Shrimati Das

Nehru College & Post Graduate Center, Hubli, Karnataka

Cyber Crime and Cyber Ethics:

Staying Safe and Enabled in the Cyber Space

Prelude:

This updated research paper is the outcome of a project undertaken by the author as the Project Director for a major survey and study under the aegis of the National Commission for Women (NCW), Government of India, New Delhi and Karnataka State Police (KSP), Bangalore.

The author deems it her privilege for having presented this paper as an invited keynote addresser at the Global Lecture Series at Northern Kentucky University (NKU), USA in 2011 and Universitas Gadjah Mada, Yogyakarta, Indonesia in 2012. This talk has been delivered at many universities and colleges across India, particularly addressing the girl students and lady faculty members, including Sarojini Naidu College for Women, Dum Dum, Kolkata in January 2014.

Introduction:

Money, Wealth, Leisure, Success, Happiness … these are the components of a dream, which every individual seeks to grab. But alas! Modern day dreams seems to have gone sour with the seen, unforeseen forces of Cyber Crime menace all around us, many times questioning the very basic need of humanity-‘safety’. But again we are a generation, which knows how to turn the lemons into lemonade. Taking the Cyber Crime bull by the horn a need for empowering the women and girls towards the use and misuse and the possible dangers lurking at every corner of Cyber Space and in its operation, arose through a ‘mission critical’ study and survey involving the southern states of India.

The Information and Communication Revolution (ICR) now under way through out the world is challenging the established institutions and practices in a manner difficult to comprehend for ordinary folks. The technological developments have made the transition from paper to paperless transaction possible. A new standard of speed, efficiency and accuracy in communication, has become key tools for innovations, creativity and increasing overall productivity. Computer use is increasingly spreading and more and more users are connecting to the Internet.

The growth rate of Internet exceeds that of any previous technology. Measured by users and bandwidth, Internet has been growing at a rapid rate since its conception, on a curve geometric and sometimes exponential. Today, the Internet has grown in three different directions: size, processing power, and software sophistications, making it the fastest growing technology human kind has ever developed. The Internet is universally empowering in which everyone can participate.

The Internet is a common area, a public space like any village square; except that it is the largest common area that has ever existed. Anything that anybody wishes to say can be heard by anyone else with access to the Internet and this worldwide community is as large and diverse as humanity itself. Therefore, from a practical point of view, no one community’s standards can govern the type of speech permissible on the Internet. Information wants to be free, and the Internet fosters freedom of speech on a global scale.

If we believe that there is an inherent value in truth, that human beings on average and over time recognize and value truth, and that truth is best decided in a free market place of ideas, then the ability of the Internet to promote freedom of speech is very important indeed.

Irrespective of the medium of speech used, Internet growth is mind-boggling. English language remaining forehead of other languages in the world:

Top Ten Languages Used – Number Of Internet Users By Language:

Languages	Internet Users by Language	% of all Internet users	World Population- Estimate for Language
1. English	313 million	30%	1-1.3 billion
2. Chinese	132 million	13%	1-3 million
3. Japanese	86 million	09%	128 million
4. Spanish	81 million	08%	430 million
5. German	57 million	06%	96 million
6. French	41 million	04%	381 million
7. Korean	34 million	03%	74 million
8. Portuguese	33 million	03%	230 million
9. Italian	29 million	03%	59 million
10. Russian	24 million	02 %	144 million

(Source: www.livinginternet.com)

The Internet is changing the way we live. Internet use is increasing rapidly, a trend that shows no signs of diminishing. At home and on the job, we use the Internet to conduct many of our daily activities. According to the National Science Foundation, the amount of time an average person spent on the Internet increased from 15 hours per year in 1995 to 160 hours a year in 1999. The two, where and why of Internet use reveal some interesting details. For example a survey conducted by research centers at Rutgers University and University of Connecticut, USA found that employees who used the Internet on the job spent one- fourth of their time of work online or 2 hours out of typical 8 hours a day.

Internet use varies by age. A survey of the southern states in India undertaken as part of NCW project shows the Use of the Internet was lowest among older age groups. 1/4 of people's aged 55 to 64 used the Internet. The 65 to 74 year old group had an even lower use rate at 10%. Finally, the 75 and older age group had the lowest rate, about 4%. Not surprisingly, the data show higher Internet use among younger people. Those aged 18 to 24 had the highest use rate in 2012 at 85%. Individuals between ages 25 and 34 had the second highest use rate, at more than 62%. The 35 to 44 year old group had the next highest use rate, almost 55% close behind them, the 45 to 54 year old group had a use rate of 49%. The youngest group, those aged 3 to 17 had a use rate of 40%.

The relatively high Internet use rates for younger people are attributable, in part, to their early introduction to the Internet. Contrary to expected belief that women are a large part of the IT workforce in three Southern states in India, women are less familiar and comfortable with computers because of a lack of exposure or formal training and thus are more prone to be victims of Internet related crimes. As most of the IT workforce are drawn from the rural areas the computer knowledge was found to be sketchy, giving rise to being vulnerable in cyber space operation.

The Internet capabilities are continually expanding, making many of the daily tasks faster, cheaper and more prone to all kinds of exposure to wanted and unwanted sights. Even the use of receiving and sending e-mails has increased very significantly in recent years. In 1998, 78% of persons with Internet access at home and 54% with access outside the home used it to send e-mail, making this the most common Internet activity. Searching for information was the second most popular use of Internet. Almost 60% of those with Internet access at home and 50% of those with access outside the home used it to search for information.

But the Internet is also a source for almost anybody to access, manipulate and destroy other's information. The rapid development of Internet and computer technology globally has also led to the growth of new forms of trans national crimes especially those that are Internet related. These criminal activities directly relate to the use of computers, specifically illegal trespass into the computer system of database of another, manipulation of theft data, or sabotage of systems and data.

The miniaturization of the world is because of 'connectivity' and 'communication'. The burgeoning of the world information technologies has however a negative side; it has opened the door to anti social and criminal behavior; computer system offer the potential to commit traditional types of crimes in non traditional ways called 'Digital Crime'; 'Cyber Crimes' ' Electronic Crime'.

Cyber Crime is the latest type of crime, which affects many people worldwide. It refers to criminal activities taking place in computer networks, knowingly or intentionally access without permission, alters damages, deletes and destroys the computer network. The enormity of Cyber Crime is incomprehensible. It is extremely difficult to determine when the first crime involving a computer actually occurred. The computer has been around since the abacus, which is known to have existed in 3500 BC in Japan, China and India.

In 1801 profit motives encouraged Joseph Jacquard, a textile manufacturer in France to design the forerunner of the computer card. This device allowed the repetition of series of steps in the weaving of special fabrics. So concerned were Jacquard's employees with the threat to their traditional employment and livelihood that acts of sabotage were committed to discourage Mr. Jacquard from further use of technology. A computer crime had been committed.

What is Cyber Crime?

Cyber Crime is a broadly used term to describe criminal activity committed on computers or the Internet. Some of it is punishable by the laws of various countries, where as others have a debatable legal status. The term 'Cyber Crime' is a misnomer. This term has nowhere been defined in any statute/act passed or enacted by the Indian Parliament. (The chief legislation regarding Cyber Crime in India is IT Act 2008, but also in this Act the word 'Cyber Crime' is not used) The concept of Cyber Crime is no radically different from the concept of conventional crime. Both include conduct whether act or omission, which causes breach of rules of law and counter balanced by the sanction of the state. Cyber Crime is an evil having its origin in the growing dependence on computer in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications.

The term 'Cyber' prefix derived from 'cybernetics', used to describe the entire range of things made available through the use of a computer. For example: 'Cyber phobia' is an irrational fear of computers, cyberspace is the virtual 'non-physical' space created by computer systems, and 'Cybernation' is the use of computers to carry out and maintain operations such as in manufactures.

Life is a mixture of good and evil. So is the Internet. For all the good it does us, Cyber space has its dark sides too. Unlike conventional communities though, there are no police men patrolling the information super highway, having it open to everything from Trojan horses and viruses to cyber Stalking, Pornography, Morphing, Cyber Terrorism and Trade Mark Counterfeiting.

Cyber Crimes can be mainly classified as:

Traditional crimes committed on or through the new medium of the Internet. For example:

* Cheating, fraud, misrepresentation, defamation, pornography, thefts etc.; committed on or through or with the help of the Internet, would fall under this category

- New crimes created with the Internet itself, such as hacking and spreading virus
- New methods used for commission of old crimes. For e.g.; where hacking is committed to carry out cyber frauds, prostitution through trafficking of women and children, drugs, and other prohibited articles

Characteristics of typical Cyber Crimes:

- The weapon with which Cyber Crime is committed is technology. Cyber Crimes are the work of technology and thus cyber criminals are technocrats who have deep understanding of the Internet and the computers.
- Cyber Crime is extremely efficiently committed i.e., it takes place in real time. It may take seconds or a few minutes to commit cyber frauds by hacking.
- Cyber Crime knows no geographical limitations, boundaries or distance. A cyber criminal, in one corner of the world can commit hacking on a system in another part

of the world. For e.g.; a hacker in the US can in real time hack a system placed in Japan.

- The act of Cyber Crime takes place in the cyber space, which makes the cyber criminal to be physical outside cyber space. All the components of cyber criminality, from preparation to execution take place in the unseen cyber space, making it virtually invisible.
- Cyber Crime has the potential of causing harm and

  injury, which is of an unimaginable magnitude.
- It is extremely difficult to collect evidence of a Cyber Crime and prove the same in the court of law, due to the anonymity and invisibility of cyber criminal and its potential to affect in several countries at the same time, which are different from the place of operation of the Cyber criminal.

Indian Scenario:

Cyber Crime is a global phenomenon. With the advent of technology, Cyber Crime and victimization of women are on the rise in India in particular and it possesses a major threat to the security of a person as a whole. Even though India is one of the very few countries in the world to enact a law, IT Act 2000 was formulated to combat Cyber related crimes, but issues regarding women and her safety in the cyber space still remain untouched and unexplored in this Act. Though some efforts have been made in the redesigned IT Act-2012, there still exist many grey zones for action and clarification. 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 covered fully 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 does not mention any crime specifically as against women and children.

Amongst the various Cyber Crimes committed against women and girl child, the following need our attention immediately to address the issues:

a) Harassment Through Emails: This is not a new concept. It is very similar to harassing through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via emails. E-harassments are similar to the letter harassment but create a problem quite often when posted from fake IDs.

b) Cyber Stalking: This is one of the most talked about net crimes in the modern world. There are three primary ways in which Cyber Stalking is conducted: E-mail Stalking; Internet Stalking; Computer Stalking. The Oxford dictionary defines stalking as ‘pursuing stealthily’.

Cyber stalking involves following a person’s movement across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms visited by the victim, constantly bombarding the victim with emails, etc.

According to a survey (WHOA (haltabuse.org) Comparison statistics-2012) on Cyber stalking cases conducted for the period of 2010-12, majority of the cases (75%), the perpetrator were male and the most preferred mode of perpetration is through e-mail (38%) followed by message boards and Usenet (17%) and chatting (10%). Generally the Cyber

Stalker is known to the victim (48%)and in this there will be good number (35%) can be his/her ex. In most cases the cyber Stalking escalated online (64%) but only in 30% cases it comes in offline state. Single persons are more likely to be victim of Cyber Stalking (35%) and in the age group of 18-30(47%).

Given the enormous amount of personal information available through the Internet, a Cyber Stalker can easily locate private information about a victim with a few mouse clicks or keystrokes. (Fisher, B.S.F.T. Cullen, J.Bellnap, and M.G.Turner,"Being Pursued: Stalking Victimization in a National Study of College of Women"). It is estimated that there are about 2,00,000 real – life stalkers in America today. Roughly one in 1,250 persons is a stalker- and that is a large ratio. Of course, no one knows the truth, since the Internet is such a vast medium, but these figures are as close as it gets to give statistics. Out of the estimated 79 million population worldwide on the Internet at any given time, we could find 63,000 Internet stalkers travelling the information superhighway, stalking approximately 4,74,000 victims. The estimate in India is not yet documented, as Cyber Stalking is not being reported yet due to public ignorance and no laws to govern such a crime though Section 503 of the Indian Penal Code can be used to deal with a section of this Internet crime. Also IPC Section 509 is sometimes cited to punish the offenders of stalking. The gravity is yet to be comprehended.(Source: 'The Cyber Angels', a not-for-profit organization that assists victims of CC, including Cyber Stalking)

c) Cyber Pornography: This is yet another threat to the female netizens. This would include pornographic websites, pornographic magazines produced using computers, (to publish and print the material) and the Internet to download and transmit pornographic pictures, photos, writings, etc. There is no doubt that sex sells and sells extremely well. It is evident from the fact that the pornography industry is larger than the revenues of top technology companies combined: Microsoft, Google, Amazon, e-Bay, Yahoo! And the likes (Source: toptenreview.com) According to Internet Filter Review report of 2012, there are 88 million requests sent by the Internet users to the biggest web browsers (Yahoo! Google) everyday. They are searching for pornographic websites. There are around 1.5 million downloads of photos or movies of illicit content monthly all over the world. 98 million people visit porno sites yearly. Where is a demand there is a supply. There are 6.2 million of IP addresses offering access to over 472 million porno sites. This is a huge industry. According to some estimates, the whole porno business is worth around 87 billion of US $ affecting 3% of world female population (For more statistics of pornography visit www. Internet-filter-review; toptenreview.com)

Pornography - Time Statistics:

Every second- $ 5,075.64 is being spent on pornography

Every second- 48,258 Internet users are viewing pornography

Every second-572 Internet users are typing adult search turn into search engines

Every 39 minutes- a new pornography video is being created in the United States

(Source: Funell, Setven; ‘Cyber Crime; Vandalizing the Information Society”,London, Addison Wesley,2010)

In India, Hicklin’s test has been adopted by the Supreme Court in a leading case of Pornography of Ranjeet. D.Udeshi vs State of Maharashtra.(AIR1965 SC 881)This case has decided many issues pertaining to Cyber Obscenity. In another case in India Samaresh Bose vs Amal Mitra (AIR 1986 SC 967)held a new definition of Cyber Pornography. Section 67 of IT Act deals with obscene and pornographic material on Internet.

d) Cyber Defaming: Cyber trot including libel and defamation is another common crime against women in the net. This occurs when defamation takes place with the help of computers and/or the Internet. For e.g.: someone publishes defamatory matter about someone on a website or sends emails containing defamatory information to all of the person's friends.

e) Morphing: This is editing the original picture by unauthorized user or fake identity. It was identified that, fake users and again re-posted/uploaded on different websites download female pictures by creating fake profiles after editing it.

f) E- mail spoofing: A spoofed email may be said to be one, which misrepresents its origin. It shows its origin to be different from which it actually originates. A review in the CyberLawtimes.com shows that India has crossed the danger mark in Cyber Crime targeting women and children.

g) Crimes related to mobile phones:

This technology is the 'new playground for Cyber criminals'.

- SMS Spoofing:

It is like e-mail spoofing, which looks to originate from one acquainted number but in reality it is spoofed, and sent from some evil minded individual. We can take this by an example. Suppose if a woman receives a Short Messaging Service (SMS) in her cellphone in the middle of the night from the mobile of her spouse asking her to bring cash as he has met with an accident. The chances are that she would check the mobile number and if she confirms the cell is her husband's then she would rush out with the cash. If this could be the response then the chances are that she is not aware of 'Mobile Spoofing'. Using a web-based software, a Cyber criminal could send anyone a message from any person's cell without even touching his mobile. And no cellular service provider can say that it was a spoofed or faked one. Women have been countless times the victims of such Cyber criminal activity. Unless there is cooperation between website owners and the administrators of message servers it is very difficult to detect the perpetrators of such crime.

- MMS (Multimedia Messaging Service).

This involves the option of sending photographs, sound clips, or even movie clips along with the message. The MMS service was basically meant for use to interact more lively with friends, family and relatives, but it was used by a large number of people to send porno clips from one mobile to another. Service providers use this facility along with 'Voice Chat', a 'Find a Friend' service that allows one to look for like-minded companions. Women and adolescent girls are very easily prone to become victims of this crime. The famous scam of reputed Public School of Delhi that was in news recently involves the use of MMS. The clip, which was made, was distributed by the accused to his friends via MMS, which soon reached the market.

Talk, text, music, photos, Internet, print, are just the beginning of the newer killer applications that are being added onto a mobile handset. Convergence has truly become the new mantra for the mobile industry. The mobile subscribers in India has a huge base of 236 million users and this also is a very fertile space for cyber related unwanted forays and victimization of unguarded users.

Social Networking/Online friendship Websites:

A social networking site is an online location where a user can create a profile and build a personal network that connects him or her to other users. In the past 5 years, such sites have rocketed from a niche activity into a phenomenon that engages tens of millions of Internet users. A great debate has ensued about the potential risks posed when personal information is made available on such a public setting.

A survey (Parents and Teens, 2010 Survey, data from October 23-November 19th 2010, Princeton Survey Research Associates International for the Pew Internet & American Life Project, 12/01/10) was conducted among a random national sample of youths ages 12 to 17 asked about the ways that teenagers use these sites and their reasons for doing so. A great surprise was that the survey found out older teens, particularly girls, are more likely to use these sites. For girls, social networking sites are places to reinforce pre-existing friendships, while for the boys who use the sites; the networks provide opportunities for flirting and making new friends. Girls (89%) are somewhat more likely than boys (79%) to post comments to a friend’s profile page or ‘wall’. 7 out of 10 (70%)online girls 15-17 have a profile on social networking site, compared with 57% of older boys.

My Space dominates the social networking world; nearly 85% update a profile on Facebook. More than 70% of teenage girls in India are also Facebook users. It is this segment which is prone to Cyber related perils and exposure. From the analysis of position and crimes due to such open revelation of personal information, these types of networks are here to stay, and they are embedded now in our daily existence. Wishing them away will not keep our youngsters safe, only Capacity Building through SAM (Sensitization/Awareness/Motivation) will create a safe and secure environment for them to operate in this multi specialty, super energized world.

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’. (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, Facebook postings, web browsing, unsolicited sites, on many more such Internet connected issues.

- 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’

- People aren’t organizations: Many people send e-mails from their work e-mail accounts because that is the only e-mail account they have leaving the space open to hacking and office data theft

- Do not publicize 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.

Remember: ‘Character is what you do, when no one is watching YOU.

References are all within the body of the text.