CYBER CRIME AND VULNERABILITY OF WOMEN

DR. SOMA GHOSH
PRINCIPAL
Hiralal Mazumdar Memorial College For Women
Dakshineswar, Kolkata - 700035

Prelude

There is a phenomenal growth in the Cyber Crimes (as per Information Technology Act, 2000) in India. 'There were 4192 cyber crimes in 2013 which were 2761 in 2012. 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 were 681 and 635 crimes in Maharashtra and Andhra Pradesh respectively. In these two states there is 50 per cent rise in 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'[1]. This updated research paper is the partial outcome of a Minor Research Project undertaken by the author as the Principal Investigator under the aegis of the University Grants Commission.

Cyber crime – an introductory note

Cyber Crime and the Victimization of Women is a new and very much relevant contribution to the literature on cyber crime. It focuses on gendered dimensions of cyber crimes like adult bullying, cyber stalking, hacking, defamation, morphed pornographic images, and electronic blackmailing. These and other tactics designed to inflict intimidation, control, and other harms are frequently been committed by persons who are hardly been punished. In such a situation socially women suffer from exclusion syndrome and psychologically they also feel exclusion.

[1] Gujarat Samachar, Ahmedabad, 3 July, 2014

Cyber crime, also called computer crime, is to be defined in terms of the use of a computer as an instrument for illegal ends, such as committing fraud, trafficking in women and child pornography and intellectual property, stealing identities, or violating privacy. Identity theft and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet. Cyber crime encompasses any criminal act dealing with computers and networks, popularly known as hacking. Cyber crime, especially through the use of internet, has grown in importance as the computer has become central to education, commerce, entertainment, and government.

Norton Report 2012[2] defines cyber crime in following terms:

Social cybercrime is defined as any of the following activities on social networking Platforms:

• being harassed or bullied or had inappropriate content posted about someone,

• responding to a forged or fake message or website trying to get one's personal details, such as passwords, bank Account information (i.e., phishing),

• clicking on a link or a 'like' that takes to a blank page, or reposts itself automatically into one's account or onto his/her profile.

There are lots of other term, of which a very few has been mentioned.

The earliest victims and villains of cybercrime were the Americans, because of the early and widespread adoption of computers and the Internet in the United States. The advancement of technology has made man dependent on Internet for all his needs all over the world; simultaneously it has made people vulnerable to all sorts of criminal attacks through computer and internet network. Internet has given man easy access to social networking, online shopping, storing data, gaming, online studying, online jobs et. It has simultaneously opened a space for criminal activities. Cyber crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber crimes, India is also not far behind the other countries where the rate of incidence of cyber crimes is also increasing day by day. However, it is to be noted that such criminal activities affect both men and

[2] Norton Report 2012- now-static.**norton**.com/.../**2012**

women, but when it affects dignity or reputation of a lady, it becomes a concern of social scientists. It needs special attention because women are also frequent users of internet. Thus with the advent of technology, the rights of women in cyber space are to be recognised as important as rights of women in physical space. Women should give equal emphasis on their rights in cyber space and their related duties.

Even though the International Covenant on Civil and Political Rights in Article 17 (1) states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation;" and Council of Europe convention for cyber crimes (2001) does protect human rights to a certain extent, we observe that there are no universal codes for specifically protecting women's rights in the cyber space. Most of the cyber crimes against women happen due to lack of recognition of women's rights and zero or less laws to protect women's interest in the cyber space. In this context, a mention must be made of "Convention on the Elimination of All Forms of Discrimination against Women"[3], 1979. The primary aim of this convention was to eradicate discriminations against women and establish equality for women in the society.

Article 1 of the convention. The convention opens with firm notes on defining what 'discrimination against women' shall mean in Article 1. To quote Article 1;

For the purposes of the present Convention, the term "discrimination against women" shall mean any distinction, exclusion or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field.

Article 2 of the Convention mentions that:

[3] *Ensuring Accountability to UNSCR 1325 and 1820 using CEDAW reporting mechanisms". Gnwp.org. Global Network of Women Peace builders. November 2010. Retrieved June 5, 2014.*

States Parties condemn discrimination against women. States Parties condemn discrimination against women in all its forms, agree to pursue by all appropriate means and without delay a policy of eliminating discrimination against women and, to this end,undertake:

(a) To embody the principle of the equality of men and women in their national constitutions or other appropriate legislation if not yet incorporated therein and to ensure, through law and other appropriate means, the practical realization of this principle;

(b) To adopt appropriate legislative and other measures, including sanctions where appropriate, prohibiting all discrimination against women;

(c) To establish legal protection of the rights of women on an equal basis with men and to ensure through competent national tribunals and other public institutions the effective protection of women against any act of discrimination;

(d) To refrain from engaging in any act or practice of discrimination against women and to ensure that public authorities and institutions shall act in conformity with this obligation;

(e) To take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise;

(f) To take all appropriate measures, including legislation, to modify or abolish existing

laws regulations, customs and practices which constitute discrimination against women;

(g) To repeal all national penal provisions which constitute discrimination against women.

Types of cyber crime that are committed against women:

Amongst the various cyber crimes committed against individuals and society at large the crimes which can be

mentioned as specially targeting women are as follows: –

1. Harassment via e-mails.

2. Cyber-stalking.

3. Cyber pornography.

4. Defamation.

5. Morphing.

6. Email spoofing.

Unfortunately even though Chapter XI of the IT Act deals with the offences such as Tampering with computer source documents (s.65), Hacking with computer system (s66), publishing of information which is obscene in electronic form (s.67) Access to protected system (s70), Breach of confidentiality and privacy (s. 72), Publication for fraudulent purpose (s.74) IT Act 2000 still needs to be modified. It does not mention any crime specifically as against women and children.

Herein lays the Significance of the study:

While women benefit from using new digital and Internet technologies for self-expression, social networking, and professional activities, cyber victimization may keep them suppressed. Women may suffer more as cyber victims, which may affect their social and political life and even can make them nonassertive. Failure to stop cyber victimization of women will definitely have an adverse effect on equal participation of women in all squares of life, including their political life.

Scope of the rules of law and of conventions, related to the rights of women in cyber space, social taboos related to women's access to different social networking sites in cyberspace, require detailed analysis, combining it with the views of women in this respect. The importance of CEDAW and its execution in cyber space needs serious introspection. Laws and constitutions of countries like USA, Canada and India are also analyzed.

Various duties of women in cyber space are to be examined in-depth with a view to generate a sense of social awareness against violations of rights of women in cyber space as well as against probable misuse of these rights by tech-savvy women themselves.

As cyber space has no physical boundaries and as such, no strict rule or regulation originating in any particular geographic region can regulate cyber space as a whole, the role of the international organizations like UNO should also come under microscope.

Basic fundamental rights of human beings, such as freedom of speech and expression, right to privacy, right to live a safe life etc, prevail universally both in the physical space as well as in the cyber space in all democratic countries. But the big difference between the rights prevailing in the physical space and those prevailing in the virtual space lies in the modes of legal sanctity and justiciability of these rights. The issues of women's rights in the cyber space demand special attention of the scholars, researchers, law makers, and ordinary women largely due to the allegation that national governments, as well as of the international ones still lag far behind because of their sluggish attitudes in executing the gender equality and gender justice promises.

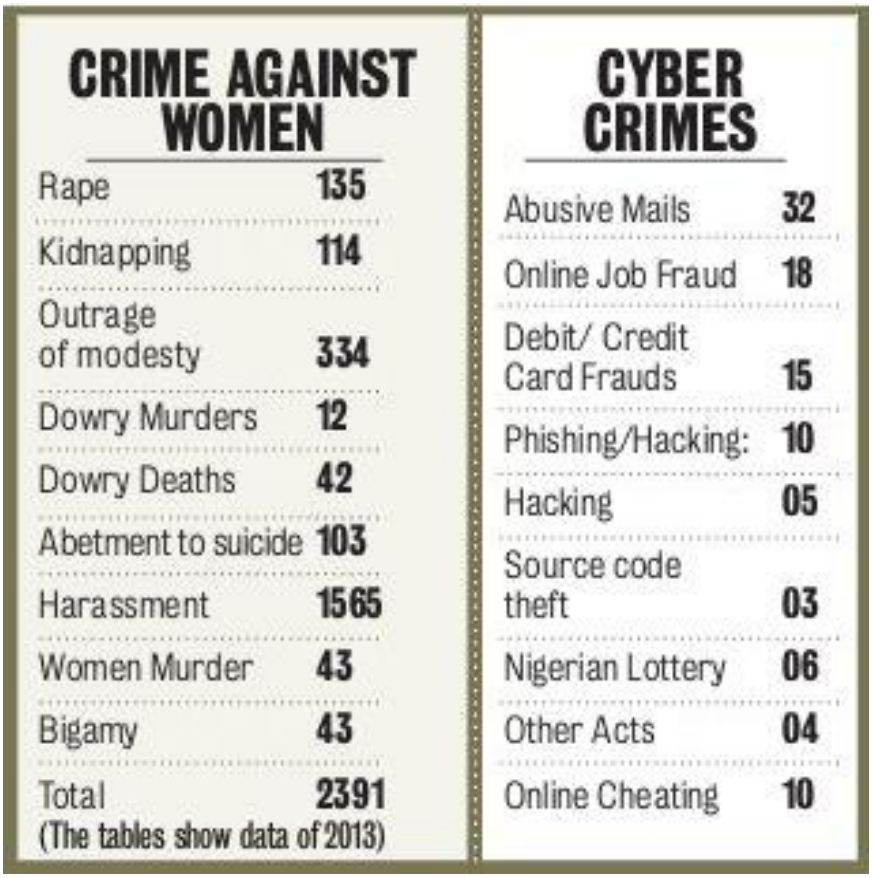
As more and more people take to the internet, cyber crimes and mobile crimes will only continue to increase at an alarming rate. However, the fact remains that Indian cyber law is still ineffective in terms of delivering appropriate cyber crime convictions. Further, cyber fraud continues to increase with dramatic force in India. 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.

Section 66A of the Information Technology Act, 2000 continues with its casual run. Various cases under Section 66A were registered in the country. In February 2013, a Palghar court closed the case against two girls who were arrested for posting a comment on Facebook on the bandh after the death of Shiv Sena supremo Bal Thackeray on November 17 last year. It was only after the Palghar case that an Advisory was issued by the Government to take the prior permission before the registration of cases under Section 66A of the Information Technology Act, 2000.

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: [4]



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)

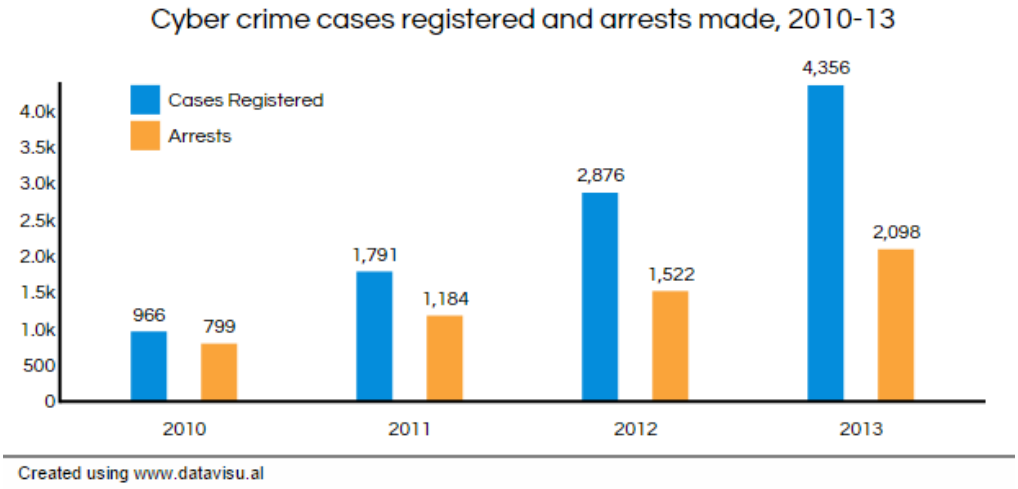
CYBER CRIMES

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

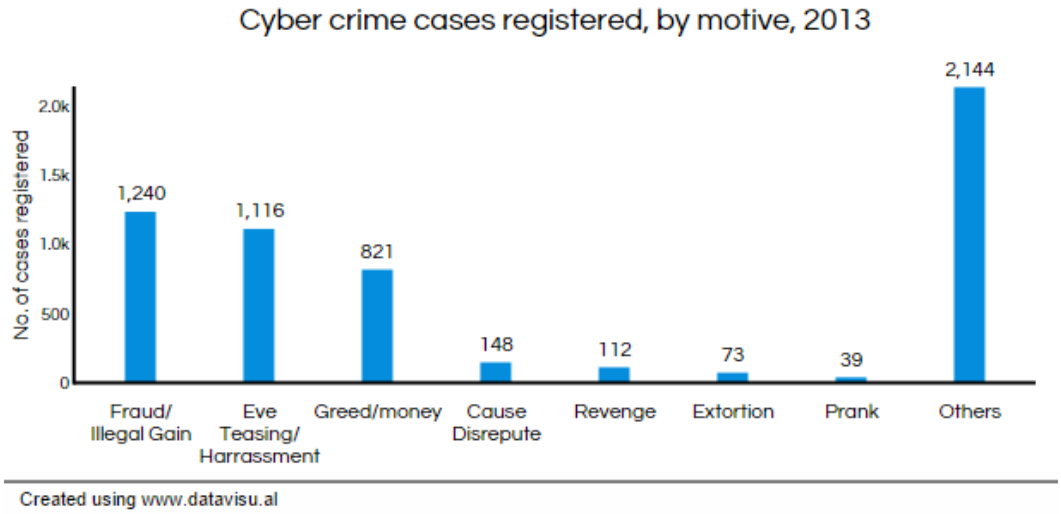
Perpetrators of such crimes can be booked under sections 66 C (which prescribes punishment for identity theft), 66A (which prescribes punishment for sending offensive messages through communication services), 66D (which prescribes punishment for cheating by impersonation) and 67 of the I.T. Act, 2000(which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

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

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.[5] Business Standard report is presented below.

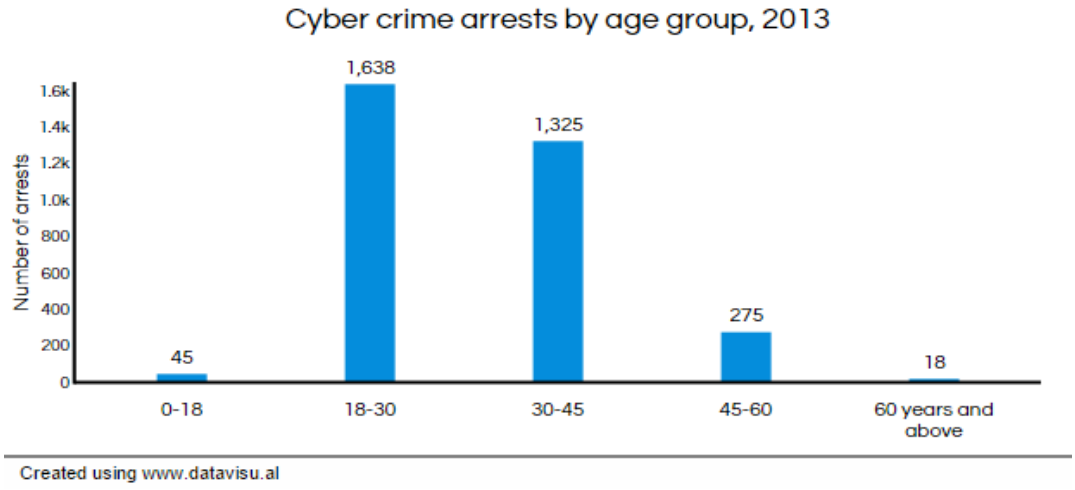


[5] Business Standard, January, 19, 2015; last updated at 13.33IST.



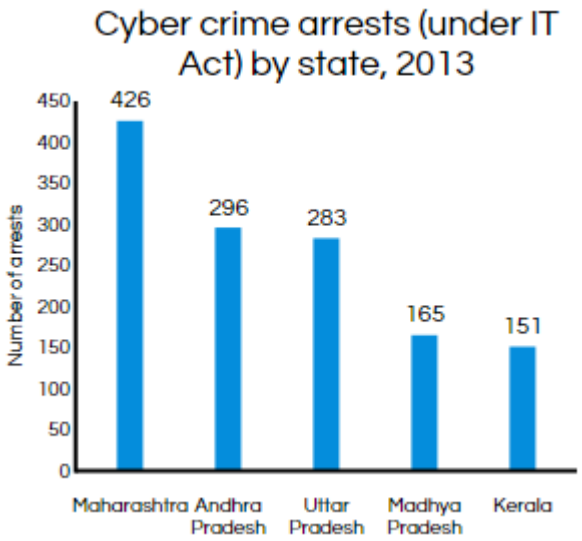
Source: NCRB

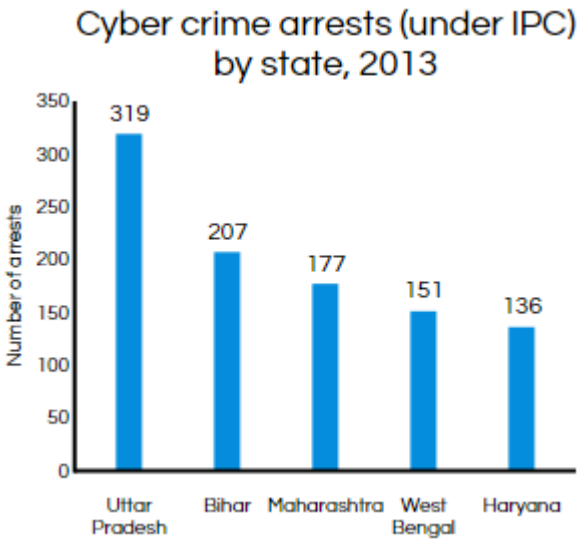
NCRB reports that incidence of cyber crime cases during 2014 in India is about 9,622.



Source: NCRB

Those who are arrested under these laws are overwhelmingly young. Data show that the age group of 18-30 accounts for the highest percentage of cyber crime with 1,638 persons arrested in the age bracket out of a total arrests of 3,301 in 2013.



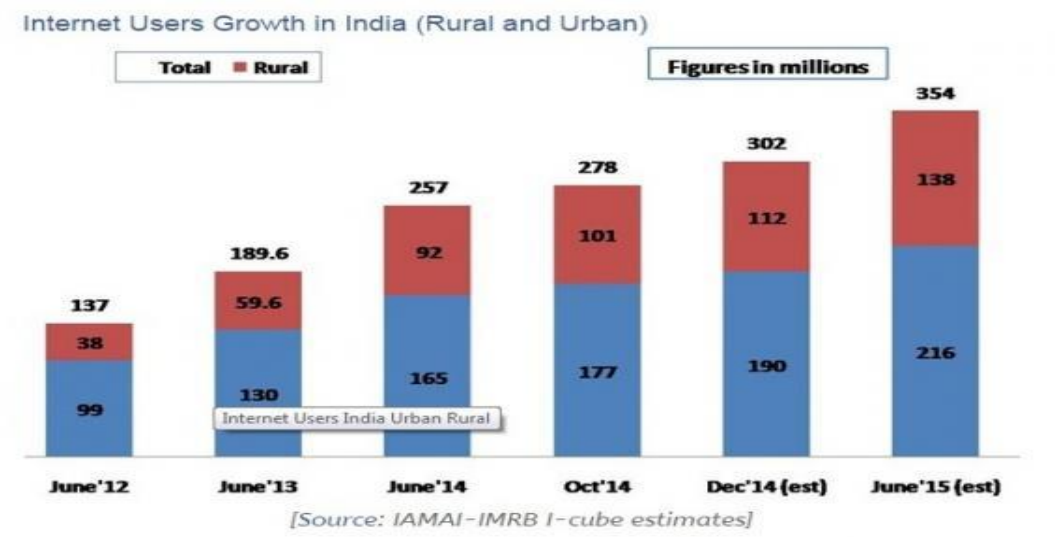


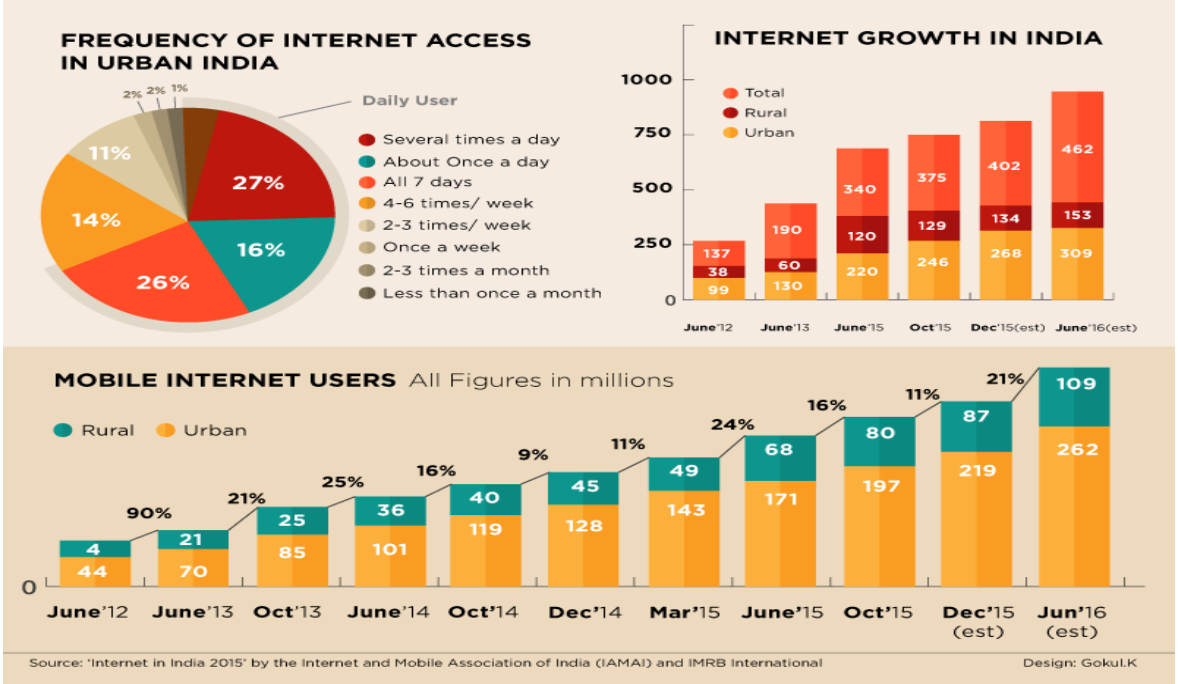
Cyber crime appears to be concentrated in states with major cities, indicating that urbanisation–and so internet penetration–is a factor. Maharashtra accounts for the most persons arrested under the IT Act, 2000, and Uttar Pradesh reported the most arrests under the older Indian Penal Code (IPC). The 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[6]. 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.

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

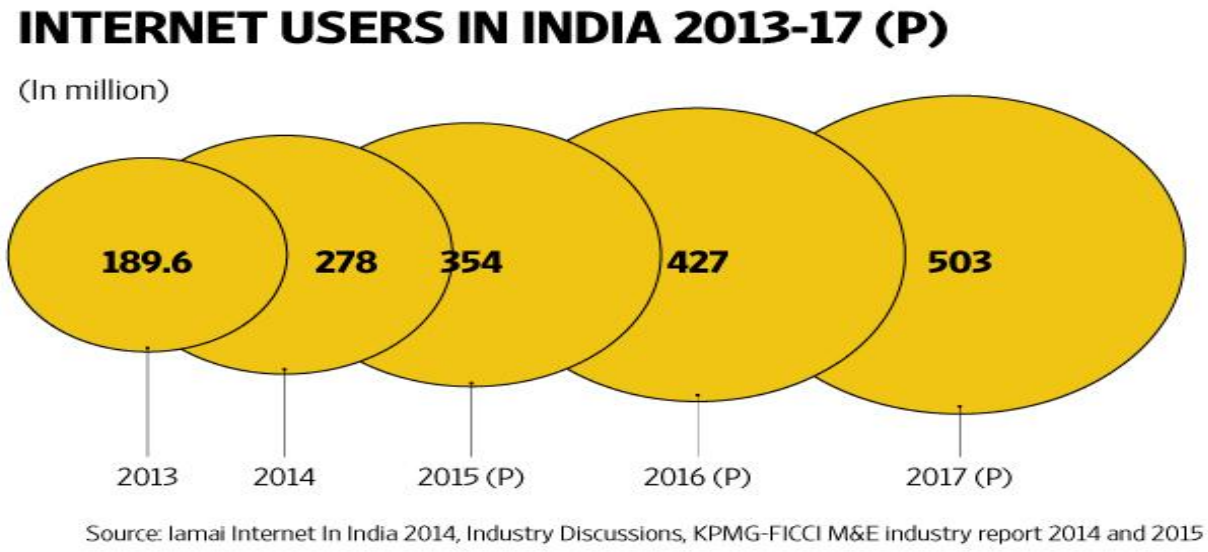
[6] Ghosh Dwaipayan, 'Kolkata tops cyber crime table' | TNN | Oct 29, 2015, 01.10 AM IST

'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. The report further states that mobile phones are fast emerging as an important point of internet access in rural India. This is just the tip of the iceberg, in the next few years, a combination of affordable smart phones and local language content is likely to lead to higher internet usage in India, empowering India with a level playing field of knowledge and information.



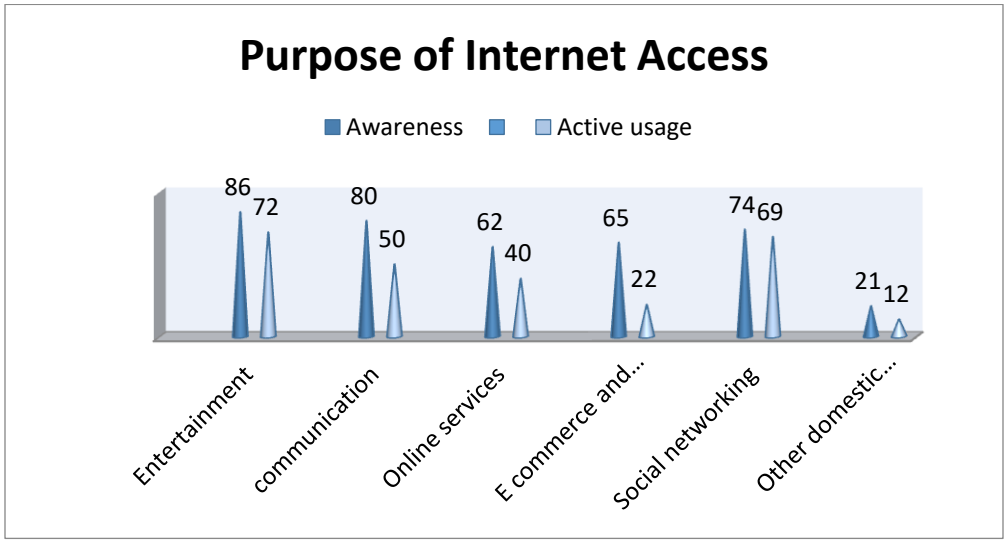
Purpose of Internet Access:

A study in some selected areas of 24 Pargans North, i.e., Barasat, Barrackpur, Baranagore, Durganagar, Madhyamgram, Dankuni, Habra, North and South Dumdum and some places in central Kolkata, like Baghbazar has detected that entertainment is the primary driver of internet use. However, there is still a difference between rural and urban areas in the nature of using internet. As per the survey report, prepared on the basis of the interview taken by the field surveyors, for 70% of the urban internet users, online communication or other services happens to be the top reason for accessing the internet on their devices. Entertainment was top priority for only 30% of these users. Among rural users, on the other hand, 62% said that their primary reason for accessing the internet was entertainment. Communication and social networking stood

at 37% and 39% respectively. After surveying the areas under Kamarhati Assembly constituency and some areas under Barrackpur Subdivision, it has come out that communication could be lower down the rankings due to a preference for offline use of services. Irrespective of rural-urban divide the survey explores following scenario.

Purpose of Internet Access:

Level of usage	Entertainment	communication	Online services	E commerce and online finance	Social networking	Other domestic needs
Awareness	86	80	62	65	74	21
Active usage	72	50	40	22	69	12



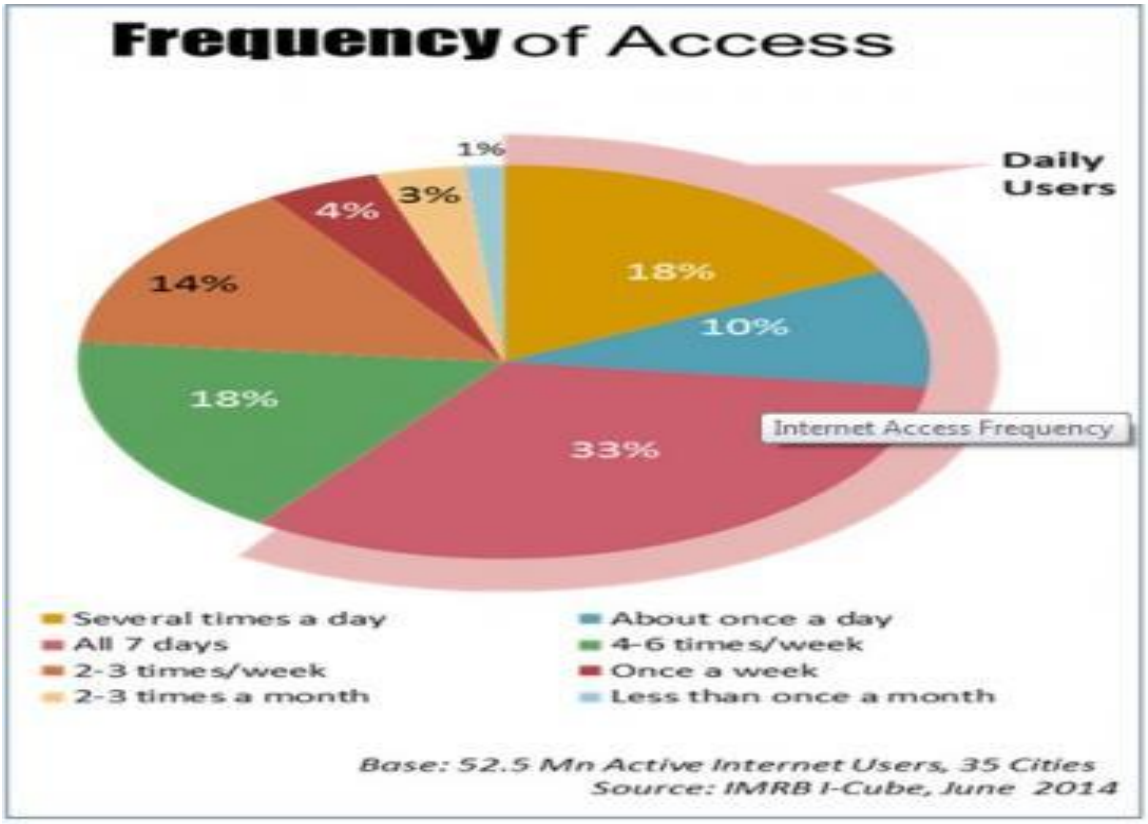
72 percent of users use internet for entertainment, like accessing Music, Videos and Photos for entertainment, while 50 percent uses it for communications; there have been 40 and 22 percent

users respectively who avail of online access for online services and online finance etc. There is a growing interest amongst the rural constituents seeking information on education. 81 percent of claimed internet users seek information pertaining to school / university and examination centres.

It is also evident that large part of internet users consider internet as a tool for male counterpart. Only 12 per cent women use internet. According to the survey report covering above mentioned areas internet user base is growing fast. But so far as the gender distribution of internet users in these areas as of March 2, 2015 to March, 2016 is concerned, only about 29% of women have been found as consistent internet users[7]. The majority of internet users were male. Primary reasons to access the internet for women are communication, social networking and entertainment. Majority of the women urban users use the internet most for communication, whereas most of the women rural users still access the net for entertainment.

On the basis of survey it has been found that frequency in accessing internet resembles mostly the IMRB report presented below:

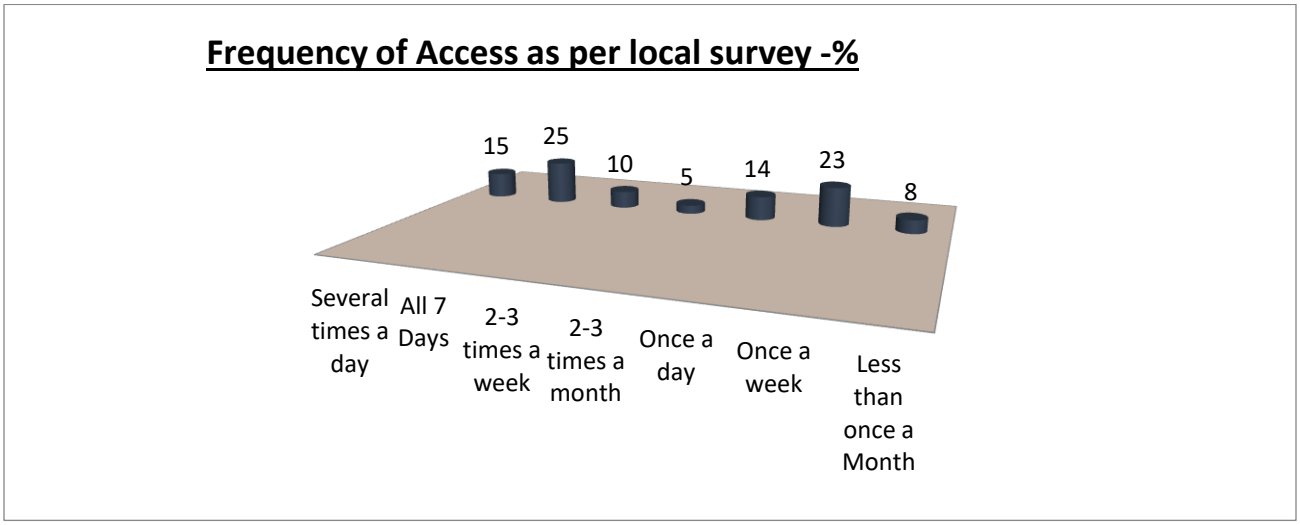
[7] Data source: Survey reports in N 24 Parganas and Kolkata Cyber cafes



Frequency of Access as per local survey

Frequency	Several times a day	All 7 Days	2-3 times a week	2-3 times a month	Once a day	Once a week	Less than once a Month

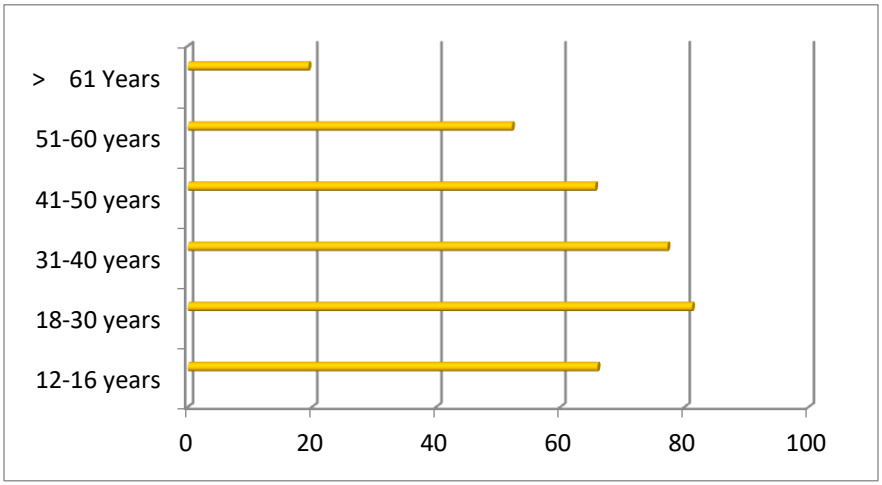
%	15	25	10	5	14	23	8



Use of Internet According to Age Group

Following statistic prepared on the basis of survey, presents information on the age distribution of internet users in India in the project years. During this period of time, 79.25 percent of internet users are between 18 and 40 years old.

Years	12-16 years	18-30 years	31-40 years	41-50 years	51-60 years	≥ 61 Years
%	66	81.23	77.27	65.63	52.23	19.45



Principal Investigator, her project assistants and surveyors have found that police are concerned by the mushrooming of internet cafes and there is little control on what people access in these places. In the suburbs, cyber cafe owners are not much bothered about restricting entry of minors too. During survey it has been observed that usually the internet is assessed through computer or laptop. However, the use of internet through smart phones is increasing at faster rate specially in semi urban and rural areas. A sub inspector under Belghoria Police station warned that they often receive cyber crime cases, though under IPC, where internet is accessed by using open/free Wi-Fi zones in malls, markets, offices, hotels, and other places. These free net zones are accessed by hackers and terrorists more frequently. This is because, many times it may be difficult to trace the users since it is openly used by anyone. By and large, such Wi-Fi zones are unsafe and it requires proper security.

What's alarming is that the trend of harassing women has flooded the CID's cyber cell and cyber crime police station in Lalbazar, said sources, while probed by the surveyors. But the problem actually lies in whether the complaints are lodged under IPC or the IT Act, a senior officer told to the PI.

The tendency to lodge cyber crime cases under IPC sections is justifiable only relating to evidence. Say for example, an SMS or an image send through a cell phone device is covered only under the IT Act and not IPC. Hacking, for example, is covered only under the IT Act and not IPC. Now gauge the fate of the case in courts if these were to be lodged under IPC," pointed out a retired OC of the cyber crime police station.

There are lots of such evidences which are admissible in a court of law under the IT Act only, said an Inspector in the cyber cell. It has been found that cases under the IT Act can only be investigated by police inspectors and above. Thus, one would need at least 113 inspectors alone for this purpose, which is highly inadequate considering the volume and number of the cases registered. The matter is to be addressed with utmost care as it is worth noting that even the number of Cyber Crime cases filed under the IPC has increased year on year, as is evident from the statistics[8] presented below , the number of cases filed under the IT Act has increased at a much greater rate.

This isn't all. These numbers have completely overshadowed the biggest cyber crime scourge - like harassing women on social networking sites and mobile devices, sending them sexually explicit content or morphing their faces etc. In West Bengal, However, targeting women through Internet and mobile phone devices have shown a higher prevalence than hacking, though Bengal is quite a long way from being the country's cyber crime capital. While visiting cyber cells under Barrackpur and Bidhannagar Police Commisionarates, it has been found that cyber Stalking is being hardly reported due to public ignorance and no laws to govern such crimes, 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.

Cyber security is very important when the use of computers, e mails and mobile phones is increasing. IT infrastructure is secure with corporates, since it is programmed internally by them. The infrastructure of use of mobile/smart phones is vulnerable to more cyber threats and needs more security. 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.

[8] NCRB REPORT,2014

Incomplete computer knowledge makes women 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. jeopardises women's safety and same applies to children also.

This study revealed that gender differences were strongest with regard to complex computer task. However, no significant differences were reported in terms of simple computer task. Males had significantly higher self efficacy expectation than females. Male respondants reported less computer anxiety and higher computer confidence than the females. A close analysis of these results of the studies shows that males have a better edge in computer literacy domain than females. Victimization of women through social networking websites is mainly because of their insufficient knowledge. Women are less aware of the privacy policies and safety tips of using networking sites. Indian women netizens still hesitate to report the cyber abuse or cyber crime. The biggest problem of cyber crime lies in the detection of modus operandi and determining the motive of the cyber offender.

Cyber crimes against women are on the raise and women have been drastically victimized in the cyberspace. Some perpetrators try to defame women by sending obscene e-mails, stalking women by using chat rooms, websites etc, developing pornographic videos where women are depicted in compromising positions mostly created without their consent, spoofing e-mails, morphing of images for pornographic content etc. The sex-offenders look for their victims on social network websites, and also on job or marriage websites where people post their personal information for better prospect. The revealing of personal information has made women more a casualty of cyber crime.

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.

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.

Pornography - Time Statistics[9]:

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

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.

[9] *(Source: Funell, Setven; 'Cyber Crime; Vandalizing the Information Society", London, Addison Wesley,2010)*

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 major section of which consists women folk, particularly homemakers(MRP survey report). A great debate has ensued about the potential risks posed when personal information is made available on such a public setting.

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)[10].

The Government of India has ordered the telecom operators and internet service providers to block 857 porn sites. The order is issued under the provisions of Information Technology Act, 2000 and Article 19 (2) of The Constitution of India. There is a view that this can be assessed in

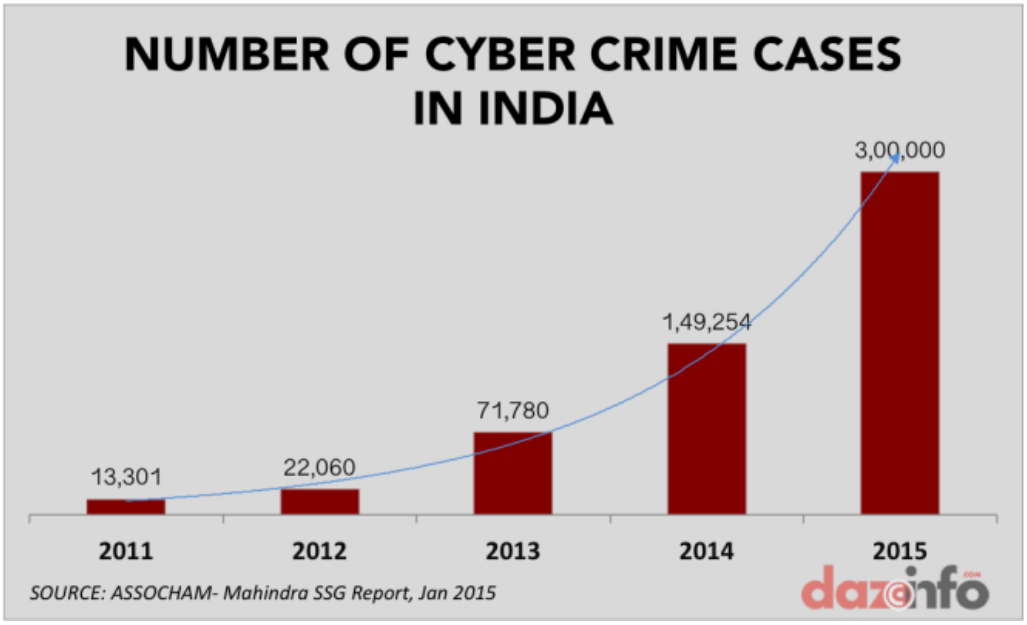
[10] *Virginia, Shea: 'Netiquette': San Francisco, lbion Books, 2010, ISBN 0-9637025-1-3*

privacy. The government is of the opinion that such things should not be viewed in public places like cyber cafes.

The Central Government is thinking to set up a Cyber Crime Coordination Centre, to which complaints relating to cybercrimes against individuals across the country will be directed for technical analysis and identification of redressal mechanism, before they are forwarded to the competent law enforcement agency for investigation.

The center will be modelled on the lines of Intelligent Crime Complaint Centre (IC 3) of US. The technical experts will look at the technical aspects of the cybercrime, including identifying the internet sites/content to be blocked before trigging a blocking request to the I T ministry. The Cybercrime coordination center will also study the laws to be invoked on the basis of the crime reported and pass on the case to the state police or CBI, as per the relevant jurisdiction, for investigation and prosecution[11].

If immediate steps are not being taken, rising at alarming rate, the number of cyber crimes in India may touch a humungous figure very soon, causing havoc in the financial space, security establishment and social fabric.



[11] (Times of India, Ahmedabad: 10 July, 2015)

Select Bibliography

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
2. Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
3. David Mann And Mike Sutton (2011-11-06). "Netcrime". Bjc.oxfordjournals.org. Retrieved2011-11-10.
4. 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
5. Spinello, Richard, Cyberethics(2009), Morality and Law in Cyberspace, Jones & Bartlett Publishers,
6. Cavazos, Edward and Morin, Gavino,(1994) Cyberspace and the Law Your Rights and Duties in the On-Line World, MIT Press eBooks, ISBN: 9780262303545
7. VIswanathan , Aparna, (2012)Cyber Law, Lexis Nexis,ISBN: 9788180387395
8. Jain, Atul,(2005), Cyber Crime: Issues Threats and Management (2 Vols), New Delhi, Isha Books, ISBN 13: 9788182051065
9. Dr. Dasgupta M., (Reprint 2014), Cyber Crime in India - A Comparative Study , New Delhi, Eastern Law House,ISBN : 9788171772773
10. Vikas, Pareek, Cyber Crime in Indian Context,(2013), LAP Lambert Academic Publishing Cyber Crime in Indian Context, ISBN-13 9783659502583
11. Halder, Debarati, Cyber Crime and the Victimization of Women: Laws, Rights and Regulations, (2011), IGI Global, ISBN-13: 978-1609608309
12. Naveed, Shazib, (2013), Internet Usage & Task Preferences Part 1 A perspective with gender differences LAP Lambert Academic Publishing, ISBN: 978-3-659-40587-7

13. Criminal Manual: Cr.P.C., I.P.C. & Evidence (with Free Guide to Criminal Pleadings - Model Forms) Hardcover – 2015 Publisher: UNIVERSAL LAW PUB CO.P.LTD.-DELHI by Universal's Legal Manual (Author)
14. Virginia, Shea(2010) 'Netiquette': San Francisco, lbion Books, ISBN 0-9637025-1-3
15. Cooper , Jonathan, (1998), Liberating Cyberspace: Civil Liberties, Human Rights & the Internet: Turtleback Books
16. Chander, Harish(2012),Cyber Laws and IT Protection, PHI Learning ISBN-13: 978-8120345706
17. 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
18. Chaubey, Manish Kumar, (2013), Cyber Crimes & Legal Measures, New Delhi, Regal Publications, ISBN: 978-81-8484-228-9

HOW DIGITAL INDIA IS TACKLING CYBERCRIME?

Ruma Saha

Assistant Professor,

Adamas University, Department of Journalism and Mass Communication

Email - ruma.saha.kolkata@gmail.com, Phone – 9433457655

Abstract

Cybercrime has extended its prowess throughout the world since its inception. India did not face the severity of its attack previously like its western counterpart as technology was still in its developing stage to transform the nation to digitally connected economy. Since 2014 onward India also advanced its footstep for more tech savvy nation where the financial transactions, records and government data are now stored on digital platform. India is moving towards the concept of e-governance and thereby opening the gateway to new form of enemies in the silhouette of cybercrime. According to IAMAI report by 2017 India is having more than 300 million internet user. [2] The penetration rate of Internet was 34.8% in 2016. [1] This shows that a huge number of people and huge amount of information are vulnerable in this cyber space. But the question arise are we still vulnerable when so many anti-virus company thrives in this market. Technology has upgraded and government data is also protected under strict surveillance but still we face the crisis like WannaCry. This article focuses on how India is capable enough to tackle cyber crime in its newly transformed digitally connected economy.

Keywords: Cyber crime, cyber security, Digital India

Introduction

Cybercrime is a crime which involves computer as the object or tool of the crime (phishing, hacking, identity theft). Cyber criminals use computer technology to get access to personal information as well as business or trade secrets, or use the internet for malicious purposes. [3] Cyber crime therefore signifies occurrence of harmful behaviour that is related to computer. It has no specific reference in law but the concept is invented by media (Wall,2003). Internet has impacted upon criminal or harmful activity in three main way. This classification has been done

to distinguish cyber crime from other crime. Firstly, internet is a vehicle of communication that assist in sustaining existing harmful activity like drug trafficking, hate speech, bomb talk, stalking and many more. Secondly, internet has created transnational environment that provide new platform for harmful activity like paedophile incident, fraud etc. Thirdly, the internet has created crime like unauthorized access to imagery, music, video, software tools etc. It has impacted both private individuals and business houses. Now the policy makers are to decide which policy is suitable for each of these crimes categorised under different level of cyber crime.[4]

The first ARPANET link was established between the University of California, Los Angeles (UCLA) and the Stanford Research Institute in 1969.[3] The first words that they send through this network was "LOGIN". At that time no one could think that internet would gain such prominence that about 48% of the world's population uses the Internet.[3] This has increased the complicacies of cyber attack many fold with its impact on half of the world population. Therefore a strong policy based on cyber ethics is required to be implemented by government of every country and also by transnational organisations like UN.

From mid-1990s onward government of India has taken e-government initiative to provide better service to the citizen. The major ICT initiatives of the government included some major projects such as railway computerization, land record computerization etc. that focused mainly on the development of information technology and systems. [5] Later on many states started implementing e-governance project to give electronic service to its citizen.

E-governance project could not make desired impact due to its limited features. E-governance project was characterised by isolated and less interactive systems, which posed as major drawback in adoption of this e-governance in broad spectrum of governance. They clearly pointed towards the need for a more comprehensive planning. Moreover, proper infrastructure is to be built in order to establish a more connected programme. As a result, government of India started the digital India programme to promote inclusive growth which covers electronic services, products, devices, job opportunities as well as transfer the entire ecosystem of public services through the use of information technology to a digital platform. [5]

In recent times, government's ambitious projects of Digital India and smart cities initiatives have already earned enough attention from heads of technology giant. But they are concerned about

the security policy to be implemented by government of India to enhance cyber security as security breaching is a regular feature now-a-days. [6] The report also suggest that the integrated digital footprint created by Digital India and digital cities will bring increasing and alarming demand for resources to defend against the threat at various level and entry point of the new system. Digital India and smart cities will create social and economic opportunities. [6] The increasing synchronisation of existing digital data and processes within government departments will require maximum security. But critical data flow is to be left uninterrupted even in this high threatening environment. [6]

This article is devoted to study the current scenario of cyber security in Digital India. Also to find out how digital India is tackling cyber crime. Issues of cyber ethics play a vital role in deciding policies made by policy makers.

Present Scenario of Cyber Crime in Digital India

Cyberspace touches every part of our daily life through wireless signals, broadband networks, local networks and even the massive grid that power our country. To create a strong defence system against cyber attack would require combined effort from both public and private sectors. Combined effort is required to develop new technologies and new approaches for maintaining real-time protection of their individual networks. Now a days as most of the business are using open source due to cost factor the cyber threat becomes more lethal for business groups. [9]

Since 2014 Indian government headed by Prime Minister Narendra Modi has taken several transformative initiatives like Adhaar, De-monetization and Digital India to add speed to India's transition from an analog to a digital economy. This is quite admirable goal and if executed properly it can jumpstart economic growth of India and creates crores of job opportunities. This goal will remain unattainable if India does not improve cyber security infrastructure. [10] Despite being IT powerhouse India's cyber security preparedness and infrastructure is far below the required level.

Recently two developments in cyber world in past few years made this scenario of unpreparedness even more dangerous. The first major development was the discovery of malicious computer worm called "Stuxnet." A group of cyber researcher had found it in 2010. Stuxnet was created to target industrial computer system. Stuxnet was different from other virus

in a way that it targeted programmable logic controller (PLC) which are not connected to the internet and previously thought to be safe from hacking. Stuxnet showed that many elements of any country's infrastructure such as water treatment facilities, hospital systems, dams, electric grids, factory assembly lines, power plant that uses PLC system and supervisory control and data acquisition system are also under cyber threat even though they are not connected to internet. It is high time for India to fortify its critical infrastructure. [10]

Second development in cyber space was the advent of another sophisticated malware named Advanced Persistent Threats (APT) in 2013. These malware perform in a different way compared to any virus. Through this malware hacker aimed at data theft and espionage. After infecting the target the malware use sophisticated root kit technique to disguise them. They connect to control servers and command on the internet. They can export data as well as take new instuction. This malware can remain undetected for months or even years while slowly collecting valuable data from victim's network. All the recent data theft incidents like Anthem, Target, Office of Personnel Management (OPM), Sony were victims of this malware attack. Government of India should think seriously regarding cyber security policy of the country. [10]

A study made by Assocham-PwC revealed that India has witnessed a 350per cent rise in cyber crime from 2011 to 2014. [11] With the spread of smartphone and internet India has emerged as one of the favourite countries to attack among cyber criminals. The Indian Computer Emergency Response Team (CERT-In) has also reported in a study conducted by them under title "Protecting interconnected systems in the cyber era" that in 2015 a rise in number of incidents of cyber attack could be noted at around 50000. [11]

Therefore, with increase in the usage of consumer technology (CT) as well as information and operational technology (OT) in critical infrastucture the threat situation is heightened. The study further noted that these vital elements have been the choice of target for attackers because they are aware of the impact of disrupting the routine way of life. [11] In USA an increase of 50 per cent is noted in cyber crime incident report against its critical infrastructure from 2012 to 2015. Victims are not only private individuals but also government and big business houses. [11]

Online news sites have recently reported in September 2016 on data breach of India's top secret file due to cyber attack. The top secret "Scorpene" submarine program was published online and this data breach has brought the issue of cyber security of India into newspaper headlines. The

cyber security firm Symantec have mentioned in its blog post on 2016 that it had traced cyber security breaches of several Indian organisations by cyber espionage group called Suckfly. [12] According to Symantec this cyber espionage group has targeted government organisations, financial institutions, large vendors to stock exchange, e-commerce companies etc. Based on the targets that the group penetrated Symantec has speculated that the espionage was targeted at disrupting the country's economic infrastructure. [12] The government authority has neither denied nor accepted of being victim of such data breach. [12]

Recently in May, 2017 world was send to edge even without losing much money as intended from the victims by a ransomware named WannaCry. Impact was heavily felt in UK where National Health Service was hard hit by stalling surgeries, calling back ambulances etc. This led the cyber experts throughout the world to think about the real time impact like this. All of us live in a digital world where destructive effect is hard to stop. [13] Researchers have observed that WannaCry is a program mainly targeting Microsoft Windows operating systems. The hacker uses this ransomware to take control of victim's computer and lock the data until the victim pay in return. The hacker demanded payment of $300 to $600 using Bitcoins. Microsoft has released cyber security to overcome this vulnerability but that will not be applicable for any pirated software. Cyber security experts were of opinion that outspread of attack would be high in India as majority of the computers are working on pirated software. [14] Some newspapers reported that Ministry of Home Affairs source had informed that Government of India had ordered to shut down the service of some ATM outlets all over the country as preventive measures against the cyber attack.[15] As far as the effects are concerned IT minister of India Ravi Shankar Prasad said that India was not affected much by ransomware WannaCry. [15] He added that ransomware WannaCry had partially affected Kerala and Andhra Pradesh.[15] Some newspaper reported of ransomware attack in parts of West Bengal. [14] Government is keeping close eye to the situation as well as improving its security system. Indian Computer Emergency Response Team (CERT-In) has recently come out with list of preventive measures to protect networks from global ransomware attack. [15]

Reserve Bank of India (RBI) has directed the banks to update the software in their ATM machines to avoid ransomware attack. [14] The attack has crippled more than 200000 computers throughout the world and affected hospital, banks, government agencies in several countries. [14] Researchers have come up with new term "cyber terrorism." Cyber terrorism is the

convergence of terrorism and cyber space. It is the use of internet to shut down critical infrastructure (electricity,bank,organisation, transport) with the purpose of coercing the people or intimidate a government. A hostile nation can exploit using these tools to penetrate poorly secured computer network and disrupt critical functions. [16]

Cyber security and policies in Digital India

What is cyber ethics?

Information Technology plays a pivotal role in every sphere in business, industry, government, medicine, entertainment, education and in society at large. The economic and social benefit gained from it hardly needs any explanation. Information technology too has negative implication in our society. This poses some problems related to ethics and generally contains three main types of ethical issues: personal privacy, access right and harmful actions. [7]
The increase in business transaction on intangible assets like Intellectual Property made cyber space an important commercial sphere. Therefore in order to extend this business, a secure cyber sphere is required. To protect intellectual property rights in online platform a strong regulatory agenda would be set and it will produce many technical methods of enforcement. Internet has turn out to become the media of the people as the internet has spread fast which initiated a change in press environment that is centred on mass media. Unlike established press there are no editors in internet; People produce content themselves and circulate it. This direct way of communication over internet created many social debates. Hence, cyberspace content demands in future a reconciliation of two views - freedom of expression and concern for community standards. [17]

Cyber laws in India:

1. Information and Technology Act, 2000 - The Information and Technology Act seeks to protect the technology and cyber space by defining crimes, laying down procedures for investigation, prescribing punishments as well as forming regulatory authority. Many cyber crimes have been brought within the definition of traditional crimes too by means of amendment

to the Indian Penal Code, 1860. The Evidence Act, 1872 and Banker's Book Evidence Act, 1891 was amended to facilitate collection of evidence in fighting cyber crimes. The IT act itself was amended in 2008 to adapt with changing cyber space. [17]

2. National Cyber security Policy 2013 – The Act was formulate to provide cyber security to growing IT industry in India but its implementation is not successfully done yet. Important features of this Act are as follows:

i. To build secure and resilient cyber space.

ii. Creating a secure cyber ecosystem, generate trust in IT transactions.

iii. 24 x 7 National Critical Information Infrasctructure Protection Center (NCIIPC).

iv. Indigenous technological solutions is to be set up,

v. Testing of ICT products and certifying them. Validated products,

vi. Creating workforce of 500,000 professionals in the field,

vii. Fiscal Benefits for businessman who accepts standard IT practices, etc. [17]

Future of cyber security in Digital India:

The government takes initiative to conducted several awarness and training programmes on cyber crimes for law enforcement body. Training is also given on the use of cyber forensic software packages and other associated procedures to collect electronic evidence from crime scene. [17] The initiative to provide cyber security and related projects are quite less in numbers. Even if there are some proposal for projects but that remained in papers only. India has launched e-surveillance projects like National Intelligence Grid (NATGRID), Central Monitoring System (CMS), Internet Spy System Network and Traffic Analysis System (NETRA) of India etc. But none of them are governed by any legal framework neither they were under Parliamentary Scrutiny. Thus, these projects are violation of civil liberties protection in cyberspace. Government has formed National Informatics Centre (NIC) to provide network backbone to manage IT services, E-GOV initiatives to state and central government. To counter cyber crime a coordination is required from different agencies working under Ministry of Home Affairs and under Ministry of Communications and Information Technology. Apart from Central Bureau of Investigation, The Intelligence Bureau, state police organizations and other specialised organizations such as the National Police Academy, there are few agencies of government which

also work for tackling cyber crime. To name few of them are : National Information Board (NIB) , National Crisis Management Committee (NCMC), National Security Council Secretariat (NSCS), Department of Information Technology (DIT), Department of Telecommunications (DoT), National Cyber Response Centre – Indian Computer Emergency Response Team (CERTIn), National Information Infrastructure Protection Centre (NIIPC), National Disaster Management of Authority (NDMA), Standardization, Testing and Quality Certification (STQC) Directorate, The Cyber Regulations Appellate Tribunal. [17]

Intergovernmental organisation and initiatives:

Various intergovernmental organisations have taken initiatives to address the issue of cyber crime at policy level.

Council Of Europe - Council of Europe aimed at protecting societies throughout the world from the threat of cyber crime through Convention on Cybercrime held at Budapest in November, 2001. It was the first international treaty to address the problem of cyber crimes that is done using internet and computers. Budapest Convention entered into force from July 2004. [18]

Internet Governance Forum (IGF) – It was established in 2006 by the World Summit on the Information Society to bring people together from different stakeholders groups for discussion on public issues related to internet. United Nation played a vital role in establishment of IGF. [19]

United Nation – The International Telecommunication Union (ITU) is the specialized wings of UN deals with information and communication of the world. They also deal with adoption of international standards to ensure uninterrupted global communications and flexibility for next generation networks. They also work for building confidence and ensure secure ICT usage. [17]

Meridian Process - The Meridian Process has set its goal in providing Governments throughout the world a platform or means to discuss on how to work together at the policy level on matters of Critical Information Infrastructure Protection (CIIP). By holding annual conference the organisation tries to build trust and establish international relations within the member countries as well as provide opportunity for sharing best practices from the world. [20]

NETmundial Conference - Brazil had hosted NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance in 2014. The meeting was held in collaboration of Brazilian Internet Steering Committee and /1Net. It is a forum that gathers international entities of various stakeholders involved with e-governance. This meeting mainly focused on elaboration of principles of Internet governance and the proposed a roadmap for future development of this ecosystem. [8]

Conclusion

The increase in the number of internet users around the world makes data security as well as its proper management very important for future growth and prosperity. The main concern is with the unauthorized people who are trying to access remote services and disrupt the system. It has become our responsibility for our own cyber security. Simple steps are to be followed to stay in secured cyber space like installing antivirus software, personal firewall and update it time to time. Also it is advisory to archive all security logs. Moreover access should be restricted to sensitive data and has to be password secured. Above all more cyber literacy related to cyber security has to be enhanced. Government can also utilise specializations of private sectors to tackle problems of cyber security and promote more PPP projects for having secured Digital India.

Reference:

1. http://www.internetlivestats.com/internet-users/india/ (Accessed on June 12,2017)

2. http://www.iamai.in/media/details/3658, (Accessed on June 12,2017)

3. Dave, D. P. H. S. S., & Patel, M. P. (2017). Organized CyberCrime and the State of User Privacy.

4. Wall, D. (Ed.). (2003).Crime and the Internet.

5. Turka, S. K., & Singh, G. (2016). Issues and Challenges of Digital India Programme in the Current Scenario. Academic Discourse, *5*(2), 76-81.

6. http://www.financialexpress.com/industry/technology/security-in-the-age-of-digital-india/91341/ (Accessed on June 13,2017)

7. Gunarto, H. (2014). Ethical issues in cyberspace and IT society. Ritsumeika Asia Pacific University.

8. http://netmundial.br/about/, (Accessed on June 15,2017)

9. http://digitalcreed.in/cyber-security-critical-for-digital-india-success/ , (Accessed on June 14)

10. http://timesofindia.indiatimes.com/people/opinion-digital-india-requires-cyber-security-investment/articleshow/57847654.cms, (Accessed on June 14,2017)

11. http://kenes-exhibitions.com/cybersecurity/blog/digital-india-cyber-security-threat/, (Accessed on June 14,2017)

12. https://thewire.in/67398/india-is-unprepared-for-future-cyber-attacks/, (Accessed on June 14,2017)

13. http://indianexpress.com/article/opinion/wannacry-attack-ransomeware-virus-patch-is-india-ready-for-the-perils-of-a-hyper-digital-world-4656925/, (Accessed on June 15,2017)

14. http://indiatoday.intoday.in/story/wanna-cry-ransomwares-impact-in-india-may-go-under-reported/1/954798.html, (Accessed on June 15,2017)

15. http://indiatoday.intoday.in/story/atms-shut-down-india-wanna-cry-ransomware-attack/1/954284.html, (Accessed on June 15,2017)

16. https://en.wikipedia.org/wiki/Cyberterrorism , (Accessed on June 15,2017)

17. http://www.insightsonindia.com/2014/11/25/cyber-security-related-issues-comprehensive-coverage/, (Accessed on June 15,2017)

18. https://en.wikipedia.org/wiki/Convention_on_Cybercrime, (Accessed on June 15,2017)

19. http://www.intgovforum.org/multilingual/content/about-igf-faqs, (Accessed on June 15,2017)

20. https://www.meridianprocess.org/, (Accessed on June 15,2017)

Cybercrimes and Matrimonial fraud

Soma Saha
Assistant professor
Department of Food and Nutrition
HMM college for women
Dakshineswar, Kolkata, West Bengal
Saha.soma14@gmail.com

Abstract - In India, online matrimonial websites play a significant role being trusted by millions of Indians globally. At the same time, these act as the playground for the fraudsters and hoodwinked duping thousands of victims by posting false and fraudulent profiles by the change of time being. All these problems are mainly due to the fact many parents arrange for marriages for their wards --secretly without being let known to their brothers and sisters. Close relatives are informed after betrothal fixed and then they used to invite into the function. At this stage, there is nothing left to take any initiative. This study will provide the data on matrimonial fraud frequently commits in the domain of cybercrime issue. It will also have an outlook in its legal recourse.

Key wards: - matrimonial websites, betrothal, fraudsters, victims

Introduction:-

Introduction:-

In the cyber age, we are about to left the traditional love marriages and arranged marriages because of the replacement of online affairs and digitally arranged marriages. Getting into relationships for a person becomes very easy by the Cyberspace. There are dating websites and matrimonial websites available online where a person simply fills in partner requirements and get a list of prospective compatible matches within a minute. The advent of relationships through the internet has changed the structure, functioning, and sustainability of relationships all over the world. Cyberspace brings many dangers platform like anonymity and lack of personal

contact, both of which are essential ingredients to healthy relationships. That is why it easy for hoodwinked to cheat and victimize.

There are many instances of fake or misrepresented Facebook/social media profiles and matrimonial profiles on online portals. Posting incorrect information about age, religion, marital status and employment status are the most common problems in online marriage portals. Nearly half of marital breakup involve partners who met online and about seven cases out of every ten that are of marriages arranged through matrimonial websites.

With the advent of online portals cyber personating made very easy to get into relationships. People can write anything on their virtual profiles without scrutiny. In May 2012, two men arrested for cheating women on online matrimonial websites with the promise of marrying them in Madurai. Most of their victims were well-educated and those who are working in the IT sector, while some were even living abroad. Their method of functioning is to make a good looking online matrimonial profile, and after establishing contact as an imminent bridegroom, they used to succor the girls through social networking chats and the mobile.

Further, they used the magic voice option on the mobile phone to pose as parents of the groom. After gaining their confidence, they used to demand money from the girls and asked them to deposit the cash in bank accounts. After collecting the money, they used to disconnect all communication with the girls and create new profiles to attract further victims. Apparently, they even blackmailed a few victims by taking semi-nude photographs of them through a webcam while chatting, to extract money from the girls.

There are many cases where people realize that they are the victims of this cyber crime after they are already married to such fraudsters when it turns out that the online matrimonial profiles of their spouse had completely fake details.

However, there is legal recourse for victims of such cheating. Section 66-D of the Information Technology Act, 2000 provides for punishment for cheating by personating by using a computer resource. This legal provision reads as under:

"Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees."[12]

This provision envisages that if a person assumes the character or appearance which is not what he is or passes oneself off as someone he is not, especially with fraudulent intent, then the victim can file a complaint before the Adjudicating Officer under this provision. A fine of up to 1 lakh Rupees will award for the victim.

The Rules under the Information Technology Act provide that the Adjudicating Officer is required to hear and decide an application in 4 months, and the whole matter has to decide in 6 months.

The online dating and matrimonial portals can also be held liable under the Information Technology Act as there are certain liabilities associated with "Intermediaries" under the Information Technology Act.

The Online Service Providers being "Intermediaries" can be held liable under Section 79 (3) (a) of the Information Technology Act, 2000 if:

"The intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act."

The matrimonial websites do guarantee suitable matches and keep emailing the same to the registered users, and also at times charge for specialized services of making correct match whereby they are presumed to have verified the credentials of the parties, thereby making them liable under the Information Technology Act, 2000.

Also, along with action under the Information Technology Act, it is advisable to simultaneously file a FIR under Section 415, 416, 417, 419 and 420 of the Indian Penal Code. All these articles deal with cheating and fraud by personating.

If you are a victim of such a cyber crime, then there is legal recourse available under the Information Technology Act against the fraudster and the Intermediary. One can directly file a

[12] https://blog.ipleaders.in/online-romance-scammers-legal-recourse-for-a-victim/, Retrieved on 08-07-2017.

complaint before the Adjudicating Officer, Ministry of Information Technology, Information Technology Act, 2000.

How to avoid matrimonial fraud:-

i. They can investigate If someone is suspicious about a profile report on the dating website or app so.
ii. Try doing your detective work – ask them for their full name and look them up on Google and social media.
iii. Don't be afraid to question their authenticity – if they are genuine, they won't mind you trying to verify them.
iv. Remember, they may spend months building a relationship with you and will only ask for money once you're emotionally involved.
v. Ask a friend for advice who are not emotionally involved as you; they may be able to see something which you can't.
vi. Look out for fake or stolen photographs.
vii. Never give out too much personal information, such as your home address, phone number or email.
viii. Consider setting up a new email address to use for online dating and perhaps even get a cheap Pay As You Go phone to use for making phone calls.

References

1. The Hindu, May 21, 2015.

2. Times of India, March 12, 2011.

3. https://blog.ipleaders.in/online-romance-scammers-legal-recourse-for-a-victim/, Retrieved on 08-07-2017.

4. http://criminalnationnews.blogspot.in/2013/03/fake-dating-sites-profiles.html**,** Retrieved on 15-07-2017.

5. http://timesofindia.indiatimes.com/city/hyderabad/Matrimonial-sites-become-a-new-crime-spot-for-con-men/articleshow/14162858.cms, Retrieved on 15-07-2017.

6. http://www.lawyersclubindia.com/articles/Fake-profiles-on-matrimonial-and-dating-websites-cyber-law-has-an-answer–6332.asp#.VCKgUvmSyRg**,** Retrieved on 15-07-2017.

Identity theft prevention: A serious challenge to high-tech world cyber security

Tamal Mondal

Assistant Professor, Department of Botany, HMM college for Women,

Dakshineswar, Kolkata-35

Email: *tamalmondal1@gmail.com*

Abstract:

In today's modern world life is become pointless without connecting to the information superhighway. Communication in the form of electronic process is under threat to loss of personal identity. This type of identity theft affects financially as well as mentally. To prevent such type of threat proper education as well as awareness in this field is necessary. A global venture is today's demand to resist from cyber identity theft.

Key Words: Identity theft, Information theft, Cyber security, Cyber crime

Introduction:

Now a day's life has become meaningless without linking to the global super highway i.e. the world of internet. Now a day's world has transformed to global village. Any information related to any field is available to us in any time at any place of the world. No doubt this type of information access reaches us a new advanced working world. But there is always a shade under the lamp. Likewise in case of open access of information there was a shade that means chances to be a victim of information theft. Information in which someone's identity is attached is called cyberidentity. This type of identity is used frequently in the Cyber world. As we all know, recently on 12th may 2017 a worldwide organized cyber attack known as Wanna Cry ransomeware attack took place in which more than 2,30,000 computers in over 150 countries infected. A bunch of Indian companies were also affected. Identity theft in such cases creates a big threat to someone's entire existence.

Significance of Cyber Identity:

A huge number of people use the Internet in their everyday lives, from buying a pin to a helicopter everything they desire. Not only buying but anything they want. They exchange their personal secure information such as credit card data, internet banking data, mobile banking data, and any type of their personal identity related data, frequently. Personal data such as banking details and passwords related to social networking information are traveling through wires, and also through the air, from one computer to another. From any time any place to any time zone in the world.

Cyber Identity theft! What is this?

Any personal information such as credit card number to banking details, social networking passwords etc that passes through this superhighway is not secure entirely. Unfortunately cyber criminals are there and they are trying constantly to steal such type of information for their benefit. Once they became successful in their mission ones all personal information comes to their hand and they can use it for their profit in any way.

Various types of Cyber Identity theft:

There are various types of identity theft from financial identity related documents such as bank balance, passwords to personal life related information such as healthcare, personal identity number, reputation.

Different techniques to steal Cyber Identity:

As the technology develops cybercriminals are engage to develop different kinds of sophisticated techniques to theft. The main techniques involves online as well as offline methods and some other types of methods to steal identity. Some of the most common types are:

Malware: It is a vast term used to describe different types of malicious software. With the help of this type of program criminals can access some ones personal computers.

Phishing: It is one of the most common types of cybercrime. In which criminals send email links look like as banks original website. Asks for ones password etc and redirects to their fake website and stole peoples online banking identity.

Spyware: It is software develops by cybercriminals which can take control someone's entire computer system and stole all the personal information.

Trojan horse: A type of malicious program which allow criminals to access someone's computer from any corner of the world. It is like the Trojan horse in the Greek mythology.

Social networking: From social networking sites criminals may get someone's various personal data.

Skimming: In this case information of credit card or debit card is recorded and transfer to a duplicate card without the knowledge of original card holder.

The above techniques are of the most common type; criminals also can steal information from homes personally or via phone call or simply via short message service (SMS).

Affects of Cyber Identity theft:

The affects of identity theft is devastating. This involves someone's financial loss to reputation loss. In short it can destroy someone financially, mentally and physically.

Prevention measures:

Although full proof plan for this type of identity theft is not known, but some major prevention measures are there, such as,

Use of Internet Security Software: Use of good quality internet security software from a reputed security firm is good practice. It can able to solve many problems regarding this type of threat.

Use of strong passwords: Using alphanumeric characters with special words is always a better choice to avoid such type of threat.

Safe surfing on public internet cafes: In public computers use of incognito mode for safe surfing all the time is the best idea.

Keeping documents safe: Personal documents must be keeping with encryption in computers is a healthy practice. So the criminals are not easily got personal information.

Delete net banking history: It is always better to delete personal banking history after living computers.

Not to share personal information: One may not share their personal information in public media, social network. This can be harmful.

Use of common séance: Use of common séance during net surfing or doing financial work is always a great deal.

Awareness: Above all awareness is necessary. Without proper knowledge no one is able to prevent such type of threat. If victimized one must report to their nearest cybercrime police station for such cases.

Conclusion:

Internet is essential for now a day's life. Without this superhighway today's' life has became worthless. So we must use it wisely. As the cybercriminals may steal information from any corner of the earth, a common worldwide awareness plan is necessary to prevent such type of identity theft. Worldwide common law implement is very necessary for this threat. Through proper knowledge and education we must protect this type of identity theft.

Reference:

"Cyber-attack: Europol says it was unprecedented in scale". BBC News. 13 May 2017. Retrieved 13 May 2017.

"Internet of Things Global Standards Initiative". *ITU*. Retrieved 26 June 2015.

'WannaCry ransomware cyberattack fails to paralyse India; some businesses hit'.The times of India.16 May,2017. Retrived 16 May 2017.

B.-J. Koops, R. Leenes, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 30 (2006) 9;

Consumer Sentinel Network data book, Federal Trade Commission, 2014.

Gasser, Morrie (1988). *Building a Secure Computer System* . Van Nostrand Reinhold. p. 3. ISBN 0-442-23022-2.

Handbook on Identity-related Crime, United Nations, April 2011.

Identity Theft Assistance Center; http://www.identitytheftassistance.org

Identity Theft Resource Center; http://www.idtheftcenter.org/

Loviglio, Joann (March 2012). "If Microsoft co-founder's ID isn't safe, is yours?". msnbc.com.

McAfee Cybercrime Response Unit; http://www.mcafee.com/cru

'Unprecedented' cyberattack hits 200,000 in at least 150 countries, and the threat is escalating'. CNBC. 14 May 2017. Retrieved 16 May 2017.

Weisbaum, Herb (2014). "Seven signs you're a victim of identity theft". CNBC. Retrieved 2016-11-12.

Gender (In) equity-Myth & Reality: A Commentary

Harasankar Adhikari
Social Worker
Monihar Co-operative Housing Society
Flat No-7/2, 1050/2, Survey Park, Kolkata-700 075
e-mail: jaoya123@yahoo.co.in

According to Simone de Beauvoir (1953), 'women are not born but made'. The men's and women's behaviour is ingrained, reflecting innate and essential differences between the sexes. Sex signifies 'the anatomical and physiological characteristics as masculinity and feminity, which are defined by social, cultural and psychological attributes in a particular society at a particular time'(de Beauvoir, 1953). The 'gender system' underpins the patriarch, 'a system of male dominance, legitimized within family and society through superior rights, privileges, authority and power'(de Beauvoir, 1953).

The Marxist Theory of Gender tells that it is an isolated piece of reality; it has to be seen in relation to the social whole (totality)(Geetha, 2002). As a social and economic system, the masculinity and feminity exist in our society. In capital system, they are interlinked through two material processes – production and reproduction to make their own lives(Engles, 1948). This production and reproduction relations have been separated the activities as performed by both gender in a family as well as society. 'The right to property and the emergence of marriage institution transform the women as men's property'(Engles, 1948). It is the historic defeat of the female sex and the emergence of patriarchy. From then, females are considered as 'the second sex'(de Beauvoir, 1953). Thus, the female lives are trapped within the realm of reproduction and male sex takes the place of superiority as 'first sex'. Fredrick Angles(1948) argues that the emancipation of women and their equality would be possible when they would take part in production on a large social scale and domestic duties would be minor. But according to social and historical contexts, production-reproduction relationship is being criticized because it does not fit in all contexts.

The critics also find that Engles' arguments about the origins of male power are problematic. They justify that male's control over production does not make for their dominance rather their control over reproduction makes them powerful because the women are the exchange of 'gift'(Mcillassoux, 1981 and Levi-Strauss, 1969)). Through this process of exchange women become objects. They loose their accessibility to their bodies and sexuality. And they are trapped with their reproductive growth. The critics also opine that the liberation of women can be achieved without destruction of patriarchy, patriarchal attitudes and relationship. Thus, women's participation in workforce is a battle against patriarchy.

According to Mitchell (1971), the liberation of women can be achieved if production, reproduction, socialization and sexuality are integrated and transformed in relation to overall production.

Freud and Freudians share that masculinity and feminity are differed by individual psyche(Freud, 1953). Thus a girl takes to mothering and child care while a boy assumes to take public roles and responsibilities. Further Feminist historians criticize it because gender differences are not eternal. It is a social norm where man manages to gain control over woman's reproduction power, rendering women powerless and dependent on their sexual lives(Dworkin, 1981; Lacan, 1981 and Rich, 1981)). So, gender difference is a social ideals developed within the matrix of compulsory heterosexuality.

Gender differences:

The norms of gender differences reflect and express the complex economic and social relationships of power in the society. In this sense, the human body becomes the locus of sexual identity, of familial and social roles, as well as sexual self-awareness and expectation. Gender is referred to as practices of the body that means expression of femaleness or maleness or it is the bodily experience of sexual love, sport, religion, motion of discipline, restraint and control. Thus human body is schooled into looking, acting, desiring, expressing and controlling its movements in a certain ways through a range of institutions and agents as well as ideas and beliefs(Geetha, 2002).

Appearance that means beauty is a physical marker to distinguish women from men. Beauty is associated with women while men are virile(Geetha, 2002). It is a common notion that women would take care over their appearance whereas men care chiefly because energy and ability are their significant aspects to act as they wish. This notion of beauty is normal rule which

women's body must adhere. It is a cultural practice that has drawn from historical epoch. Sometimes in some cases women's images are considered as mother of God or various queens and aristocratic women'(Geetha, 2002). The beauty calls attention to a woman's modesty, chastity and goodness of temper. Fundamentally, beauty is a product of ideas, opinions, entertained and expressed by men about women. It is framed by male gaze which treats women as objects, and objectification of women is notions of pleasure, gratification and desire. It cultivates a sense of bodily good looking. It does not promote power and independence to women. It strengthens only the notion of an object. In the era of globalization, education and participation in workforces imprint the culture of beauty where illicit beauty dominants. But till date, a good family is one where the women of the family are honourable and they guard their chastity with their very lives. 'The chastity of wife, a concept which has not fierce determination is very essential to her family's stability'(Geetha, 2002).

Gender practice –myth & reality:

In present contexts, we find that gender competition is very common cultural practice and gender violence is rampant. Women's education, employment and awareness as well as movement for women's liberation and equity are unable to bridge the gender gaps in the third world like India. Government of India has taken various policies i.e. reservation of seats for women from lower house to upper houses, reservation of seats in education and so forth and different programmes including amendment and enforcement of law and order for women's justice and equity. This reservation and enactment of laws and orders is the process of undermine the privilege sections. Therefore, it is evident that women are considered till as "second sex' and it impedes ultimately women's equity and justice in our society. Practically, women use to imitate overall systems of gender equity. Their imitation includes their fashion, beauty care, employment in male gazing profession (i.e. media, event management and advertisement, etc). Women use to compete male in some habits and intellectual competition is little or evident. Their imitation of gender equity is making them arrogant against male. But they are dependent on male and they have much more faith on their male partner. Majority of women regardless of their education and economy has firmed faith and belief on marriage because they think that it is the only path of liberty and their usual gossip is restricted with realm of love and marriage partner. 'They involve in body show off including body revealing dress and other sex-related outlook to attract male partner who might be under her control'.

Conclusion:

Do feminism and movement for women's justice separate female as special class/second class citizen? Because emergence of separate wing of women's right tells it and they do not fall under the platform of human rights. It reminds that they are not to be considered as human being. The women are entering into a new world of deprivation via wrong root of gender equity. The bad impact of gender's rights reveal in their daily lives. As consequence of this imitating behaviour, they are in illusion because of their tendency for self-love, level of poor satisfaction, suffering in identity crisis and so forth. For this behaviour, they are deprived and exploited when they are involved in conditional consent to sexual relation. The incident of pre-marital sex, love victims, marital conflict, extra-marital relations and divorce is increasing day by day. So, a wrong pathway of gender equity is the principal cause of daily violence (within family and outside). Therefore, matrix of gender education and gender practices should be free from sexual lenses. Otherwise, gender equity is far way or never being achieved for gender balance in our society.

REFERENCES:

De Beavoir, Simone (1953), *The Second Sex,* New York : Knopf

Dworkin, Andrea(1981), *Pornography:Men Possessing Women,* New York : Putnam

Engles, Freidrick (1948), *The Origin of the Family, Private Property and the State,* Mascow: Progress Publishers

Freud, Sigmund (1953), *Three Essays on the Theory of Sexuality-Complete Psychological Work,* Vol-7, London : Hogarth

Geetha, V (2002), *Gender,* Kolkata : Stree

Lacan, Jacques (1981), *The Four Fundamental Concepts of Psychoanalysis,* New York: Norton

Levi-Strauss, (1969), *The Elementary Structure of Kinship,* London: Tavistock

Mcillassoux, Claude (1981), *Maidens, Meal and Money,* Cambridge : Cambridge University Press

Mitchell, Juliet (1971), *Women's Estate,* New York : Pantheon

Rich, Adrienne (1981), *Compulsory Heterosexuality and Lesbian Identity,* London: Only Women Press

Cyber diplomacy and cybercrime-An unholy nexus in world politics

Dr. Rupa Sen

Associate Professor, Department of Political Science

HMM College for Women,Dakshineswar, Kolkata-35

Diplomacy in International relations is resolution of problems by government and non-government agencies to strike a balance between sovereign states engaged in power politics. Diplomatic decisions are normally taken behind closed doors but the stupendous growths of communication technology have transformed the entire gamut of the activity, making it widely open and public. Technological revolution has widened the horizon of opportunities and possibilities for Governments to engage in constructive interaction with public resulting in intrusion of elements unconventional and evolving as a subject of international diplomacy. A popular outcome of the evolution is cyber diplomacy, a new component in the realm of foreign policy. However Cyber diplomacy should not be understood as just using modern means of communication; instead it should be comprehended as a crucial part of public diplomatic strategy.

Worldwide information communication and technological explosion undoubtedly influenced and enhanced life of mankind; but generated adversaries too.

Large scale use of internet facilities opened vistas of opportunities for social, economic and political benefits but the same facility emerged with the potentiality to aggravate tension in the political and military sphere leading to unwarranted misconception in relations and conflicts between nations, posing serious challenge to national and international security system. The asymmetrical and transnational nature of cyber threat, and corresponding impediments caused for political leaders, calls for accurate diplomatic effort to fight tension; because cyberspace is equally accessible to terrorists and criminals from both political and militaristic angle depending on targets fixed by perpetrators. ***Already the world is beset with four types of cyber insecurity namely cybercrime, cyber espionage, cyber terrorism and cyber warfare.*** Cyber warfares are. Largely conducted by national actors; wherein terrorist outfits need not develop malware

themselves for hacking. They may buy malware from commercial hacking crew and engage in malicious aims. Added to it access to malwares could be possible, if such groups were obliged with state sponsorship, to execute asymmetrical cyber terrorist attacks.

A few years ago Edward Snowden's revelation of cyber espionage activities of United states on NATO allies and mass surveillance upon people of America and some European countries had a diplomatic rendition at international level(here insiders compromised a great deal of information)This incident upholds how vulnerable the nations stand where cyber security is still not strong. This prompted many west European nations to adhere to US centric model of Governance, to prevent damaging effect to their systems inflicted by high powered nations.

Donald Trump announced his interest to harbor good relation with India soon after his presidential victory. But his anti-Indian rant and speaking in favour of Pakistan and China now persuades India to measure her steps cautiously in building diplomatic ties with America.

Candidly ambitious America seeks to promote its desired interest promoting its desired interest at the cost of manipulation or suppression. In this context, it seeks to contain the growing power of China in Asia and aims to use the regional powers like India as a platform for support. Now China is not only a close neighbor to India but also the biggest market for trade and business. On the other side China is perhaps the only country who managed to surpass America digitally. America wants Russia to prevail over China. Russia on the other hand is biggest supplier of arms to India. It enjoys close ties with Russia and strong economic ties with China (New Delhi being the largest trading partner) Pakistan exports terrorism in the area especially to India. America funds and supplies arms to Pakistan. America's only agenda is to promote its economic and political interest. Naturally its market interest with the rogue state, Pakistan, shall prevent it from displaying any friendly gesture to India in its war against Pakistan for combating terrorism. Hence India needs to measure her steps toward US; unless she streamlines her own cyber capability any possibility of her maintaining a voice in world politics would remain a far cry. North Korea refuses to be complacent with United States. While China continues to be the economic lifeline of Korea. The overtures of politics compels each nation to chart out a balanced cyber diplomacy to combat possible crisis slammed by an opponent or camaflouging ally, to ensure security, peace and stability.

With societies increasingly becoming digitized a paradigmatic shift is observed in the realm of International politics. Some changes are profoundly reflected in terms of priorities acquired by hard power versus soft power. The earlier conventional modes of economic coercion or military force is now obsolete, and losing ground against more subtle and effective technique of persuasion in the form of soft power and encouraging empowerment of public opinion both within and beyond the territory of ones nation. Under the circumstance it is necessary that governments, inform and influence foreign audience to create empathy as prerequisite for achieving its policy objectives abroad and also strategic aspect of their diplomacy.

North Korea's publicised inclination to test nuclear weapons or India's digital response to Pakistan's threat of nuking or constant publicizing of news from Iran, Iraq, Syria, Turkey and host of other nations inflicted with mindless ISIS and their activities are all part of the strategy called cyber diplomacy. The dastardly covert pogroms engineered by Big powers that so long remained under cover, is popped up with the boon of advancement of technological capabilities, strengthening the scope of strategic formulations required to address a crisis. This bears a direct impact upon the unidimensional advantage enjoyed by US, in the context of diplomacy and detterence in International relations. ***Cyberdiplomacy is a strategy wherein, a nation enjoys the opportunity of exposing actual cause of their crisis and the rogue engaged therein. Also this form of diplomacy helps a nation find global support, for its activities back home.***

This strategy also contributes largely to conventional mode of diplomacy in implementing plans and achieving objectives of foreign policy issues. It builds empathy for the country in question. If Public diplomacy of US is to spread its values and ideas internationally it is normal they adapt to mass media and growing influence of culture tied to political and social change. The ability to reach people with mass diplomacy increases with strategic communication programme designed for foreign audience and supported by wide range of technological facilities like internet talkshows, tweeting, publications etc. mediums much stronger. France has subscribed to similar diplomacy of sharing its values and ideas to carve a niche in the world forum. Culture information and communication are strategic assets in the field of security policy in Germany as well.

Moscow has a troll Army under internet Research Agency to wage a disinformation campaign in support of its invasion of Ukraine and Kremlin in general. A couple of months ago Putin nudged

a hint at Russia's role in hacking of America's Presidential election. Intel Agencies claimed that Putin himself directed a Russian influence campaign involving cyberattacks and disinformation intended to tilt the election in favour of Donald Trump***(Times of India dated 2nd June 2017)***

Club of Middle East countries like Saudi Arabia, UAE, Bahrain, Egypt And Yemen recently severed diplomatic ties with Qatar with the belief that the state has befriended Iran the regional enemy of the Arab world and supported terrorism in the belt following a CNN Report on 6thjune 2017, where it was alleged that Russian hackers had breached Qatars state news agency. This implied even fake news could spark a crisis anywhere in the world.If Russian hackers have done it or America falsely implicated Russia to make the news viral the result remained the same; leading to isolation of Qatar impairing its socio, economic political existence***.(Times of India dated 8th June 2017)***

Brexit Campaigner Nigel Farage is alleged to have clandestine links with FBI and Russia-----a belief viral in social media.All such link ups are aired to capsize the growing influence of a group or a nation, engaged in power politics; In this case it was sheer hatred simmering within liberal elites, who were unable to accept both Brexit and Trump. Similarly, the Boko Haram sect of Nigeria who kidnapped nearly 276 school girls and held them hostage for months, in 2014-15 drew attention by taking recourse to social media. It publicized the link between Boko Harams and ISIS and Al Qaida. In 2013 Syrian Army (SEA) hacked twitter account of a news agency and falsely claimed that White House was bombed and Obama injured.

AgainCyber-attacks on IT infrastructure from Estonia in 2007, the hybrid war fought in 2008 in the conflict between Russia and Georgia the cyber-attacks on Uranium enrichment programme from Iran in 2010 all denote a cyber component. The virtual attacks following conflict between Russia and Ukraine aimed not just IT infrastructures, including military communication system of Georgia but also of Russia, European countries and NATO Allies. All the episodes beginning from war between Eastonian government and media in 2007,the German Bundestag in 2015,Ukraines power grid in 2015 and Swedish media in March 2016 account to cyberwars. Reports said that United States collaborated with Sweden and other nations to develop hacking and surveillance tools; and assured that the devices used be more powerful than that used to attack Russia. The Swedish FRA was ensured access to National security Agency of America a powerful analytic tool called Xkeyscore that would enable an internet user to find access to

entire gamut of datas at his disposal. Politically and military motivated cyberwars permanently eroded mutualtrust between political leaders shrouding the global ambience with suspicion and ambiguity.leaving trail of tension,competition and conflict hovering overhead***,(Ref The Swedish kings of cyberwar by Hugh Eakin,Newyork Review 19th january 2017)***

Further the US president Donald Trump is reported to have breached a protocol with cellphone diplomacy. Leaders of Canada, Mexico and France have US President on speed dials, which proves that all such leaders have contact numbers of Trump saved for direct communication. World leaders calling up one another may appear common but in diplomatic matters where leader to leader interactions are orchestrated it is certainly a break of protocol for a president who himself expressed distrust of official channels. More so he is the man who pilloried Hillary Clinton for lax in security for keeping an email server in her residence and generated chants of 'lock her up' for her infractions.

When the world is grappling for cybersecurity, tinkering in the social media could prove disastrous for a nation. ***Typos like China steals US Navy research drone in international waters-rips it out of waterand takes it to china inunpresidented act(Dec 2016) tweeted by Trump, caused shamming of the presidential post of a country the world looks upon. Secondly such irresponsible tweet could trigger unpleasant bilateral relations Thirdly such acts and informations bears a direct impact not only on the economic index of that nation in question but others who are committed or dependents in the system of economic cycle. With internet infrastructure going down by few hours could catapult and cause a rupture in economy, politics and society at one go. Already Fiscal loses adhering to cybercrime and cyberwars across the globe today is alarm ing.The expenditure amounts to US$81 billion just in Asia Pacific region***. ***Social media has evolved into diplomacy's second self, a significant other, according to a report by Burson-Marsteller, a global PR company. It provides a platform for unwarranted communication with targeted groups.***

The Paris Agreement signed by 177 nations on climate change is due to be implemented within 2020.Cyberdiplomacy is expected to play a crucial role in keeping alive the awareness of the problem; ofcourse to weed out the challenges, adhering to it, requires tranformative technology based sustainability revolution to enable countries like China and India breathe with ease in the Asian belt atleast. Cyberdiplomacy has the potentiality to generate Asian public opinion to keep

China from asserting control over South China Sea. But when countries like America withdraw from their resolution of working together for a sustainable environment stategy of cyberdiplomacy ought to be applied to persuade and convince them to be back on track.With increasing use of technology as a component for military response, primarily the need is to consider the threat as seriously as a conventional one. Singapore has already deployed Cyberdiplomacy building Alliances with other nations to sweep expertise to regularly monitor and test its defence and fruitful implementation.

If cyberdiplomacy is observed as a growing strategy in the field of international politics, cybercrime, cyberwarfare and terrorism are also growing rapidly, as an organised network of business, where huge number of populace are engaged directly or indirectly, threatening Governments, Business, social media etc. leaving the world in a dilemma. The unholy nexus between cyberdiplomacy and cybercrime dwindles and dodges the nations and nationalities to adestination of uncertainity.

Many Internet users indulge in nefarious acts jeopardizing peace and security of a region or state. The US produces malware, spams and viruses more than any other country in the world.It is the hub for illegal IT jobs that scams anything that profits them; yet the scammers remain free from the legal claws ,often insulated and secured from distant lands by high powered influentials and underworld mafias.

However recent reports hold that China has outsmarted the US by hosting web pages that install malicious programme in computers to steal private information or send spam e-mails. According to Symantec Report in 2006 Beijing was found home to largest collection of malware inflicted computers.

Infact China is the biggest threat to United States. Numerous Cyber groups are nurtured in Beijing. Many under the tutelage of the Government itself. More than 70% of US corporate intellectual property theft originates in China. Chinese military strength is still to match the impeccable competency of the US defense Unit. As an alternate path to edge over US military acumen Beijing chose to bank on commercial and Government espionage, in which they have excelled enormously. Even the US can ill afford to ignore their technological smartness, because they are still struggling and grappling to protect their technological secrets from China. The

Chinese hold that they harbour no intention to disrespect sovereignty of nations in Cyber space, even though they focuss on commercial diplomacy and paricipation as per international technical parameters to shape cyberspace for economic and political interests; As a nation state they too intend to fight terrorism, control regional influence and manage bilateral relation with US.

Around 150 countries were targeted recently with ransomeware cyberattack, disrupting normalcy in both public and private life. The malware called wannacry paralyzed computers, running factories, banks, government agencies and transport systems affecting 200000 victims in more than 150 nations. Among the worst hit was Russias interior ministry and companies including Spain's Telefonica and FedEx corp in the United States. The pirates of the cyberspace has demanded to be paid in bitcoins and threatened to release five minutes of a film of Disney company followed by 20 minutes segment until the ransome was paid. The role of pirates and cybercriminals interfering the creative world is quiet common across the world. Very often cultural icons buckle under duress to the dictates of the digital dark world to survive financial setbacks that could ruin them forever.

Recently an atack on a plush hotel at Austria (Alpine Hotel)where computer system was locked which compelled guests to be stranded in the lobby. This incident was a novel example of an increasingly malicious and prevalent type of modern day privacy through software, called ransomeware. Ransomeware is pandemic with internet, anything can be switched on and off from computers to cameras to baby monitors. But hacking a hotel and locking people out of their rooms is a new line of attack in the league of nefarious activities**. *(TOI, 1February2017)***

Reports from the Japan's computer Emergency Response Team coordination center, a non-profit group, said that 2000computers at 600 centres in japan werecrippled andhit. Companies like Hitachi and Nissan motor Company faced problems though managed later. Chinese state media announced that 29,372 institutions had been infected in the land along with hundreds of thousands of devices. Educational institutions were adversely affected because of using old computers slow in updating operating systems and security.

The Railway stations, mail delivery, gas stations, office buildings, shopping malls and government services in China were affected. Common Chinese public vented their grievance in

social networking sites. This shows greatest techno savvy country could also fall a prey to malwares and disfunctionality of the system. Similar stories followed from Indonesia, where malware locked patient files on computers in two hospitals in the capital Jakarta, causing restlessness. The effect of the malware in India was however comparatively low as precaution for insulation from malware affliction was taken. Reserve Bank of India directed Banks to operationalize this only after software updates were completed corporate houses urged employees to back up their data and refrain from opening unfamiliar files attachments. Windows users were urged to install software upgrades and firewalls. FMCG companies Marico and Godrej issued advisories to employees asking them to guard against the malware. South Korea, Malaysia, Bangladesh and host of other countries experienced the consequence of being targets of cybercrime, freezing their computers and causing encryption and than demand ingransom through online bitcoin payment to unlock files. ***So the stealthy underhand of cybercrimes are constantly on the vigil undermining the positive intensions of cyber diplomacy.***

An Indian origin Google security researcher found proof suggesting that North Korean hackers may have carried out the unprecedented ransomware cyberattacks that hit multiple nations across the globe. Researchers claimed that some of the code used in recent ransomware called Wannacry was nearly similar to the code used by Lazarus group a pack of North Korean hackers who used a similar version for the attack on Sony pictures Entertainment in 2014 and Bangladesh Central Bank last year.

Researchers found similarities between the code found within Wannacry and other tools believed to have been created by the Lazarus group. A security expert Prof Alan Woodward said that time stamps within the original Wannacry code were set to UTC+9—Chinas time zone and the text demanding the ransome used machine translated english but a chinese segment apparently written by a native.

Cybercrime has evolved into a full-fledged industry indulging into marketing, providing service, trading, financing and others. The growth of the industry fuelled by cyber currencies like biticoin and protective cloak for criminals provided by Technology like TOR. Increasing sophistication of the industry has lured criminals to engage in bigger crimes ranging from implementing ransomeware encrypting contents of the computer and demanding ransome to unlock the system, to exploit users engaged in publishing personal data's from various dating

sites. With 1.5 million annual cyberattack online Crime is a real threat to internet users. There are nearly 4000cyber attacks every day,170 attacks every hour and 3 attacks every minute. In 2014,47% of American adults had their personal data stolen by hackers through data breaches at large companies. In 2013,43% companies had a data breach, in which hackers got into their systems to steal information. Data breaches targeting consumer information are on the rise, increasing 62% from 2012-13.

By the grace of social media anyone could be duped by a link posted in a twitter or facebook, or from a cloned account would easily enable a hacker to break into their computer network. Once a person compromises attack (spear phishing) could move fast through that persons friend network leading to nightmare for the targeted. According to a 2016 report by Verizon around 30% spear phishing emails were opened by targets.But research published by cybersecurity firm ZeroFox showed that 66$ of spear phishing messages sent through social media sites were opened by their intended victims.

NCRB report holds that there has been an escalation of 70%rise in cybercrime in India between 2013-15; with a consistent growth of 17----18% annually.

According toNCRB Report 2014 cybercrime was a little more than 9600;while in 2013 it was somewhere around 5693.Estimates for 2015 crimes were 16000;;all targets being active participants or users of social networking sites. Large scale technological adoption with minimal awareness has led to rise in such crimes. Besides lottery and job scams are rampant that evolved as organized crimes in India. With 780 cases of cyber crimes reported in 2015 Noida saw setting up of centre for cybercrime investigation in 2016.It is essential that people learn to protect themselves, the menace would loom large with its devastating effect.

The National cyber security policy is a framework for protecting information in cyberspace, by eliminating vulnerabilities. Major clauses include greater emphasis on research and development of indegenous security, technology and effective testing and deployment. Need for Public-Private partnership visa -vis technical and operational cooperation to adopt regulations and infrastructure in conformity with International best practices policy related to cybersecurity facilitated the creation of new agency called National critical information Infrastructure Protection center(NCIIPC) charged with protecting assets in sensitive sectors such as finance

defence, energy and telecommunication. Unfortunately laws formulated by Government are not binding or enforceable. Besides the budget is not enough. Telecommunications is integrated into cyberspace, since the advent of internet protocols on mobile devices, one of the primary reasons for the rise in attacks. Besides UGC directed universities (technical)and institutions to add cybersecurity and information security as subject of higher studies in 2013.When common man and his life is affected by cybercrimes, can Government institutions remain unfazed? The fruitfulness of cyberdiplomacy depends on intension of leaders, rule bound administration and stable digital system because disruptions and disturbances would invariably cause turbulence and impair the objectives of nation states.

Countries across the world is trying to manage cyber related issues via existing diplomatic methods using diplomatic resources. Cyberspace seldom conforms to conventional norms of diplomacy in vogue in the 20th century. Studies show that the ability to engage in cyber war with a country in the virtual world while maintaining normal diplomatic relation in actual world can no longer be addressed by current standards.

Countries like Singapore has already adopted cybersecurity measures to challenge objectives of perpetrators. They resolved to strengthen cyberdiplomacy, developing a vibrant cyber security ecosystem by educating individuals, creating jobs by developing defense of the lands critical infrastructure cybersecurity talent and building international partnerships to respond to cyber threats. Singapore aims to work with ASEAN and secure the internet space of the region. They are looking forward to form a forum that would attract high ranking military and political officials…forge a dialogue with nations of ASEAN and team up for a joint mission.

The European Union now seeks to initiate proper administration and implementation of International law in cyberspace. They wish to enhance the building capacity of 3rd world nations and engage in promoting international stability and protect digital economy. China has agreed to comply and cooperate in cyber investigation to nab criminals. South korea subscribed to active cyber diplomacy. India embarked upon the mission to spread cyber security awareness. Today America encourages countries to engage in transnational cyber cooperation and promote cybersecurity.

Terrorism and crimes would continue unabated; terrorists would scale dizzy heights to discover new devices and methods of attack but to fight the mindless mayhem of a handful should still continue. ***Unless nations club together spontaneously, adhere to rules, step up public education to propagate public safe use of internet combating the unholy nexus of cybercrime and diplomacy would remain a far cry. Sailing through uncharted sea may be difficult and dangerous but surely not impossible.***

References

1. ***Ransomeware blow contained in India, Times of India dated 16May 2017.***
2. ***Wannacry virus spreadsto Asia, fear of new wave looms, Times of India 16May 2017.***
3. ***Indian origin techie links cyberattack to North Korea, Times of India dated 17May 2017***
4. ***Notes on Diplomatic practice by Odeen Ishmael***
5. ***The new public diplomacy: Soft power in International Relations editor Jan Mellisen, palgrave, Macmillan.***
6. ***Cyberdiplomacy: Managing foreign policy in the 21st century by Evan H Potter(ed)***
7. ***Cyberdiplomacy by Lindelwa Makhanya***
8. ***Cyberdiplomacy:A new strategy of influence,Halifax Nova Scotia,May30,2003***
9. ***Can cyberdiplomacy replace traditional diplomats and help us get a handle on world most complicated problems? by Narain D Batra.Times of India dated 27th August 2016***
10. ***The Straits Times,Singapore,24th october 2016***
11. ***The United states-Australia cyber dialogue:fighting cybercrime in Asia-Pacific, November 4th 2016 by Liam Nevill and Zoe Hawkins(In technology policy blog from CSIS)***
12. ***Trump breaking protocol with cellphone diplomacy by Chidanand. Rajghatta,Times of India dated jine1st 2017.***
13. ***Fighting ISIS in cyberage by OZ Sultan, March 17 2017***
14. ***The Diplomat, How china became a world class cyber power by Greg Austin dated 30th April 2015.***
15. ***Cyber diplomacy is the answer, Wikimedia by Oon Yeoh in Malaysia Today on september 4th 2008.***

16. ***Cyberdiplomacy versus digital diplomacy and Terminological distinction by Shaun Rlordon May 12th 2016.***
17. ***The coming age of cyberterrorism by Scott Stewart, VP of tactical analysis, Stratfor.***
18. ***Is cyber terrorism the new norm***al? ***By Dan Holden, ASERT.***