Soma Ghosh

Cyber Crime: A Menace in the World of Technology

Foreword

Cybercrime is a criminal activity which is committed by the use of computers, laptops, tablets, mobiles and by using Internet connectivity through these devices. Some of the common cyber crimes are hacking, cyber stalking, denial of service attack (DoS), virus dissemination, software piracy, credit card fraud & phishing**.** As per the data developed by National Crime Record Bureau (NCRB), a total of 5,693, 9,622 and 11,592 cyber crime cases were registered during the years 2013, 2014 and 2015, respectively, showing a rise of 69 per cent during 2013 to 2014 and 20 per cent increase during 2014 to 2015. CIDs (Criminal Investigation Departments) of various cities opened up Cyber Crime Cells in different cities to tackle the issue of cyber crimes. *As* the Information Technology Act of India a cyber crime has a global jurisdiction and hence a complaint can be filed in any cyber cell. The role of this Cell is to detect, prevent and investigate Cyber crimes that come under the ambit of Information Technology Act 2000 and assist the other Law Enforcement in the investigation of crimes in which elements of Computer related crime exists.

SCRB West Bengal had organized a 2-day Cyber Crime Workshop on June 16 & 17, 2007 at SCRB Bhawan, Salt Lake Kolkata. The Workshop was meant to create awareness on the emerging cyber crime and as to how the Police Department needs to equip itself to successfully handle such cases. Participation was received from Kolkata & West Bengal Police as also from the neighboring states of Jharkhand, Sikkim & Meghalaya. SCRB West Bengal organized the

Second 2-day Cyber Crime Workshop on 25th and 26th August 2008 at SCRB Bhawan, Salt Lake Kolkata in association with NASSCOM. But Kolkata Police has confessed that ‘There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to calculate.’[1] But regarding cyber crime against women the Indian police system is still in its infancy. Further there are lots of confusions and unaddressed areas in IT Act, 2000, and even in its amendment in 2008, especially in the events related to cyber crime against women. The research and Government or semi government projects or even private academic endeavours have rarely shown deeper interest in dealing with the occurrences of cyber crime against women. Though ‘every woman has a right to take legal action against any person who assaults or tries to outrage her modesty by any deliberate constant gesture or physical force’ (Sec. 354 of IPC), in the virtual space there is absence of any such distinct legal promises; IT Act in India is also incomplete and almost ineffective in this regard. An attempt has been made in this UGC_MRP Project work to pay due attention to this area of cyber crime, i.e., cyber crime against women.

A Conceptual Framework

Technology has made us wise, wealthy and has enriched us with all sorts of resources; it has connected us with the rest of the world. Technology has converted the globe into village and enabled us to think in terms of global brotherhood. But at the same time, a debate has been

[1] ‘Computer and Internet-Related Crime - Kolkata Police’, www.kolkatapolice.gov.in/ComputerandInternet.aspx

initiated regarding the curse it has brought about in our life. The network which was designed to give shape to global democracy, has taken away the basic rights from some fellow netizens, because rights and duties in cyber space are not being positively nurtured by some among us. Some of us unknowingly are getting trapped by the persons who, instead of performing their duties to maintain etiquettes in the cyber zone, are misusing their right to go online freely. Onus lies on the victims also, because they do not use their right to go online with adequate precautions, thereby giving plenty of opportunities to the criminals to violate their right. Cyber crime and victimisation of women are on the rise in India in particular and it possesses a major threat to the security of a person and his/her individuality and personality as a whole. Even though India is one of the very few countries in the world to enact a law like IT Act 2000 which was formulated to combat cyber related crimes, but many of the occurrences of cyber crime are still beyond its reach; specially criminal activities regarding women and her safety in the cyber space still are in a grey domain and often unexplored in this Act. Though some efforts have been made in the redesigned IT Act-2012, there still exist undefined zones that require better clarification, especially for police administration to act faster and proper. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences, but the grave threat to the security of women in general is not yet being covered distinctly by this restructured IT Act. Chapter IX of the IT Act deals with offences such as tampering with computer sourced documents (Sec.65), hacking with computer system (Sec.66), publishing of information, which is obscene in electronic form (Sec.67), access to protected system (Sec.70), publication for fraudulent purpose (Sec.74). IT Act 2012 still needs to be modified. It should be made more stringent against any sort of cyber crime specifically if it is committed against women and children, as in such situations the crime may infringe one' fundamental right to life and personal liberty.

Cyber Crime: A Menace in the World of Technology

World, today, can be better designated as E-World or cyber world, surrounded by e-commerce, e-governance, e-communication, e-security. E-technology has become indispensible part of our daily life, as it provides worldwide uncontested opportunity to promote and progress human society. The era of modern computers, which began with the analytical engine of Charles Babbage has now taken a revolutionary turn. National Science Foundation reveals some interesting details -

Internet World Stats estimates of the number of Internet users by language as of June 30, 2016[2]

Table 1 - World Internet Users by Language

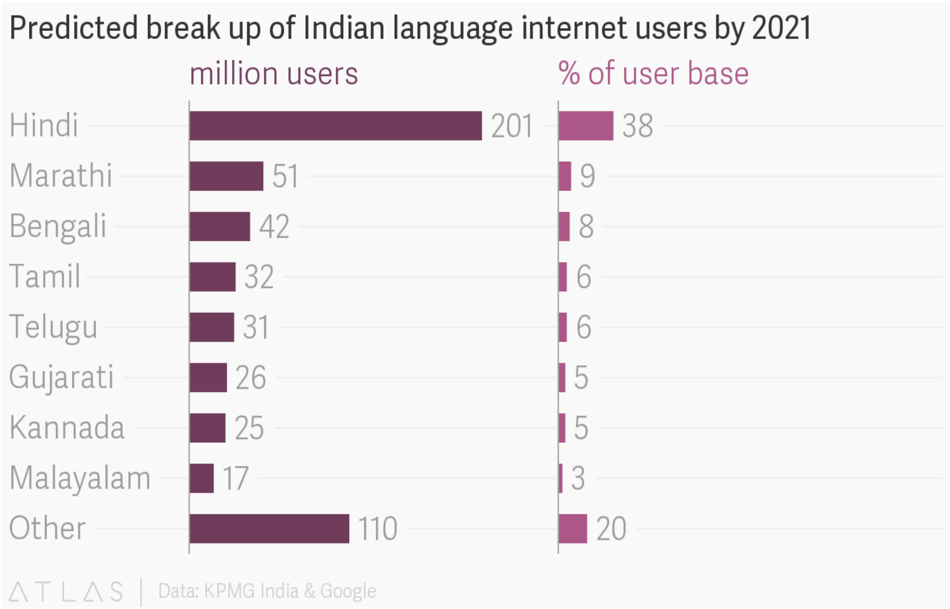
RANK	LANGUAGE	INTERNET USERS	PERCENTAGE
1	English	948,608,782	26.3%
2	Chinese	751,985,224	20.8%
3	Spanish	277,125,947	7.7%

[2] "Number of Internet Users by Language", *Internet World Stats*, Miniwatts Marketing Group, 30 June 2016, accessed 15 November 2016

4	Arabic	168,426,690	4.7%
5	Portuguese	154,525,606	4.3%
6	Japanese	115,111,595	3.2%
7	Malay	109,400,982	3.0%
8	Russian	103,147,691	2.9%
9	French	102,171,481	2.8%
10	German	83,825,134	2.3%
11–36	Others	797,046,681	22.1%
TOTAL		3.61 Billion.	100%

Figure: 1 - Predicted

Break up of Indian Language Internet Users by 2021



Source: ATLAS KPMG INDIA & GOOGLE

The trend shows that internet is changing the way of life. Internet use is increasing rapidly. According to the National Science Foundation, the amount of time an average person spends on the hi-tech devices has increased rapidly.

This revolution in the world of technology has brought about a positive change in our socio-economic life and livelihood, but simultaneously has made us vulnerable to the threat, called cyber crime, making our e-life a target of cyber criminals. ‘Cyberspace has no specific jurisdiction; therefore, criminals can commit crime from any location through computer in the world leaving no evidence to control[3]. A new breed of criminals has appeared in the earth to cause damage and injury to society through some unprecedented criminal activities. Now-a-days everyone who has to work on a computer is vulnerable to cyber crime. Intensity of attacks by the cyber criminals is far beyond the extent of physical assault or mental torture. ‘…cyber crime, e-crime, hi-tech crime, or electronic crime …is nothing but an activity done with a criminal intent in cyber space.’[4] Cyber criminals make computer as their target and the tool for penetration of crime. The Information Technology Act, 2000, specifies the criminal activities which have been identified as punishable with extent and intensity of punishment. Statistics show that cyber crime is on the rise and India is no exception to it.

With the gradual development of Information Technology (IT) cyber crimes are like cancerous inflammations threatening human existence and civilization. It has been globally extorting the aspects of social, cultural and economic stability by means of Internet and or mobile technology. It is a heinous form of dangerous crime that involves computer to derive unbound criminal profits. It gets into the depth of success of organisations, fields of governmental services and or any individual's peripheries without their knowledge or trotting into the secrets of activities of any organisation or individual to snatch all essential information regarding their highly personal and/or official business.

[3] *“Cyber Crimes: A New challenge, Deputy Controller(Technology),* CCA, Ministry of Information Technology, India, 2002.

[4] Dr., Rao, I. Jagadeeswara, ‘Cyber Crimes: Issues and concerns, ISRJ Vol. I, ISSUE-X ISSN No: 2230-7850, November, 2011.

Women are often worst victims of cyber crimes, as these may hurt their dignity also. Union minister Ravi Shankar Prasad on 1st August, 2017, asked law enforcement officials to be "very harsh" in dealing with cases of abuse and offence against women on social media. The IT and law minister also said that the government would ask firmly all social media platform to follow Indian laws specially in issues related to women. Addressing a conference of superintendents of police and commandants of central armed police forces in New Delhi, the minister said, "I have to make one request to all of you. In case of offence against women, abuse in social media, become very harsh. We are doing our best. Large number of sites has been blocked."[5]

With the growing penetration of the Internet and Information and Communication Technologies (ICT) in countries around the world, and, in particular, in developing countries, criminal and mischievous elements around the world are becoming active with the intent to abuse the open facilities of the ICT technologies for their benefit or entertainment. The central problem of law enforcement and regulations is to establish the framework within which such abuses can be checked.

In India, the penetration rates of the Internet and of ICT are fast growing and along with this the problems of usage and enforcement are on the rise. There is a phenomenal growth in the world of Cyber Crimes booked under existing laws in India. 'There were 4192 cyber crimes in 2013 which were 2761 in 2012. 11,592 cases of cyber crime have been registered in India in 2015 as per 2016 NCRB report. Uttar Pradesh recorded the highest number of cyber crimes at 2,208, Maharashtra followed closely with 2,195 in this 2016 report.

If one considers such crimes as per Indian Penal Code also, the number of crimes was 5500. Police has arrested 3301 criminals in this regard. Under Information Technology Act, 2000, there

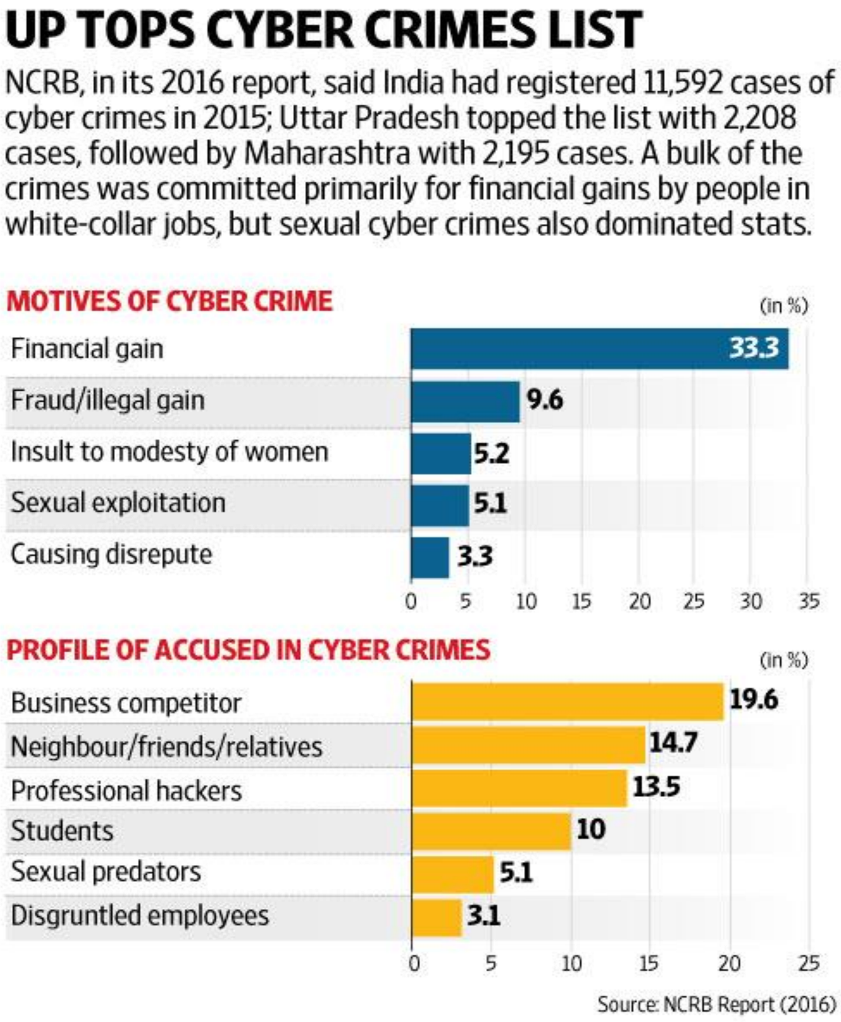
[5] The Indian Express, **PTI** | New Delhi , August 1, 2017

were 681 and 635 crimes in Maharashtra and Andhra Pradesh respectively. In these two states there has been a steep rise of 50 per cent in recorded cyber crimes. As per National Crimes Records Bureau (NCRB), in 2013 there was 122 per cent increase in cyber crimes in India. Such crimes in other states were: Karnatak (513), Kerala (349), Madhya Pradesh (282) and Rajasthan (239). In the state of Gujarat, such crimes were 68 in 2012 and 61 in 2013'[6].

As more and more people are internet and having access to computers, cyber crimes and mobile crimes have become a regular botheration to the governments of different countries of the globe and India is no exception to it. But the efficacy of Indian cyber law is under the scanner of the experts and they feel that Indian cyber laws are still ineffective in terms of dealing with appropriate cyber crime convictions. Further, in India, recorded number of cyber fraud is alarmingly increasing with continuous momentum.

Figure : 2 - NCRB Presentation 2016

[6] Gujarat Samachar, Ahmadabad, 3 July, 2014



UP TOPS CYBER CRIMES LIST

NCRB, in its 2016 report, said India had registered 11,592 cases of cyber crimes in 2015; Uttar Pradesh topped the list with 2,208 cases, followed by Maharashtra with 2,195 cases. A bulk of the crimes was committed primarily for financial gains by people in white-collar jobs, but sexual cyber crimes also dominated stats.

Source: NCRB Report (2016)

As per one Norton report, more than Rs 50,400 crore was lost by Indians during 2012 on cyber fraud itself and that trend showed no signs of lessening. Following 2008 amendment the Indian information technology law has become softer in terms of cyber crimes, because except crimes like cyber terrorism and child pornography, almost all other cyber offences are bailable. This means that it is not very difficult for a convict to come out of imprisonment and delete evidence. India is moving ahead with its plan and policy of bilateral cooperation with around 15 countries for exchange of information and status on cyber crime. The Indian Computer Emergency Response Team (CERT-In) also working hard to address the issues related to latest cyber threats. There has been a wide penetration of internet in urban and rural India today, which was being centered in the purely urban areas even few years back. The penetration of active internet users in India has grown rapidly. These are some of the findings from the latest I-Cube Report on 'Internet in Rural India' which was released by the Internet and Mobile Association of India (IAMAI) and IMRB. According to the report, the number of claimed internet users even in rural India is expected to rise more rapidly.

This isn't all. A more serious mode of threat is for women, as in our social process women still are very sensitive regarding their dignity and social reputation. Harassment via e-mails, cyber-stalking, cyber pornography, defamation, morphing, emails spoofing etc. are some of the dirty mechanisms which affect the women to the extent of taking away their right to life and personal liberty.

Chethan Kumar wrote in an article, '*One cybercrime in India every 10 minutes'* on Jul 22, 2017[7],

> 'from the global ransomware attacks that hit hundreds of systems to phishing and scanning rackets, at least one cybercrime was reported every 10 minutes in India in the first six months of 2017. That's higher than a crime every 12 minutes in 2016. According to the Indian Computer Emergency Response Team (CERT-In), 27,482 cases of cybercrime were reported from January to June. These include phishing, scanning or probing, site intrusions, defacements, virus or

[7] http://economictimes.indiatimes.com

> malicious code, ransomware and denial-of-service attacks. With more Indians going online, cyber experts said putting in place critical infrastructure to predict and prevent cybercrimes was crucial. India has seen a total of 1.71 lakh cybercrimes in the past three-and-a-half years and the number of crimes so far this year (27,482) indicate that the total number is likely to cross 50,000 by December, just as in 2016.

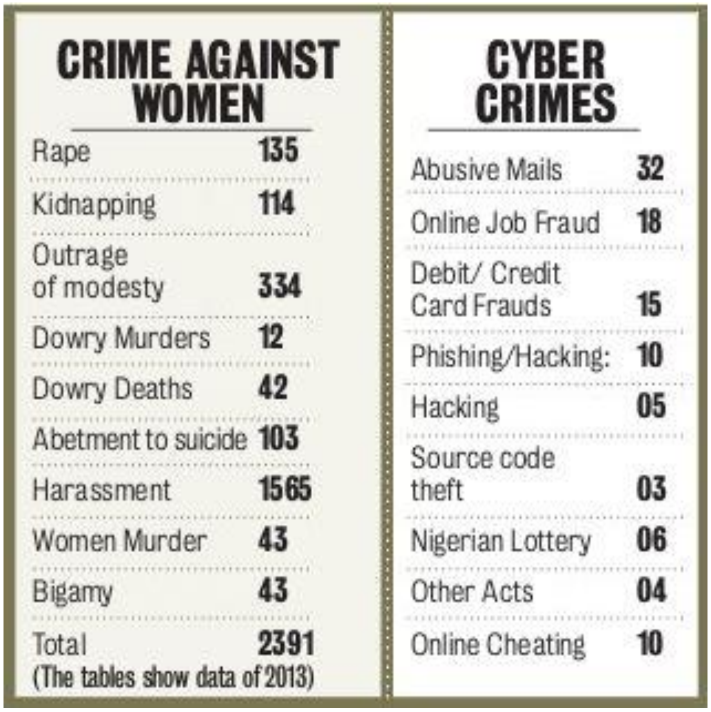
Incomplete computer knowledge makes women and rural people more vulnerable. Browsing the internet through Google or the use of social networking websites like Facebook, Twitter, or Orkut without proper knowledge of privacy protection, protection from spy ware, internet viruses like Trojans, tracking cookies etc. jeopardizes their safety and same applies to children also. In West Bengal, targeting women through internet and mobile phone devices have shown a higher prevalence. Though West Bengal is quite a long way from being the country's cyber crime paradise, but time has come to think over the issue and the task must begin with generating awareness among people.

Social media as a phenomenon has grown by leaps and bounds in 2013. However, with the passage of time, 2013 has exhibited that the Information Technology Act, 2000 is not capable of effectively addressing the legal, policy and regulatory concerns generated by the use of social media in India.

The report presented below upholds an alarming scenario for us: [8]

[8] The Hindu, Bangalore, October 31,2013, Updated: October 31, 2013 00:42 IST

Figure : 3: Classification of Crime On Gender Basis



CRIME AGAINST WOMEN	
Rape	135
Kidnapping	114
Outrage of modesty	334
Dowry Murders	12
Dowry Deaths	42
Abetment to suicide	103
Harassment	1565
Women Murder	43
Bigamy	43
Total	2391

(The tables show data of 2013)

CYBER CRIMES	
Abusive Mails	32
Online Job Fraud	18
Debit/ Credit Card Frauds	15
Phishing/Hacking:	10
Hacking	05
Source code theft	03
Nigerian Lottery	06
Other Acts	04
Online Cheating	10

Perpetrators of such crimes can be booked under sections 66 C (which prescribes punishment for identity theft), 66A (which prescribes punishment for sending offensive messages through communication services), 66D (which prescribes punishment for cheating by impersonation) and 67 of the I.T. Act, 2000(which prescribes punishment for publishing or transmitting obscene material in electronic form).

They can also be booked under 499 (which defines defamation) /120B (which prescribes punishment for criminal conspiracy) of the Indian Penal Code and Section 6 of the Indecent Representation of Women (Prohibition) Act. But these are insufficient measures or inadequate tools to fight against growing menace of cyber crime in India.

West Bengal - Kolkata in particular - has shown the biggest jump nationwide in cyber-crime cases, according to the National Crime Records Data for 2012. From six cases in 2011, Kolkata Police has registered 68 cases in 2012 and 84 in 2013. The case details depict that most cases relate to damage or loss to a computer or device (section 66(1) of IT Act, 2000) and hacking (section 66(2) of IT Act, 2000). In the three years up to 2013, registered cases of cyber crime were up 350%, from 966 to 4,356.[9]

Cyber crime appears to be concentrated in states with major cities, indicating that urbanization and consequent internet penetration are the factors. Maharashtra accounts for the most persons arrested under the IT Act, 2000, and Uttar Pradesh reported the most arrests under the older Indian Penal Code (IPC). The figures are also indicative of a rising trend among cops in states like West Bengal to register cyber-crime cases under the traditional IPC sections giving the IT Act, 2000, a pass. The Kolkata figures are even scarier - a 1033.3 % jump between 2011 and 2015[10]. Among those arrested last year for cyber crimes were four students and six minors, who were treated as "sexual freaks". In such cases also police cops are increasingly filing cases under IPC sections, giving the Cyber Crime Act a miss.

Under such circumstances the question is whether the IT Act has at all been effective in checking cyber crime. The government had enacted the IT legislation in 2000. The IT (Amendment) Act came into force in 2009 and was aimed at facilitating e-governance, preventing cyber crime and fostering security practices within the country.The IT (Amendment) Act, 2008, made almost all cyber crimes, barring a couple, bailable offences. The focus was more on enhancing the quantum

[9] Business Standard, January, 19, 2015; last updated at 13.33IST.

[10] Ghosh Dwaipayan, ‘Kolkata tops cyber crime table’ | TNN | Oct 29, 2015.

of civil liability and reducing the quantum of punishment, for which the number of cyber crime convictions in India is still not remarkable. The amendments made to the act in 2008 have covered a lot of cyber offences but considering the modus operandi in these crimes and in clarifying certain specific crimes against women and children, the Act remained ineffective and inadequate. Without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction is a difficult proposition.

Netiquettes- Ethics in Computer Usage

Netiquette is a set of rules (mainly unwritten) to follow while you are on-line. These rules have sort of evolved and exist to make the Internet a safe and secure place. While these are not carved in stone – you may become unwelcomed if you deviate too far from them. This term 'Netiquette' is coined for either 'network etiquette' or 'Internet etiquette'. 'The more power you have, the more important it is that you use it well'. (Rule 9- Don't abuse your power)[11].

Netiquette is a set of rules (mainly unwritten) to follow while you are on-line. These rules have sort of evolved rules and exist to make the internet a safe and secure place. This term 'Netiquette' is coined for either 'network etiquette' or 'Internet etiquette'. (Virginia, Shea: 'Netiquette': Albion Books, 2010)

- Help the Newbies: share your knowledge with the 'Net Newbies' on mailing list, in chat rooms, safety over the net, Face book postings, web browsing, unsolicited sites, on many more such Internet connected issues.

[11] Virginia, Shea: 'Netiquette': San Francisco, lbion Books, 2010, ISBN 0-9637025-1-3

- Research before asking: check the ‘Frequently Asked Questions’ files for any doubts lurking in your mind. Search the Internet; search the newsgroups for the answer to a question before sending e-mail to a human being. Never venture out in the Computer Space as a novice. Ask questions, Google will answer.
- Remember Emotion: Do not use capitals unnecessarily in e-mails, it designates shouting, and is considered rude. If you want to emphasize a word, use stars or underlines sparingly. Remember that subtle emotions and meanings do not transmit very well over e-mails. Be particularly polite when disagreeing with others or else you may become victim of ‘hate mails’
- Do not publicise others’ e-mail addresses: Do not distribute others e-mail addresses to strangers or by posting messages to the Usenet, unless the e-mail is on a public work and meant for distribution. Otherwise you may be responsible for getting spam e-mails from commercial sites, and strange mails from unwanted strangers
- Never Send What You Do not Read: Never forward an e-mail you haven’t read, or send someone an attachment you have not examined. For many undiscerning users it has been a huge embarrassment as the attachment turned out to contain information they really shouldn’t have forwarded.
- Respect Copyright: It is easy to copy something from the Internet and put it in e-mail or on a web page and give the impression that it is your work. Always cite references
- Respect other people’s bandwidth. Others time is not your time.
- Adhere to the same standards of behavior online that you follow in real life, so be ETHICAL.
- Be your own Policeman. No one can control your E- habits it is only YOU.

Finally being safe in the Computer Space is in our hands. Better to be safe than to be sorry.

Maintain a standard of ethics and safeguards for yourself:

- **Don't open email attachments unless you're expecting them.** Many viruses are attached to email messages and will spread as soon as you open the email attachment. It's best not to open any attachment unless it's something you're expecting.
- **Use a firewall.** Windows Firewall (or any other firewall) can help alert you to suspicious activity if a virus or worm attempts to connect to your computer. It can also block viruses, worms, and hackers from attempting to download potentially harmful programs to your computer.
- **Use your browser's privacy settings.** Being aware of how websites might use your private information is important to help prevent fraud and identity theft. If you're using Internet Explorer, you can adjust your Privacy settings or restore the default settings whenever you want.

Projects like India, Central, National Counter Terrorism Centre (NCTC) Of India, National Intelligence Grid (Nat grid) Project of India, National Critical Information Infrastructure Protection Centre (NCIPC) Of India, etc must be managed not only in a Techno Legal Manner but also in a Constitutional Manner. At the same time government of India must ensure a Strong and Effective Legal Enablement of ICT Systems in India. Solutions are possible with active intervention of government.

Select Bibliography

1. Belapure, Sunit & Godbole, Nina(2011),Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, New Delhi, Wiley India, ISBN: 978-81-265-2179-1
2. Cavazos, Edward and Morin, Gavino,(1994) Cyberspace and the Law Your Rights and Duties in the On-Line World, MIT Press eBooks, ISBN: 9780262303545
3. Chander, Harish(2012),Cyber Laws and IT Protection, PHI Learning ISBN-13: 978-8120345706
4. Chaubey, Manish Kumar, (2013), Cyber Crimes & Legal Measures,New Delhi, Regal Publications, ISBN: 978-81-8484-228-9
5. Cooper , Jonathan, (1998), Liberating Cyberspace: Civil Liberties, Human Rights & the Internet: Turtleback Books
6. Döring, N.,(2000), Feminist views of cybersex: Victimization, liberation, and empowerment. Cyber Psychology & Behavior.
7. Dr. Dasgupta M., (Reprint 2014), Cyber Crime in India - A Comparative Study , New Delhi, Eastern Law House,ISBN : 9788171772773
8. Foucault, M., (1980)Power/knowledge: Selected Interviews and Other Writings, 1972-1977. New York, NY: Pantheon Books,.
9. Funell, Setven;(2010) ‘Cyber Crime; Vandalizing the Information Society, London, Addison Wesley.

10. Griffiths, M. D.(1998), Internet addiction: does it really exist? in J. Gackenbach (Ed.), Psychology and the Internet: Intrapersonal, Interpersonal and Transpersonal Applications (pp. 61-75). New York, NY: Academic Press.

11. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

12. Jain, Atul,(2005), Cyber Crime: Issues Threats and Management (2 Vols), New Delhi, Isha Books, ISBN 13: 9788182051065

13. Moore, R., "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing, 2005.

14. Naveed, Shazib, (2013), Internet Usage & Task Preferences Part 1 A perspective with gender differences LAP Lambert Academic Publishing, ISBN: 978-3-659-40587-7

15. Spinello, Richard, Cyber ethics(2009), Morality and Law in Cyberspace, Jones & Bartlett Publishers

16. Spitzberg, B. H., & Hoobler, G., (2002)Cyberstalking and the technologies of interpersonal terrorism. New Media & Society.

17. Thomas. D. and Loader, B. D.,(2000) Cyber Crime Law Enforcement, Security and Surveillance in the information Age, London and N. Y. Routledge.

18. Vikas, Pareek, Cyber Crime in Indian Context,(2013), LAP Lambert Academic Publishing Cyber Crime in Indian Context, ISBN-13 9783659502583

19. Virginia, Shea (2010) ‘Netiquette’: San Fransisco, Ibion Books, ISBN 0-9637025-1-3

20. Viswanathan , Aparna, (2012)Cyber Law, Lexis Nexis,ISBN: 9788180387395

21. Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials. Addison-Wesley. P.* 392. ISBN 0-201-70719-5