*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. 16, Issue No. 5, April-2019, ISSN 2230-7540*

# Impact of Cyber Crimes on Young Adults in India

**Amit Gupta[1]* Dr. Nitu Nawal[2]**

[1] Research Scholar

[2] Supervisor, Faculty of Law, Career Point University, Kota, Rajasthan

***Abstract – Cybercrime will have a big effect on younger people. Young adults are more likely than any other age demographic to access the Internet, because they are the first victims of cybercrime. This article would discuss how cybercrime impacts and creates challenges for younger generations. Themes such as fitness, in particular emotional wellbeing, are addressed to explain the many cybercrime issues. Many younger people have been trying to kill themselves because they have been victims of cybercrime. This paper would examine all the consequences of cybercrime, including cyber bullying (a kind of cybercrime), and how young people may prevent cybercrime.***

***Key Words – Cyber Crime, Young Adults, Cyber bullying, Advanced Technology, Internet***

----------X----------

## INTRODUCTION

Cybercrime is an expression that is used to define illegal activities in a general way in which machines or computer networks are a weapon, a destination or a crime scene. It also includes typical crimes that are used by machines or networks to permit criminal behaviour. Cybercrime will stop every train on which it is, misguide aircraft during their flight by erroneous signals, bring any valuable military data into the hands of foreigners, stop the e-mail, and trigger any device to fail within a fraction of a few seconds. The current thesis has addressed many dimensions, effects and perspectives of cyber technology with particular regard to cybercrime threats from India. An examination of the legal system applicable for its regulation in India has been undertaken. In order to begin, the measurements of the term 'crime' therefore have to be demarcated. There is also no question that 'crime' is a relative concept, which is common in nature and has clearly shown its existence in all cultures, from old to new. Each company has provided its own definition of illegal behaviour, punished by the political community's express will to rule on society, which has often been influenced by the economic interests of a religious-social-political society. Thus, the behaviour, which has often been conditioned by and marked by the final consequence of these criteria, was "penal responsibility." Parenthetically, as the definition of criminality [has] changed, the types of offenders committing those offences shift with the rise of information technology. The concept of crime marked by religious understanding concerns Indian culture, particularly during the ancient era. The time was famous for the full rule of faith. The intervention of supernatural force found both political and social events in general and the "crime" in particular to have taken place. This time resulted from the demonological theory of crime. Medieval times have shown the revival and restore ages, which gave a modern look to 'crime.' Concepts such as utilitarian method, constructive approach, analysis, ideals of natural justice or laissez faire thoughts, hedonistic ideology and idea of pain and enjoyment became the result of an era that helped open up broader horizons for crime research. Later era opened the way for the revolution in science and industry, and logical interpretation influenced thought. Computer technology services have not gone without inconvenience. And if it makes life too rapid and quick, it will almost stop working in an eclipse of threats from the mortal kind of crime known as 'cyber-crime,' without computers. The abundance of inexpensive, strong, user-friendly computers has enabled more and more people to use them as part of their daily way of life. The offenders continue to depend increasingly on them as companies, government departments and individuals. Cybercrimes are restricted until their conduct and their effect on different levels of community, particularly young people, are properly analysed and understand. In collaboration with the U.S. Federal Bureau of Enforcement, International Computer Crime Squad [CSI/FBI 2006], a Computer Crime and Security Survey 2006 carried out by the Computer Security Institute revealed an alarmingly large amount of companies

experiencing electronic and internet fraud problems. Of the companies that recognised financial damages as a result of computer violations, several were unable to estimate the losses. Machine vireo observed 65%; 48%, in one to five security events, recorded between one and five; Incidents from sources inside the organisation have been identified by 42%; In the last year, 32 percent of respondents had improper usage of their operating systems; Laptop and handheld devices have been thefted 47 percent; in the field of e-commerce: Both participants had some kind of website incidence: 9% indicated that confidential details had been stolen; 6% reported website default; 9% were financially fraudulent. The sabotage was 3 percent. Data protection losses totaled more than US$ 52 million in 2006, which is 30 percent less than that recorded in 2004 for 141 million dollars. However, these numbers only concern 313 respondents, who advised the findings of the CSI / FBI survey and not all businesses in the US. It is worth noting. In January 2006, it was circulated in response to 5,000 businesses with a return rate of 6%.

## CATEGORIES OF CYBER CRIME

In order to collect intelligence, cyber-crime and data interception while an attached tracks data streams to or from a destination. This assault may be carried out to capture intelligence in favour of a future attack or the gathered evidence might be the ultimate objective of the attack. In general, this attack entails sniffing network traffic, yet some data sources may be observed, including radio. The attacker is passive in most types of attack and only regularly monitors the correspondence, but, in certain versions, the attacker may try to set up the data stream or manipulate the essence of the transmitted data. However, the intruder is not the expected beneficiary for the data source in all versions of this assault and differentiates this attack from other types of data collection. The intruder not only observes overt data sources (e.g. networking) and reads the content but also several other data leakage assaults. This is not the same as attacks which gather more qualitative details, such as amount of contact not expressly conveyed via a data source.

### Data Modification

Communications privacy is necessary if data cannot be changed or accessed in transit.

Distributed environment allows a malicious third-party to commit a cyber-fraud by manipulating data as it travels through locations. An unwanted entity on the network intercepts and modifications portions of the data before retransmitting data in a data manipulation assault. The value of a financial transaction from $100 to $10,000 is changed from one illustration. An entire series of correct data was interjected frequently on the network during a replay assault. One example was to replicate a legitimate bank payment transaction of $100 a thousand times.

### Data Theft

Terms used to characterised the unauthorised copy or taking away of knowledge by a company or some other individual. User data, such as codes, social security numbers, payment card details, contact records, or other private organisational information is often used in this regard. Due to the unlawful collection of this material, it is likely that the person who stole this information is apprehended to the maximum degree possible by law.

### Network Crime and Network Interferences

Network Interfere with computer network functionality by entry, transmission, harm, delete, deteriorate, change or delete network data.

### Network Sabotage

"Network sabotage" or inept administrators who are usually responsible for the tasks of individuals. The above may be the only item, or a mixture of items. But if Verizon uses the children's aid to prevent first responders, they could raise network concerns to get the federal government to interfere for public safety purposes. If the federal government obliges these citizens to do as the unions are intended to do and strike, so obviously.

### Access Crime and Unauthorized Access

The insider view of the underground machine cracker is "Unauthorized Access." The movies were shot in the USA, Holland and Germany. 'Unauthorized Access' examines the characters behind computer screens and attempts to distinguish the 'outlaw hackers' media hype from the truth.

### Virus Dissemination

Malicious software which connects to other software. (The victims' systems are destroyed by viruses, worms, Trojan Horse, Temporary bomb, Logic Bomb, Rabbit & Bacterium).[1]

### Related Crimes like Aiding and Abetting Cyber Crimes

In most of the charges against a person, there are three factors. First, another person was guilty of the offence. Secondly, the accused person was aware of the offence or motive of the principal. Thirdly, the individual supported the principal with some kind of support. A legal accessory is normally identified as an individual who helps conduct a crime by another person or others. In certain instances, an individual

responsible for supporting or supplying the offence is aware of it before or after it is committed. A individual who is conscious of the offence prior to it and who provides some kind of assistance to those who conduct it, is legally recognised as "a pre-fact accessory." He or she may help with guidance, acts or financial assistance. A individual who is innocent of the crime, but who assists with the crime, is called a "accessory after the fact"[2,3]

**Computer-Related Forgery and Fraud**

Computer forgery and computer-related fraud constitute computer-related offenses.

**Content-Related Crimes**

Included with contents-related offences are cyber-sex, unwanted commercial contact, cyber slander and cyber-attacks. The estimated expense to victims of these assaults is $1 trillion a year, which is a substantial improvement to developing countries in the situation of undeutschen or underdeveloped countries. The details supplied by a U.S. Base News Agency is essential for certain cyber-crime facts:[4]

1. Studies also shown that in the last two years, one in five internet shoppers in the United States have been victimised by cyber fraud.

2. EMC's Protection Division, the RSA, has published a Q4 analysis of identity fraud, phishing and ransomware, privacy violation and lack of data.

    i. The review finds that 23% of the worldwide population would be attacked with spear phishing, while average websites will be compromised every 4.5 seconds.

    ii. Cybercrime costs companies more than $600 million a year in Australia, while cybercrime costs in the US have fallen to one in five Internet users in the last 2 years, or $8 billion.

    iii. The review also showed that the online protection of users is being even more concerned. A U.S. Consumer Awareness Survey in 2009 showed that 85% of interviewees expressed concern about the safety of transmitting data over the internet, while 59% expressed a desire to increase privacy of their website data.

    iv. Cases of spam, hacking and fraud have been recorded to multiply 50 times between 2004 and 2007.[5]

3. India became the fourteenth nation in the world to host phishing websites in 2008, according to a recent survey. Moreover, the booming of telephony centres in India have created a niche for cyber-crime in the collection of data..

4. Prasun Sonwalkar's words represent India's challenge from cybercrime — In India, the slowdown is turning informal offenders into electronic scams, according to a report carried out by Brighton University academics, quickly emerges as a global centre of cybercrime. Titled 'The Crime Online: computer crime and Illegal Innovation,' the report notes that cyber-crime is a source of 'particular interest' in India, China, Russia and Brazil, and that the large number of callcenters have been the cause of 'cyber-crime breakthrough' in India over recent years. At the UK crime scene, the Association representing police officers has been provoked in FT to claim "police are being left in the background of sophisticated gangs" that the value of online theft in the world is about £50 billion a year. Computer spam applies to unwanted internet promotional advertising, which may often transport viruses and other programmes to machines. The UAB Spam Data Mine analysed millions of spam e-mail messages to date and effectively linked the thousands of advertised Web pages to 69,117 separate hosting domains in spam, said Warner. Warner. Out of the overall domains analysed, 48,552 (70%) had Internet domains — or addresses — ending with the Chinese country code ".cn." In addition, on Chinese machines, 48,331 (70%) of the pages had been hosted. In India, the major cyber-crimes identified are service denial, website defacement, SPAM, computer viruses and worms, pornography, cyber hyper infection and cyber stalking. As cell telecommunications costs in the world are missing or robbed last year for about $120 million, consumers need to encrypt documents, contact information and telephone numbers so they could be misused. Present and former staff and hackers perform almost 69% of stealing of intelligence. In order to secure sensitive records, India must take a great deal. In its first comprehensive survey on Indian Net Scene, Symantec shares the numbers: The nation is the most senior in the world (76%) of legal e-mail traffic with outgoing spam or junk mail. India's home computer owners are its 37.7 million internet users' most targeted sector: More than 86 percent of all assaults, mainly by bots, were directed at lay surfers, with the two most

vulnerable towns in Mumbai and Delhi. Many countries in Africa neglect cyber policies and legislation (many articles and news are available at in this support). Because of that, and so, a cyber-terrorist will escape. Cyber rules and regulations are almost free in countries such as Kenya, Nigeria, Tunisia and Tanzania etc. The above-mentioned text covers only few instances of the horrendous state of cybercrimes in India, the US, Europe, Asia and Africa.

## TYPES OF CYBER CRIME

Telecom services theft Theft Three decades earlier, the "phone phreaker" provided a precedent for a major crime sector. Through accessing a PBX, people or illegal groups may get access to dial-in / dial-out circuits and either make their own calls or offer call time to third parties (Gold 1999). Offenders can access the control panel by the impersonation of a technician, the dishonest obtaining of an access code of an employee or the use of Internet-based software. Any advanced criminals loop between PBX networks in order to avoid detection. Additional services provide the collection of information about the "calling card" and on-sale calls paid to the calling card accounts, including forgery or illegal reprogramming of stored value telephone cards. Communications to promote the offender The operations of criminal organisations are technologically strengthened, just as legal private and public organisations rely on messaging and record keeping information systems. Telecommunications facilities have been used to support systematic drug trafficking, gambling, prostitution, money laundering, child pornography, and the arms trade (in those jurisdictions where such activities are illegal). Crime messages can be beyond the control of law enforcement using encryption technologies. Growing focus has been paid to the usage of computer systems to create and transmit infant portnography. These goods are today available to be imported at light pace through national boundaries (Grant, David and Grabosky 1997). The more obvious forms of internet pornography in children include a moderate degree of coordination as required by IRC and WWW infrastructure. Piracy in telecoms Digital technology makes paper, sound and multimedia variations simple to reproduce and distribute. Many people have proved irresistible in their attempt to replicate copyrights for personal usage, for selling at a cheaper price or indeed for free delivery. The creators of proprietary works have been quite concerned with this. It is projected that market damages in the range of 15 to 17 billion USD are suffered annually due to infringement of copyright (United States, Information Infrastructure Task Force 1995, 131). If designers of a job are unwilling to take advantage of its inventions, in addition to financial failure, it may usually have a refreshing impact on artistic efforts. Offensive materials dissemination In cyberspace content is abundantly found to be unacceptable by others. This contains, amongst other things, sexually suggestive content, racial advertising and manuals for making fire and explosive devices. The mechanisms of telecommunications may also be used to intimidate, threaten or disruptive correspondence from conventional obscene telephone calls to their current manifestations of the "cyber chat." Laundering and tax evasion of electronic money For some years now, flows of electronic money have helped to hide and move criminal profits. Emerging technology can profoundly help to disguise the source of ungotten profits. Legally generated revenue from taxing authorities may even be more readily disguised. The only financial entities able to reach electronic funds transactions that transit multiple jurisdictions at pace of light would no doubt be larger financial institutions. The creation of informal banks and parallel banking structures will allow central bank regulation to be overcome, but also help to prevent the reporting of cash transactions in the countries with them. The usage of telecommunications is going to make traditional underground banks that flourished in Asian countries for decades. Vandalism, terrorism and extinction electronically Western industrial civilization relies, like never before, on sophisticated data treatment and telecommunications networks. Damage to either of these structures or interaction with them can lead to disastrous consequences. If technological intruders are driven by fascination or vindication, they at best trigger discomfort and can do massive damage.[6]

### Sales and Investment Fraud

The widespread application of new technologies to illegal efforts would be even greater as electronic trading is increasing. The usage of telephones is increasingly prevalent in false advertising pitches, misleading charity requests or misleading investment openings. Cyberspace now offers many investment options, from the conventional stocks and shares, to exotic opportunities including coconut cultivation, auto teller sales and lease-back, and international telephone lots. In reality, the modern era has seen unparalleled disinformation opportunities. Fraudsters already have immediate and limited links to millions of potential victims around the world.

### Illegal Interception of Telecommunications

New opportunities for electronic eavesdropping are created in telecommunications. Telecommunications interception is increasingly applicable, from the time-honored practises of monitoring the unfaithful partner to the newest modes of political and industrial spying. Again, new vulnerabilities arise from technical advances here. Another choice is to intercept electromagnetic signals generated by a robot.

Cables may serve as antennas for broadcasting. Existing legislation would not prohibit computer radiation remote control.

**Electronic Funds Transfer Fraud**

Transfer networks of electronic funds have started to proliferate, thus risking interception and diversion of such transfers. Both remotely and physically, valid payment card numbers may be intercepted; data saved on a card can be falsified. Much as an army thief can rob a motor vehicle for a fast getaway, so can telephone systems be robbed and used for vandalism, bribery, or to promote criminal conspiracy. In the context of computer-related crimes, two or more of these generic types combine.

## IMPACT OF CYBER CRIME

Crime as a bad social factor Since crimeless culture is a fallacy, crime is an all-pervading phenomena, and a non-separable element in societal life, the query "Why is there so much crime ado?" is irritating. There is nothing fresh about criminality as one of the characteristics of every society that has been present to date, be it civilised or undeveloped, and is one of the fundamental impulses of human behaviour. It is omnivilized, omnipressant and there is no new thing about crime. However, the social anxiety over the high crime rates should be taken into account not because of its origin but because of potential disturbances that it causes to society. Moreover, several people are specifically victims of violence. Anything that has meaning may be lost to the survivor. Security, harmony, money and property can be fundamental virtues, since they can satisfy several wishes. Cyber crime's effect on social and environmental policy riders Crime is a complex and relative phenomena conceptually and subject to relative sociopolitical and economical shifts in current societal systems. As a result, no systematic understanding of all forms of 'crime' is available at any given period or can be applied to a single definition in any culture. It is affected by the variations in the associated phenomena and value framework generated by these shifts with their dynamicity. A definite increase in corruption-based crimes, in which societal moralization is small and the commission of crime is undermined by fewer social shame, is seen as obvious in today's situation, where money is more important than ideals. Economic crime is, however, at its height. This shows directly the crime interdepends on other societal phenomena, economic processes and political machines. The demographic is also one of the main variables that affect the impact of crimes. A strong association has been found between the increase in crime incidences and the population in the region. Other variables driving crime include the situation in a certain location, urbanisation rates, demographic displacement from nearby countries, housing, economic disparities, [Cyber Crime tech literacy] etc. 2 Around the same moment, too, economic offences are influenced by the system of social giving. Because every crime prevention scheme has something to do with the political system prescribing standards, making laws, creating protective measures, the political process and mechanism affects crime in a particular community. This shows explicitly that the concept of crime is related to socio-economic and political conditions. Cyber-crime effect on young people Cyber bullying is a biggest fear in the minds of young people today. It has been widespread in the past five years, mostly from the age of less than 18 years, and Cyber Bullying is most sensitive and feared by inspection. In our culture it is becoming a disturbing pattern. The worst fear of cyber-crime is among young women according to inspection of results. Cyber bullying is fear of receiving attacks, negativity, or other person's derogatory photos or comments This is primarily achieved by means of the above-mentioned key technology online. You can chat, text messages etc. Cyber Bulling. Where websites such as Facebook, Orkut, the consumer of Twitter is most influenced. My research shows that an individual who is commonly hated will achieve a cap on depression, embarrassment and threats. This research enables one to analyse whether Bulled will be stressed to the extent of self-harm whether he or she is online. Cyber-crime effect on the private sector I might use invasive, quiet and risky terms if I had three qualities to characterised cybercrime. The very silence of this sort of criminality is a big challenge in the fight against the hazard. Indeed, the businesses very often forget that until far after the case they have suffered scams or assaults. The effects are disarming because it is often difficult to find the case again, only like the time difference between this offence and its detection offers advantages to those who perform offences which are sometimes unbridgeable, making persecution impossible. However, the truth is that many businesses are, in fact, over the years the victims of cybercrime but they are not conscious of cancer which destructs them from the inside. It's not all so. But this is true. The Second Annual Cost of Cyber Crime Survey, released by the Ponemon Institute, shows that, while a higher degree of understanding of the cyber threat, the effect of cybercrime has significant financial implications on enterprises and governmental entities, a study is focused on the representative sample of 50 larger organisations. The research is published at the Ponemon Institute. The study reveals that 50 organisations' average annualised expense of cybercrime is $5.9 million a year, ranging from $1.5 million per business, to $36.5 million per year. Compared to the first report in the previous year, the gross costs are raised.

**Impact of Cyber Crime over Youth**

The newest way to communicate is cyber networking. The blogs, instant messaging and e-

mails of online social networking provide consumers with an easy and quick way to communication with others across the globe. Teens spend hours online, especially on computers or electronic devices every day. Family-rescource.com reports that 48% of teenagers agree that the Internet enhances their friendships. With the popularity of social networking platforms, youngsters are able to keep up to real friends online. Some young people claim that cyber interactions allow them to feel sure that they are their true selves. Instant message programmes, which are utilised by approximately 13 million teenagers, facilitate real-time discussions with peers. The path to partnerships with other teens close and far opened by online networking platforms. Writing when adolescents are mostly online has no structured writing skills using cyber communication. Quite the contrary, young people frequently write digitally in jargon, abbreviations or slang. The National Writing Commission says that 85% of adolescents use contact across social networks, but 60% do not see the form of communication as "writing." Teens should consider the distinction between formal and informal writing and understand whether it is not suitable (in school).

**Cyber Bullying**

Online contact between young people has a detrimental impact on cyber bullying. Cyber bullying victims also face rumours and misinformation on social networks online. Bully pictures of their victims can seem indecent or shameful. The use of mean text messaging as harassment is another aspect of cyber bullying. The National Council on Crime Prevention says that over half of the American youth have problems with online bullying. The young took their own lives because of online bullying in some serious situations.

**Sexual Solicitation**

For teens who use cyber communications forms, sexual solicitation is increasingly concerned. It may occur on social networking platforms or in chat rooms. Sexual application takes place anytime an adult or a friend attempts to partake in sexual intercourse online. A teen could be required to share personal details, watch porn or talk about sex online. About 70 per cent of teenagers online are females. Young people should be careful to put provocative images in chat rooms online and to speak with strangers.

## FUTURE TRENDS IN CYBER CRIME

One of the more alarming phenomena is the rate at which cybercrime is increasing. "Last year has been the first year where cybercrime revenue has been higher than that of illicit narcotics sales and this, I think, is over $105 billion.," says Valerie McNiven, U.S. treasury advisor." She said that more "At such a fast pace cybercrime is moving that the police are unable to pick it up. It is certain that the problem can only worsen in the coming years now, as professionals have noticed the windfalls if they are properly used. There has recently been much debate on organised crimes and cybercrime amalgamation. Indeed, such a connection foreshadows an unfortunate odour for the foreseeable future. With several crime gangs from East Europe, Russia, and Asia, with little legislation and compliance, there is little hope that conventional means can control and neutralise the danger. The problem was briefly summarised by Phil Williams, a visiting researcher at CERT. "The internet offers all criminal networks and goals and can be used with very little risk for significant gains. It's hard to call for more for organised crime." As a consequence, the advanced phishing attacks and other means that can be two-way identity fraud can be predicted to increase. For example, call centres may be used to alert consumers in advance of a problem and then track emails that need personal details. In several third-party data centres, the addition of personal details can prove to be useful goals for infiltration. Criminals employing data-mining technology to locate the most vulgar customers or to customise phishing emails for real individuals depending on their medical, financial or personal backgrounds are not difficult to envision. Theft can now be identified in more automated ways. Botnet, for example, can be used to locate personal data, such as credit card details and social security numbers, not only for denying service and spam assaults. Botnet controllers may accept reimbursement for their "database" requests. It begins to wonder where all technological know-how can come to conduct cybercrime for experienced offenders manager of money-laundering and the organisation of those systems. Unfortunately, there are increasing amounts of smart, university-wide blackhats, often working in countries where legal work is insufficient and the risk of getting captured is small. But it's more troubling to be a hacker willing to do big damage to networks and execute cybercrime than ever before. The Internet provided an information base where anyone can learn the basics of computer systems subversion, and with several videos accessible that describe almost laypeople how to carry out a buffer overflow or a mid-attack guy. It is interesting because those who are not taking the initiative to study and discover new achievements are not the main challenge. Indeed, this community is likely to remain a tiny, very smart network of researchers and protection organisations focusing exclusively on software troubles. This requires a degree of investigation, expertise and persistence that the majority are unable to spend even though someone is inspired to understand how the exploits function. The actual threat is due to the deep simplicity with which someone may execute a programme, such as "MetaSploit," a system that enables new modules to be instantly downloaded and run. In addition to the

way one works, the perpetrator simply has little to do with machines. Really, with almost all assaults, a tiny number of individuals work diligently, and eventually they are published to the public domain, which allows virtually anyone to carry out the assault. Botnets are no longer handmade apps by one party, which has really understood its underlying principles, but instead open-source community projects to ensure that distributed computers like BotNET, Eggheads and CSharpBot, all accessible from Source Forge, can be controlled as easily as possible. The barrier to entrance to the sector is so minimal that nearly anyone will experiment and enter cyber criminals. With the learning curve too short, a debate over how to prevent and cope with offenders in a manner that is no longer bound to outdated approaches should be prompt. For example, once anyone enters the home, they need to prepare not just for the right time, but also to be mindful of the seizure of locks, evasion of the protection framework and a gulf in overcoming moral thresholds. In contrast, cybercrime's ease appears inversely related to its profitability and, in addition, these patterns suggest signs of acceleration.

## CONCLUSION

The Internet's future remains for predators and ordinary people to grab. There are also many fears of cyber apocalypse, while the possible harm to large-scale fraud is almost limitless. These fears should be rationed, knowing that the issues are dealt with, but just not quickly enough. The value of the Internet has been shown in a number of respects that I believe would be sufficient to prevent it from being a wasteland for crime and a bastion for evil people. The government also has an important part to play, but private companies who produce apps and others that are able to deter fraud have to do much of protection. Consumer outreach services concern just a minority of potential victims. The others must be covered immediately by steps not stressing and requiring significant involvement. If it does function, security must be simple and effective. It cannot be said if cybercrime is a relevant problem ten years from now, so as the Internet continues to increase it must be addressed such that cybercrime's realities are proportional to, if not greater, real crime. The position and contribution of parents and teachers is essential in order to monitor and avoid the effect of cyber-crimes on young people so they can empower them to better use it without being held up by incompetence and unregulated behaviour.

## REFERENCE

1. DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-

2. IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/,

3. Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml, Visited: 28/01/2012

4. Legal Info (2009), Crime Overview aiding and abetting or Accessory, Available at: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html, Visited: 28/01/2012

5. Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/forensic/cybercrime.htm,

6. Hundley and Anderson 1995, Schwartau 1994

**Corresponding Author**

**Amit Gupta***

Research Scholar