Aayushi International Interdisciplinary Research Journal (AIIRJ)
UGC Approved Sr.No.64259
Vol - V Issue-IV APRIL 2018 ISSN 2349-638x Impact Factor 4.574

Cybercrime in India: A Trend Analysis Specific to North East

Dr.R.D.Padmavathy
Department of Education, Tezpur University (A Central University)

Abstract:

Development of internet and the growth of its usage have crossed more that 1000% times in the world compared to early years. Though internet usage has grown there is still knowledge existence of ignorance about proper handling of internet and preventive measures to be adopted from getting any risk. This study explores the basis about cyber crime, types and acts, cyber crime statuses in India a trend analysis from year 2006 to 2016 specifically to north east for understanding the nature. In addition to that adolescents and their problems while using social media without knowing consequences, cyber crime cases registered on adolescence and the trend, role of parents, teachers, and community and policy makers in preventing the adolescents from risk are discussed briefly.

Keywords: *Cybercrime, Adolescents, Internet, Social media, Victims*

Introduction

The University of California introduced the public to the Internet on July 3, 1969 and Tim Berners Lee introduces "*world wide web"* to the public on August 6, 1991 changes the millions of people life upside down . The initial vision of the Internet (1969) was implemented to bring together a global world population segregated by geography under one umbrella and remove the negative problems that would manifest among future generations makes one consider the positive impacts versus the negative. After the introduction of this technology, world faces a vibrant culture of different dimension, produce new strange curiosity turned our existence as well as life style upside down. Internet extent its limits and it is now becomes the preferred medium of many individuals' communications. National Studies provides evidence that internet users spend longer period of time and increases the usage duration day by day and when they do not have access to internet connectivity they feel they were not in the world. The excessive uses of internet have been documented worldwide. Understanding this fact internet hackers use their knowledge and skill to gain benefit by exploiting and victimise others.

James(2009) in his article highlight President Obama's announcement on May 29 about a high-level initiative to address the growing problem of computer attacks against the government, corporations and individuals by coordinating the various efforts to fight hackers and other computer criminals under the direction of a coordinator already dubbed the "cyber czar." "I know how it feels to have privacy violated because it has happened to me and the people around me". In 2011, President Barack Obama in White House hosted the first White House Conference on Bullying Prevention and brought national attention through conference to educate students, teachers, coaches and parents on how to identify and explain the effects of cyberspace communication about cyber bullying. He reveals furthermore, bullying is problematic for Americans and the practice of cyber bullying can only become obsolete with the help and involvement of all individuals functioning in today's society. This made social workers and professionals involved in this process to advocate, educate and create aware among the youth about this cyber culture. This problem is now all over the world. Adolescence is getting in to trouble without knowing the fact about cyber crime. This shows how the cyber crime related problem harassing many individual like a strange virus without showing any symptoms outside make them physically, mentally and psychological ill persons.

Cyber Crime

Cybercrime is defined as "any unlawful act where a computer is used as a tool or target or both and offenders are booked under the Information Technology Act. However, according to the government's own admission in Parliament in July, the rate of conviction is very low till now. Debarati Halder and Jaishankar defines cyber crimes as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Cyber crime becomes a real threat to the society and a new criminal indulge in cyber crime and his victims are growing exponentially. In comparison, theft and robbery, which account for the highest incidences of crime in India, show an annual growth of 17-18%. Every sixth cybercrime in India is committed through social media, Alok Mittal, the chief of the National Investigation Agency (NIA) has said. Though he did not divulge the basis of his findings, data from the National Crime Records Bureau (NCRB) show around 70% rise in cybercrimes annually. "The number of cybercrime cases reported across India in 2014 was a little more than 9,600, a mere fraction of the estimated three lakh theft cases (that year). But the concern is an annual growth of 70% for the last three years," Mittal said. In 2013, the number was 5,693 estimates for 2015 put the number of cybercrimes at 16,000. As reported by Dubbudu (2016) with increasing internet penetration, cyber crimes have also increased in the last few years. A total of 1.71 lakh cybercrimes were reported in India in the past three-and-a-half years. The number of crimes that have been reported so far (27,482) indicates that the total number is likely to cross 50,000 by December (Chauhan, 2017).Cyber experts said high rate of cyber crime is natural in a country where technology adoption is high but awareness is low. "Most of cyber crime emanates is targeted towards people with social media accounts since in India knowledge about security and privacy protection is low," said Mrityunjay Kapoor, head of risk analysis at KPMG (Ray & Ghoshal, 2016). In India, at least one cyber attack was reported every 10 minutes in the first six months of 2017. In 2017, as per the Indian Computer Emergency Response Team (CERT-In), a total of 27,482 cases of cybercrimes have been reported across the world. These include phishing, site intrusion, virus, and ransom ware (Chauhan,2017). Cyber crime are categorised broadly in three categories namely crime against individuals, property and government. In India Cyber Crimes are registered under three broad heads, the IT Act, the Indian Penal Code (IPC) and other State Level Legislations (SLL). The cases registered under the IT Act include

1. Cyber crimes under the IT Act -Computer related offences:

- Tampering with Computer source documents - Sec.65
- Computer related offences - Hacking Computers, Data alteration - Sec.66&66B to E
- Cyber Terrorism - Sec.66 F
- Publishing/Transmission of obscene /Sexually explicit information- Sec.67,67Ato C
- Un-authorised access to protected system Sec.70
- Breach of Confidentiality and Privacy - Sec.72
- Publishing false digital signature certificates - Sec.73

2. Cyber Crimes under Indian Penal Code cases, special and Local Laws:

- Fabrification of false evidence/destruction of electronic records for evidence- Sec. 193,204 IPC
- Data Theft - Sec. 379 to 381 IPC
- Web-Jacking - Sec. 383 IPC
- Criminal Breach of Trust/Fraud- Sec. 406 , 408,409 IPC
- Bogus websites, cyber frauds, Cheating - Sec 420 IPC
- Forgery of electronic records, Email spoofing - Sec 463 IPC
- Forgery -- Sec. 465 to 468,471& 477 IPC
- Counter Feiting - Sec 489A to 489 E IPC

- Sending defamatory messages by email - Sec 499 IPC
- E-Mail Abuse - Sec.500 IPC
- Sending threatening messages by email - Sec 503 IPC

3. Cyber Crimes under the Special Acts:

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms Act

Types of Cyber Crime

Cyber crimes as listed by Aggarwal (2015) can be of the following types-

A. Hacking- *In* this type of crime person's computer is accessed by criminals without the knowledge of person from remote locations. Hacking is done to access the personal, confidential or sensitive information from person's computer. Hacking can also be done to change the passwords of login accounts either of social networking sites or any other business transaction site and use the information against them.

B. Theft- When a person violates or breaks the copyrights of a particular website and download songs, games, movies and software is known as theft. There are many websites which allow downloading the data that is copied from other websites. It is known as pirated data as the quality of data is not up to the mark.

C. Identity theft- In this type of crime, criminals steal data about person's bank account number, credit card number, debit card and other confidential data to transfer money to his account or buy things online by acting as the original person

D. Defamation- In this attack, the criminal hacks the email account of a person and send mails using abusive languages to known persons' mail accounts so as to lower the dignity or fame of the person.

E. Malicious software- These are the programs or software that are used to access the system to steal confidential data of the organization or this software can be used to damage the hardware and software of the system.

F. Cyber Stalking- This is the type of attack where online messages and e-mails are bombarded on victim's system. In cyber staking, internet is used to harass an individual, group or organization by using defamation, identity theft, solicitation for sex, false accusations etc.

G. E-mail harassment- In this type of attack, the victim is harassed by receiving letters, attachments in files and folders of e-mails.

H. Spoofing- Spoofing attack is a situation in which criminal masquerade as another person i.e. the criminal acts as another person by using his identity and therefore takes advantage of illegally accessing data of the other person.

I. Fraud- Fraud is done by transferring money from victim's bank accounts either by using their bank account numbers or credit cards.

J. Virus- Virus is a small program that is loaded on the victim's computer without his knowledge which causes a large amount of damage to the system. Viruses attach themselves to files and circulate themselves to other files on the network which leads to damage of the system.

K. Trojan horse- Trojan horse is a harmful code which is present inside data such that it convinces the victim to install his code as it is useful which after being installed causes damage to the system.

L. Phishing- Phishing is an attack in which criminal sends genuine looking emails to victim to gather personal and financial information of the victim which can then be used against him.

M. Grooming- Grooming is the process of influencing the children and youth emotionally for sexual exploitation. In this process, an adult wins the trust of victim by giving flattery offers and then attempts to sexualize the relation between them which leads to pornography or sex trafficking.

Trend Analysis Of Cyber Crime In India

In India the first cyber crime case reported in Chandigarh on 2000. From that year the cybercrime came to light and numbers of cases registered under the IT Act and IPC have been growing continuously. The cases registered under the IT act increase by more than 2000% from 2006 to 2016. There was almost a 70% increase in the number of cyber crimes under the IT act between 2013 and 2016 and increasing continuously.

Comparing the status of cyber crime 2006 to 2016 showed declined status only in 2006 and 2008. The cases registered under the IT increased by 550% times and the IPC increased by 100% more during the period 2006 to 2016.This is shown in Table 1 and 2. The increase in the number of cyber crimes is because of introduction of technologies, devices and lack of awareness. Between 2011 and 2016, the number of cyber crimes registered in the country has increased 5 times. The details are shown in Table 1.

Table 1: Cyber Crime in India- A Brief Analysis (2006-2016)

Year	IT	IPC	SLL	Total	Status	%	Cyber Forgery	Cyber Fraud	Age 18 - 30(%)
2006	142	311	Nil	453	Decline	-5.8	51.4	28.9	70.80
2007	217	339	Nil	556	Increased	22.7	64.0	21.5	63.05
2008	288	176	Nil	464	Decline	-16.5	31.2	44.9	61.20
2009	420	276	Nil	696	Increased	50	57.2	32.6	64.60
2010	966	356	Nil	1322	Increased	89.9	52.8	41.0	54.20
2011	1791	422	Nil	2213	Increased	67.4	61.3	27.9	54.20
2012	2876	601	Nil	3477	Increased	57.1	46.9	43.1	58.70
2013	4356	1337	Nil	5693	Increased	63.7	55.9	38.7	56.70
2014	7201	2272	149	9622	Increased	69.0	52.7	44.4	46.40
2015	8045	3422	125	11592	Increased	20.5	65.9	81.6	59.70
2016	8613	3518	186	12317	Increased	6.30	56.0	81.0	60.00
Total	**34915**	**13030**	**460**	**48405**	Source: National Crime Records Bureau, MHA, India : Data (2005 - 2016)				

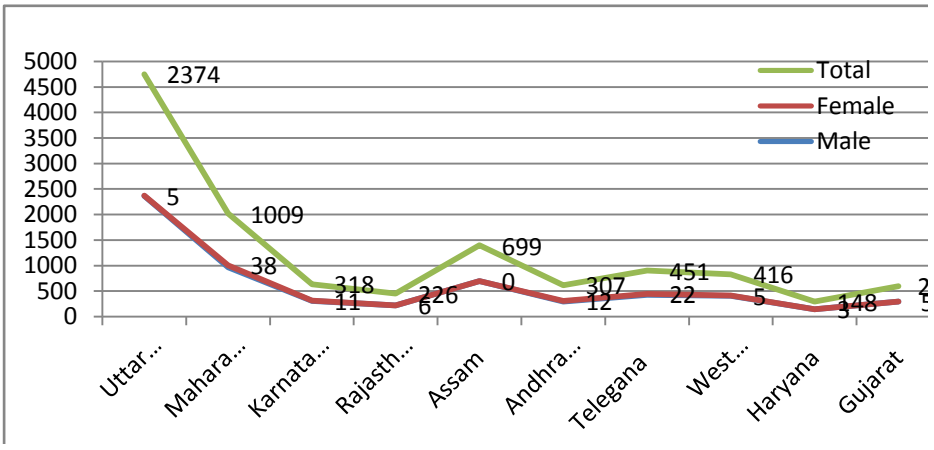
As inferred in the NCRB report "Crime in India" (2016) the maximum numbers of cyber-crimes cases were reported in Uttar Pradesh 2,639 cases (21.4%) followed by Maharashtra 1009 cases (29.3%) and Karnataka with 318 cases (8.9%). This showed that number of cases registered in Maharashtra & Uttar Pradesh alone accounted for 1/3rd of these cyber crimes. During 2016, 48.6% of cyber-crime cases reported were for illegal gain (5,987) followed by revenge with 8.6% (1,056 cases) and insult to the modesty of women with 5.6% (686 cases). The details are shown in Table 2 and Fig 1:

Table 2: Gender and percentage wise number of cyber crime cases registered in India

State/UT	Male	Female	Total	Incidence share of State	
				% wise	Rank
Uttar Pradesh	2369	5	2374	21.4	1
Maharashtra	971	38	1009	29.3	2
Karnataka	307	11	318	8.9	3
Rajasthan	220	6	226	7.6	4
Assam	699	0	699	5.7	5
Andhra Pradesh	296	12	307	5.0	6
Telegana	429	22	451	4.8	7
West Bengal	411	5	416	3.9	8
Haryana	145	3	148	3.3	9

Gujarat	293	5	298	2.9	10

Figure 1: Number of Cyber Crime cases registered in India Gender wise



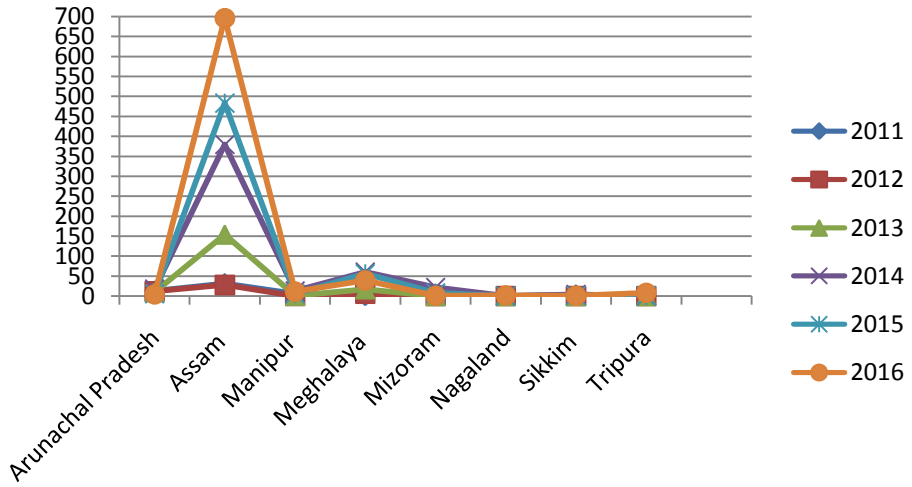
The findings revealed that number of males (6140 cases, 98.2%) were more likely to engage in cyber crimes comparing with females. This situation alarms to save women netizens from victimization. Mittal reported in his article frauds through matrimonial sites were also raising in the past few years. Gangs look for vulnerable women picking on divorced or single women as targets. "Organised financial crime was a feature of east European and former USSR countries. But with high internet user density and inadequate knowledge of net users, various cities in India are also becoming locations for perpetrating such crimes," In recent years, Noida has turned into a hub of cyber attacks in the national capital region, with 780 cybercrime cases of reported in 2015, Noida saw the setting up of the centre for cyber crime investigation in 2016. "This is a menace that will only increase with the rising number of internet users in India. Unless people learn to protect themselves, this cannot be controlled," (Ray&Ghoshal, 2016). The top states in the list are the ones with a greater internet subscriber's base. The bottoms 10 are relatively smaller states with lower population & lower internet penetration. The present offenders were in the age group 18, age ranged from 18 to 30 increasing and also the computer forgery and computer fraud are increased very high comparing with early years. In reality cyber obscenity starts with the conversation using attractive words to tease their women friends and it on rise to next level of conversation. This type of problem would be solved only victimized women come forward and take action against the offenders.

Trend Analysis Of Cyber Crime In North East India

In total 2139 cyber crime cases were register in North East India. Comparing North East Indian states very high numbers of cyber crime cases were registered in Assam. There has been a phenomenal raise to 1771 cases in 2011 to 2016 followed by Meghalaya with 182 cases. MukeshSahay, Assam additional Director-General of Police (CID) said greater Internet penetration was one of the reasons for the increase in cyber crimes in the state, "with the rising popularity of social networking sites, there has also been an increase in the cases of defamation on those sites," "Some people also misuse the Internet and social media for rumour-mongering, which had led to thousands of people from the Northeast fleeing Bangalore in 2012" (Sarma, 2014). In Mizoram and Manipur less than 40 cases were registered and no cases were registered upto 2013 in Nagaland, Sikkim, Tripura and in 2014 to 2016 less than 10 got registered. The details are listed in Table 3 and Fig 2.

Table 3: Cyber Crime in North East India- A Brief Analysis (2006-2016)												
Year	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**Total**
Arunachal Pradesh	0	0	0	1	3	13	12	10	18	6	4	**63**
Assam	1	1	1	4	18	31	28	154	379	483	696	**1796**
Manipur	0	0	0	1	0	6	0	1	13	6	11	**38**
Meghalaya	2	2	0	0	0	0	6	17	60	56	39	**182**
Mizoram	0	0	0	0	2	3	0	0	22	8	1	**36**
Nagaland	0	0	0	0	0	0	0	0	0	0	2	**2**
Sikkim	0	0	0	0	0	3	0	0	4	1	1	**9**
Tripura	0	0	0	0	0	0	0	0	0	1	8	**9**
Total	**3**	**3**	**1**	**6**	**23**	**56**	**46**	**182**	**496**	**561**	**762**	**2139**

Figure 2: North East India Cyber Crime Incidence Recorded 2011-2016



Status Of Technological Gadgets And Social Media Usage By Adolescence

The technological revolutionised society found lots of digital gadgets and apps to promote human comfort and made easily available, accessible to all with moderate price. The easy availability tablets, IPods, smart phones to modern adolescence make them to use the gadgets at all time. The mobile and internet become the part of adolescent's life. The continuous use of mobile and internet intertwined their activities and provide to face online risks and problems. These involve a diversity of phenomena that can be categorized into three broad groups: content, contact, and conduct (Livingstone et al. 2011). Van Kokswijk (2007, 40) remarks this development in the concept of "inter-reality," as a "mix of the virtual and physical realities into a hybrid total experience." They took photos through that (whether it is an exotic location or not they ever care for that) and immediately upload those pictures in the facebook, instagram, twitter etc without thinking any of the consequences. By exploring those photographs or by touching the like of those new strangers gets introduce to the adolescence.

Many parents appreciate and feel proud about the technology handling skill of their children without knowing that they are getting addicted to gadgets. The over freedom, love and fulfilling the wish of their children without care and awareness makes the child to select a different companions and gets attraction

towards others. In the same way in a home the gadgets was not only used or handled by the own person. In a family where there is adolescence there is always a chance to handle and misuse of that. If at any one situation it is knowingly or unknowingly misused it gives birth to various cyber crimes issues. Paganini (2012) pointed out the most seven common crimes committed on face book by criminals are scams, cyber bullying, stalking, robbery, identity theft, defamation and harassment. The basis of the crime starts at a single point unknowingly committed or misused gadgets.

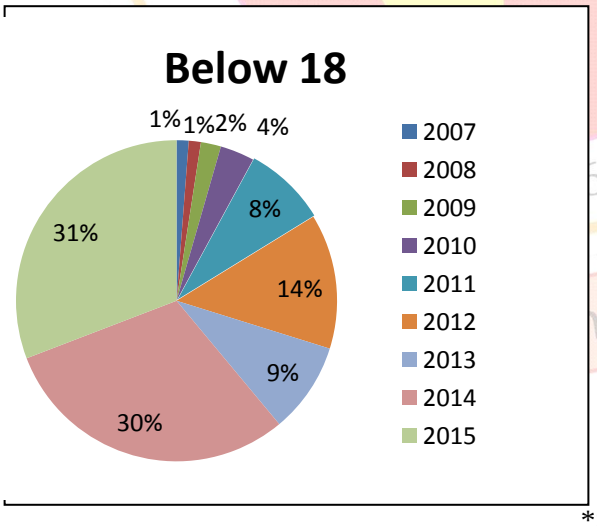
Table 4: Number of Persons arrested under Cyber crime cases during 2006-2015

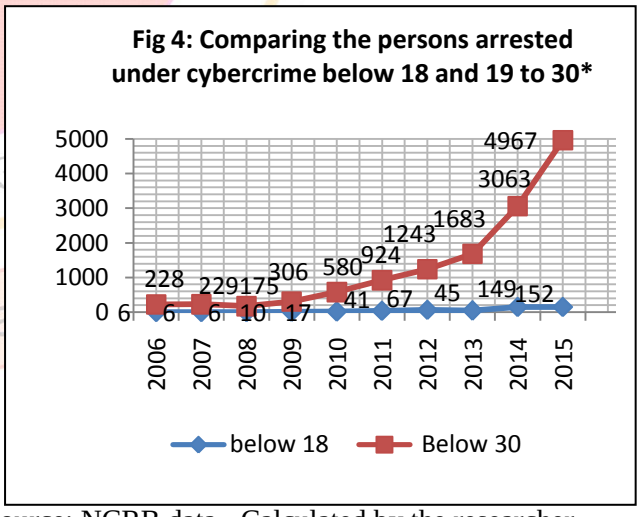
Years	Below 18	18-30	30-45	45-60	Above 60	Total
2006	6	222	260	73	4	565
2007	6	223	283	70	1	583
2008	6	169	168	29	1	373
2009	10	296	202	41	2	551
2010	17	563	491	114	8	1193
2011	41	883	554	139	13	1630
2012	67	1176	657	162	9	2071
2013	45	1638	1325	275	18	3301
2014	149	2913	2293	384	13	5752
2015	152	4815	2642	402	50	8061
Total	**499**	**12898**	**8875**	**1689**	**119**	**24080**

Source: NCRB Cyber crime statistics (2006- 2015) - Calculated by the researcher
***2016 data not available**

Livingstone et al. (2011) remark the growing use of mobile and Internet of ever younger youths, the number of online risks grows. According to NCRB data there were total more than 24000 cases registered under cyber crime. The data given in Table: 4, shows that the registered cases cyber crime cases registered on adolescence below age 18 was 499 and below 30 were 13397 for last ten years. The figure 3 & 4 shows the percentage of persons arrested under cyber crime cases below 18 years.

Figure 3: Percentage of person arrested under cyber crime cases





*Source: NCRB data - Calculated by the researcher

It is inferred from the Table 4, cybercrime cases are increase every year comparing with the early years. Most of the adolescence without knowing the consequences gets in to cybercrimes. The indicated the other stake holders that there is a need to provide more awareness among adolescence about cybercrime and its need training and supervision to use the gadgets in a proper way to reduce the chance of being victims.

Role Of Parents And Stake Holders In Promoting Safety Of Adolescence

Many students have access to 24/7 internet. They perceive internet as a digital communication platform to share their information without any hesitation to a wide variety of individuals. Though internet provide more opportunities of children growth these natures raise concerns among the parents, teachers and community to save their children from hazards and dangers and to provide an awareness among them. The initiatives and measures to address by the stakeholders are discussed below.

Role of Parents

Parents should understand only their supervision protect the children / adolescents from the risk of being victim. There are many factors like family environment, violence in the family, over love without care with freedom are strongly influence students to over use the internet or make them to addict to the internet. Such things should be taken proper care at the home. Safety for children and adolescents, both offline and online, is primarily a responsibility of parents, but where parents cannot or do not sufficiently manage this; it is also a matter of public policy to see that young people are protected. Alongside protecting youths against risks and harm, however, protection also involves fostering self-development and freedom in adolescence. Adolescent autonomy is relevant for youths to develop into responsible and independent adults. Part of this maturing process involves youths conducting risk-taking and experimental behaviour, including online sexual exploration, which as such is perfectly healthy even though it may sometimes involve particular vulnerabilities or harm (Kohnstamm 2009). Somehow, an optimal balance must be found between controlling that which is wrong or involves too high risks, and fostering the freedom and opportunities of the internet that are essential for adolescent self-development. At the same time, online risks are also addressed in policy measures targeted at combating cybercrime. Criminal law is being used to protect (younger and older) youths against potentially harmful behaviour. Consequently, keeping an eye merely on physical, offline experiences is not enough if parents wish to remain involved in their children's lives; their children's online (ad) ventures have become equally important. Parental engagement should be extended to this online reality, which can be rather diverse in the ways in which children use the Internet—including social networking sites, online games, virtual worlds, chat rooms, instant messaging, webcam use, etc. and where they use it at home, at school, and basically anywhere with smart phones. Parents often still seem to be much less aware of what happens online than offline; it may therefore be difficult for them to effectively identify particular online risks their children may run (Van and Koops, 2011). Parents should use parental control software, control the use of internet at late nights, fix proper time and space will help to move away from cybercrimes.

Teachers, School Environment and Community

Next to parents, teachers, school social dynamics and academicians play a critical role in using Internet and strengthening capacity. Community includes the environment where they are living and with whom they are living. Peer groups have a strong influence on every community particularly adolescents. They are the one who can make awareness about the cyber crime activities taking place when children used the technology what sort activities they have to perform and what they have to avoid should made clear to them. Adolescence usage of social media without understanding the consequences should me made clear to them. Teacher and school should made adolescence to aware about the basics security of internet and gadgets, impact of technology on cyber crime, information about cyber law and policies in India to save from cyber crime.

Conclusion

Technology and the internet are acting a global linking all over the world which helps to gain information in any field with a single click. This provide and amazing public accessibility and become a mode of communication like use of data storage, intra and inter organisational emails, management and transfer

social websites and network for netizens. Internet world statistics (2010) report the rate of internet usage was 444.8%. The developments of internet usage provide many benefits at the same time associated with many risk when it was over used. It is the collective responsibility of parents, teachers and policy makers to talk to them about the dangers of internet and to take necessary preventive action to save the internet users from being victims.

References

1. Aggarwal, Gifty. (2015).General Awareness on Cyber Crime. *International Journal of Advanced Research in Computer Science and Software Engineering* ,5 (8), 204-206.
2. Chauhan,S. (2017). 7,482 Cases of Cybercrimes Reported in 2017, One Attack in India Every 10 Minutes. Retrievd from http://www.india.com/news/india/27482-cases-of-cybercrimes-reported-in-2017-one-attack-in-india-every-10-minutes-2341055/ on 25 January 2018.
3. Dubbudu, R.(2016). Most number of Cyber Crimes reported in Maharashtra & Uttar Pradesh, Retrieved from https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/
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. James, R. (2009). A brief history of Cybercrime. *Time.* Retrived from http://content.time.com/time/nation/article/0,8599,1902073,00.html on 25, Janauary 2017.
6. Kohnstamm, R. (2009). Kleine ontwikkelingspsychologie—De puberjaren. Houten:Bohn, Stafleu, Van Loghum. ibid Van Der Hof(2009).
7. Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children Full Findings and Policy Implications from the EU Kids Online Survey of 9-16-year olds and their Parents in 25 Countries.LSE, London: EU Kids Online. Retrieved from http://www2.lse.ac.uk/ media@lse/ research/ EUKidsOnline/ Initial_ findings_ report.pdf. on Oct 2016
8. National Crime Records Bureau (2006- 2015). http/ncrb.nic.in/data portal Retrieved from http/ncrb.nic.in/data portal on 20 October 2015.
9. Crime in India Report. (2016). National Crime Records Bureau (2006- 2015). Retrieved from http/ncrb.nic.in/data portal on 20 November 2017.
10. Ray, S and Ghoshal, A.(2016). Every sixth cybercrime in India committed through social media: NIA ,Hindustan Times, New Delhi
11. Sarma,P.(2014). 450% rise in Assam cyber crime. The Telegraph. July 3, Retrieved from https://www.telegraphindia.com/1140703/jsp/northeast/story_18576563.jsp on 20 October 2015.
12. Vanderhof. S, and Koops, B.J. (2011). Adolescents and Cybercrime: Navigating between Freedom and Control, *Policy & Internet*: 3(2), Retrieved from http://www.psocommons.org/policyandinternet/vol3/iss2/ art4 on Oct 2016
13. Van Kokswijk, J. (2007). Digital Ego: Social and Legal Aspects of Virtual Identity. Delft: Eburon Uitgeverij.