship by them. But the service provider is the only one person apart from the information provider himself, who can prevent the crime being committed by way of closing the site. At the same time every possible thing should be done to trace the source of the information. And hence it is the source and not the service provider primarily is liable for the content. But sometime the service provider may be held responsible by compelling him to reveal the identity of the owner of anonymous home page during investigation.[42] The Anti-Terrorism, Crime and Security Act, 2001 was passed in UK as an emergency legislative measure in

38 For example, in recent incident of terror attack on Mumbai on 26/22/2008, which was evidently done by the terrorist's groups operating in Pakistan, but inspite of the demand from Indian Government to hand over the offenders for the purpose of prosecution, it is trying to protect them by assuring that they be tried if proved guilty in their own country only and will not be handed over to India.

39 Sec.79.

40 Rider Rodney D., Third Ed., 2007, "*Guide to Cyber Laws*", Wadhwa and Company, New Delhi, p. 1173

41 Ibid.

42 Ibid. these threats.

the wake of the September 11 terrorist attacks. The Act provides for a code of practice on the retention by the ISPs, etc, of communications data obtained held by them such as websites visited by the customers and when and to whom emails are sent would also be retained. The data will be made available on the request to law enforcement agencies for the purpose of safeguarding, or preventing or detecting crime that related to, national security.

X. Prevention and Control of Cyber Crimes:

Following are the steps which may be initiated by various individuals, organizations and other agencies to prevent ant /or control cyber crimes.

In the case of Organisation:

a) The first step must be to begin the process of fully understanding the organisation's exposure to the threat of data/information. For instance, at the time of recruitment of staff, the organisation must make sure that they must have an adequate background.
b) There must by reasonable restrictions imposed on the employees' access to data based on their role and there must be adequate control on their activities.
c) There must by reasonable restrictions imposed on the employees' access to data based on their role and there must be adequate control on their activities.
d) Adequate training must be provided to the employees in coping up with cyber crime threats and to report immediately their incidents.
e) There is a need to make Acts like Data Protection Act (DPA), etc., mandatory for Indian companies.
f) There is a need for an effective process such as information sharing and cooperation with foreign countries as cyber crimes are not confined to geographic borders.
g) The Companies must register themselves with the CERT[43] to stay updated with latest vulnerability and treats.
h) They need to conduct user awareness programmemes periodically.
i) They must update their security polices and procedures regularly.
j) They must perform security audit and implement suitable recommendations.
k) Companies must adopt global security practices so as to encourage more and more people to prefer online transactions.

---

43 The Computer Emergency Response Teams (CERTs) which has been created in order to coordinate and respond during major security incidents/events. These organisations identify and address existing and potential threats and vulnerabilities in the system and coordinate with stakeholders to address these threats.

In the case of Law Enforcement Agencies:

a) There is an urgent need to introduce Graduation as one of the minimum qualification for the police personnel.

b) Basic computer training is a must for the newly recruited police personnel.

c) The Law enforcement officers must be provided with adequate training in various broad range of issues relating to
   i. cyber crime,
   ii. forensic work,
   iii. online sharing procedures and communication protocols.

   Such training needs to be conducted more frequently for the law enforcement officials so that enforcement units are capable of investigating cyber crime.

d) Some of the basic skills required by the law enforcers are:
   iv. Common forensic computing techniques;
   v. automation of digital evidence analysis;
   vi. procedures for data recovery and analysis;
   vii. legal considerations;
   viii. principles of forensic computing;
   ix. disk and file system forensics;
   x. operating systems forensics; and
   xi. Internet and organisational networks.

e. Finally, for the complete realisation of the provisions of the cyber laws, a cooperative police force is required to encourage victims to report cyber crimes.

In the case of Individuals:

a. Children:

Children should not give out identifying information such as Names, Home Addresses, School Name or Telephone Number in a chat room. They should not give photographs to anyone on the Net without first checking or informing parents or guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to –face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

b. Parents:

Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol. There is also software to establish time controls for use of limpets (for example blocking usage after a particulars time) and allowing parents to see which site item children have visited. Use this software to keep track of the type of activities of children.

There must be proper user awareness programmemes conducted to educate the people about the seriousness of cyber crime and its prevention.

a. A counseling session for college students has to be launched to educate them on the gravity and consequences emanating from cyber crimes.
b. Individuals must avoid giving out any personal information about themselves to any one specially the strangers.
c. Children should never be allowed to arrange their face-to-face meetings or send their photographs online without informing their parents.
d. The latest and updated anti-virus software, operating systems, Web browsers and email programmemes must be used to fight against virus attacks.
e. One must always thoroughly check the site he is doing business with.
f. One must send credit card information only to secured sites.
g. While chatting on the net one should avoid sending photographs to strangers along with personal data as it can be misused.
h. Backup volumes of the data should always be kept to prevent loss from virus contamination.
i. Children should be prevented from accessing obscene sites by the parents to protect them from spoiling their mind and career.
j. A credit card number shall never be sent to an unsecured site to prevent fraud or cheating.
k. Effort shall be made to make a security code and programme to guard the computer system from misuse.
l. We must use a security programme that gives us a control over the cookies that send information back to Web sites. Letting all cookies in without monitoring them could be risky.
m. If anyone owns a Web site, he must watch traffic and put host-based intrusion detection devices on his servers. Monitor activity and look for any irregularities.
n. A check should be kept on the functioning of cyber cafes and any mishappening shall be reported to the concerned authorities. Efforts should be made to discourage misuse of computers and access to unauthorised data.

d. Cyber Café's Responsibilities:

Though the cyber café' owners cannot be held liable for anything done by any person accessing the internet without their knowledge, but it is their duty to maintain proper records about their customers. A register wherein the customers can enter their names, addresses, phone numbers, etc. may be installed at the counter of such cyber café's. The can also be allowed to enter the café' only by checking their ID cards if any, etc. This will enable them to

keep track of their customers.

XI. Conclusion:

To conclude one can say that with the rapid increase in science and technology, the Cyber Crimes are here to stay in our modern world. One of the greatest loop-hole in the field of Cyber Crime is the absence of comprehensive law anywhere in the World. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of I.T. Act and amendments made to Indian Penal Code, problems associated with cyber crimes continue to persist.

Similar efforts have been made by various countries to fight this menace by enacting national legislations but in the long run, they may not prove to be as beneficial as desired. An effort is still wanted to formulate an international law on the use of Internet The Information Technology Act 2000 was passed when the country was facing the problem of growing cyber crimes via internet and other media. It was felt necessary to take certain precautions while operating the internet, etc. Therefore, in order to prevent cyber crime it is important to make public aware of using the computers and modern technology for the betterment of the society. Another challenge is that most of the cyber criminals are those who are under the age of majority; therefore some other legal framework has to be evolved to deal with them. Since cyber world does not recognize any geographical boundaries, it is a Herculean task to frame laws to cover each and every aspect. But, however a balance has to be maintained and laws be evolved so as to keep a check on cyber crimes. However, it is not possible to eliminate cyber crimes from the cyber space, but it is quite possible to check them. The only promising step is to make people aware of their rights and duties to report cyber crimes in time as and when they occur recognising it as their duty towards the society. The judiciary should also make the application of laws more stringent to check cyber crimes. No doubt the IT ACT is a welcome step in the cyber world, but it needs to be suitably modified so as to make it more effective and powerful to combat cyber crimes.[44] To some extent the Parliament of India has attempted to cover many cyber crimes under the I T Act, 2010 by enacting the I T Amendment Act of 2008. But even then it would be incomplete as new and new cyber crimes are being committed by the criminals and it is indeed a one of the greatest challenge to the criminal justice system of India.

44 As amended in 2008.