CYBERCRIME IN INDIA

SAURABH SOTWAL
National Law University Odisha,
Brajbiharipur Near Naraj Barrage, CDA- Sector 13, Cuttack- 753014
Email: 13ba035@nluo.ac.in

ROHIT KUMAR
National Law University Odisha,
Brajbiharipur Near Naraj Barrage, CDA- Sector 13, Cuttack- 753014
Email: 13ba035@nluo.ac.in

ABSTRACT

The aim of this paper is to study the effect of cybercrime on society. The objective is to bring the awareness in society regarding all these cybercrimes and suggesting them to take preventive measure to tackle these kinds of problem. The scope of this research paper is the full analysis of the cybercrime and its laws. But the researcher limited herself to the sociological perspective of cybercrime. This paper deals with concept, types, intention, motive, role of government to prevent cybercrimes in India. This paper also deals with the present IT Act in India. In this paper as strong emphasis is made on the impact of the cybercrime on Indian society.

KEYWORDS: Cybercrime in society, concept, types, role of government, IT Act

INTRODUCTION

Present age is the age of automation where man is shifting his maximum burden on machines to get work done. The Computer Technology is helping the present human civilization to such a great extent that without computers their life seems to be impossible. Cybercrime is the word which we are reading in the newspaper and seeing in the TV more often. But we still do not know about it. The increasing need of internet of individuals and organizations has resulted in a corresponding increase in cybercrime. Because of lack of proper training and education, lack of awareness of cybercrime in Indian society, cybercrime increased. Even the officers do not have the proper training and expertise to tackle cybercrime. Although there are firewalls, antivirus software and technological solutions for safeguarding the data but in India there is need of much effective use of technologies for safeguarding the important data. Along with the advancement in technology it is also necessary to be aware of cybercrime and related issues. Every cyberspace should provide safety to the data. The cyber-safety depends on the knowledge of the technology, the care taken while using the internet and preventive measures adopted by users and server system. Therefore there is a need to enhance the awareness about cybercrime. India needs technological and legal awareness and proper education and training to combat the growing danger of cybercrime.

The researcher in this paper is going to study the cybercrime. And also study its effect on society and the laws of cybercrime. The first section deals with concept of cybercrime, the definition of cybercrime and its types. The second section deals with the concept of
cybercrime in our society. And researcher also described the effect of cybercrime on our society, studying the behaviour of victims as well as cybercriminals. Third section deals with the need of cyber laws in India. Fourth section deals with measures taken by government to tackle cybercrime and suggestion for individuals to take preventive measures.

CONCEPT OF CYBER CRIME

Cyber is a prefix used to describe a person, thing or idea as a part of the computer and information age. Cyber term is coined by Norbert Weiner. The virtual world of the internet is known as cyberspace and the laws governing this area are known as the cyber laws. Increasing use of cybercrime leads to the need of knowing more about cyber. We need to know what exactly cybercrime is.

International organization provided the clear concept of cybercrime. On the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, matter of crimes related to computer networks was raised. Then the meaning of cybercrime was wrecked into two categories and distinct thus:

- Computer crime: Any illegal act by means of electronic working that aims the security of data and computer systems processed by them.

- Based on Computer crime: whichever illegal conduct committed by means of, or in connection to, a computer system or network, including crimes as illegal control and distributing or offering information by way of a computer method or network.

Individual criminal activity is in which computers are a place, a tool, or a target of criminal activity. Computers are used as a tool to commit crime such as Pornography, threatening emails, assuming someone's uniqueness, sexual harassment, slander, SPAM and Phishing. And another type of criminal activity is when computers become the target of crimes. For example viruses attacks, worms and industrial espionage, software piracy and hacking. Hence, the computer is either used as a tool to commit crime or as a targeted victim. But under Indian Law, there is no such definition of cybercrime in any legislation. Crime relates to computer network are divided into three categories viz. Crime against person, property and government. The researcher discussed it below-

a) Against Property- It means cybercrimes against all forms of property. These crimes include the destruction of other’s property, intellectual property crimes, internet time thefts and transmission of virus and harmful programs.

b) Against Government- the most common cybercrime against the government is cyber terrorism. Individuals and groups use the cyberspace to threaten the international governments and moreover to terrorize the people of a country. When an individual "cracks" into a government website then this is called cyber terrorism.

c) Against Persons- This category includes various kinds of crimes such as transmission of child pornography, harassment of anyone via mails, cyber-stalking, indecent exposure, email spoofing etc.

These are major crimes that we see now days. Most cybercrime is against government and persons.
The people of our society are not fully aware of the types of cybercrimes. People come across so many problems but they don’t know what these are. There needs to be clarity between the types of cybercrimes. The types of cybercrime are as follows -

**Cyber-stalking**

Cyber-stalking is the use of the internet, through electronic communications or emails to stalk, and in general it refers to a pattern of malicious or threatening behaviours. It is a continuous process and done repeatedly by a stalker. Cyber-stalking may be considered the most dangerous of Internet harassment, based on a getting credible threat of harm. It involves person’s actions across the Internet by posting messages which are sometimes threatening, entering the chat rooms often used by the victim, constantly bombarding the victim with emails. Therefore, cyber stalking is a serious offense and need to be tackled.

**Hacking**

It is a crime which means cracking system and getting unconstitutional access to the data stored in them.

**Phishing**

It means trying to fool people in parting with their money. For example, unsolicited emails of financial institution requesting customers to enter their name, password and other personal information to access their account. And when the customer click on the link fraudster has the access to his bank account and the funds in that account.

**Vishing**

It is a criminal perform of using social engineering and Voice over IP (VoIP) to entrance private, personal and profitable information from the peoples for the reason of financial reward.

**Cyber-squatting**

It is an act of making and registering a domain name and sale it for a fortune.

**Online credit card fraud**

It is the illegal online acquisition of a credit card number and use of it for unauthorised purposes, such as fraudulent purchases.

There are other various cybercrimes which harm the persons and their property. Understanding types of cybercrime and basic prevention technique can help people evaluate whether they have adequate defences or not. Depending upon the type of cyber problem people are facing, they can accordingly take measures to prevent it.

**CYBERCRIME IN SOCIETY**

For a sociologist it is important to know the effect of cybercrime on society and to see the social behaviour of individuals. The researcher in this section tried to study the cybercrime from the perspective of sociology.
Crime is term define by the social and economic phenomenon and also the human society. In another word Crime is a legal belief and has the sanction of the law. A crime might be said to be any behaviour accompanied by omission or act prohibited by law and substantial breach of which is imposed by penal consequences. As said by Henry Thomas Buckle, “Society prepares the crime, the criminal commits it.” Crime has there been in society since ages but it has more impact in the present world than ever before. If we see the world of today and the past, we can absolutely see the change in our way of life. The definition of crime has not changed but the means to commit crime became fast and easy.

For instance take technology; it brought the positive change in our life but along with negative changes. Everybody’s life is transformed because of technology. Technology has definitely brought changes in our society. On the mainly part these changes have been helpful. Ameliorations communication and entertainment have afforded us many benefits. It transformed the method we work, shop, speak, learn, and perform banking action. Cybercrime has also increased and expanded with the increase and expansion of positive aspect of technology. Though the internet and other information technologies are bringing profit to society, they also give new opportunities for criminal behaviour. This situation drastically affects our society. In our current society most citizens are considered cybertizens. With this increase in cybertizens, there is an increase in cybercrime.

**Cybercrime is a heavy burden on society.**

Companies are so bothered that recently Microsoft opens a quarter of a million dollar prize for the capture of the individuals answerable for the MSBlast worm and the SoBig F virus. These cybercrimes are also against law enforcement and government agencies. The fact is that technology has brought about a lot of positive changes in society. It is only people’s use or use wrongly of technology that is harmful. Therefore we cannot prevent using the computer and the technology connected with it.

One side it is easy for the criminals to execute and operate their intentions and on the other side victim faces traumatised situation where she feels exposed to the world.

Why and how the internet or cybercrime is a threat to our society? The answer is in the nature of our technology. First of all internet is easily accessible to people. The personal computer is common in every household and the internet is also available from all parts of the globe. Access to the internet is very fast and easy. For example with the help of 3G network, individuals can access to the internet in seconds. Increasing cybertizens is one of the reasons. The users of internet are rapidly increasing.

It also affects the privacy of the people. The cyberspace used by internet users generates a blueprint of our entire behaviour when we navigate through a health plot, pay our bills, or shop for books at Amazon.com. This data composed by surfing through all these domains generates a profile of who we are. When hackers steal this information and it becomes a gross infringement of our privacy.

This act of cybercriminal has a very serious effect on victim. Cybercrime can affect victim in many ways and the impact of stalking may depends upon the victim’s characteristics, past
experience, current circumstances etc. It can affect their mental health – frustration, self-blame, fear, terror, anger, panic attacks, feeling isolated and helpless to stop the harassment etc. are some example of effect on mental health. Effect on physical health – dizziness, shortness of breath, headaches, hypertension, heart palpitation and sweating are some example. It also affects your work and school life like changing career/school, deteriorating performance, taking leave often etc. Some of the effects on social life are victim move to new area, inability to trust others, physical and emotional intimacy and avoidance of usual activities. Hence, the victim is highly affected by the act of stalker. Victim is affected mentally, physically and socially. Because of fear, victim does not take part in usual activities and became isolated from society. Being a part of society victim finds it very difficult.

![Top 10 emotional reactions to cybercrime](image)

**Figure 1 Reactions of victims of cybercrimes**

Generally any one can be victim of cybercrime but cybercriminals have their targets. People of society are more targeted than other. The following are-

1) Naïve/ Gullible – they target people who are easy to deceive. Usually older people are prone to being scammed as they are trusting and helpful people. On a more dangerous level are children. They believe people they meet on the net are as trustworthy as their parents.

2) Desperados – these people are desperate for quick case. They easily fall prey for such cybercrime information such information as “get rich fast”, “you won 2 crore rupees call on this number” etc.

3) For friendship – especially teenagers and children are the victims who are desperate for friendship. The result is that they are most likely to be harassed.

4) Inexperienced – the people who have limited knowledge such as rural and older people. They are incapable of protecting their computer from cybercriminals. Worse, they may not be aware of such crimes, therefore become easily fooled.
Therefore, the victims who are easily and more targeted have to take more safety measures and they need to be alert about all these technologies.

Why the cybercriminals do such act? What is the intention behind their act? The behaviour of every human being has a social aspect; it is the subject of sociology. Every human activity is based on reason.

- Cybercriminal envies victim,
- He is obsessed and needs to fulfil his wishes or cravings.
- He may think that he or she is invincible because no one can “see” what they are doing
- He is unemployed or not happy with his/her current job/career and needs a distraction or wants to intimidate you and make you feel inferior
- He is delusional or wants to instil fear in you to justify his/her status
- He wants to embarrass you or is curious.

Therefore, there are social, economic and emotional reasons behind the acts of stalker.

The first recorded case of cyber-crime took place in 1820. However, India’s first case of cyber stalking is recently registered by Delhi Police. One Mrs Ritu Kohli filed a complaint to the police against anyone who was using her individuality to chat over the internet. She also complained that the person is giving her address and using her name and was chatting obscene language. The same person is giving her telephone number to another to encourage them to call Ritu. Consequently, Mrs Ritu received almost 40 calls at odd hours in three days. This created havoc in her personal life then she decided to complain to police.

Police investigated the entire matter and arrested Manish Kathuria on the said complaint. A case was registered under section 509, of the Indian Penal Code (IPC) but he was released on bail. The case of cyber stalking was reported first time in this case. Cyber stalking is a latest phenomenon and women usually are the main targets of this cybercrime. This case raises numerous Cyber law issues. The above case was registered under section 509, IPC which does not exactly cover cyber stalking.

Therefore, where the victim will go? What remedy will victim get under Indian law? This case raises so many questions about the Indian law. Awareness amongst the law enforcing agencies and legislature regarding this new cybercrime is needed to be created in order to enable its earlier regulations.

Keeping this in mind India formulated a special law for cybercrimes. In the next section researcher will study the cyber-law in India. Cyber security should take strict action.

**CYBER LAW IN INDIA**

The group of every human being needs to be controlled. Human beings live in social groups. And social control regulates the behaviour of members of the group. Social control is necessary in every human group. Social control is basically the enterprise subjecting the human behaviour to the governance of rules. The law is generally looked as sub-set of social
control. As Griffith said in his article, social control is genus and law is its species. Therefore, social control and law cannot be separated. Social control is used to regulate every individual and group but the law is used more in complex forms of society. Laws must be interpreted sociologically. As Roger Cotterrell said, “legal ideas are means of structuring the social world, and to appreciate them in this sense and to recognize their power and limits, it is necessary to understand them sociologically”.

Hence, in today’s complex society there is need of law to regulate the individuals and human groups. Therefore to deal with cybercrime, there is one branch of law i.e. cyber law.

Cyber law is that branch of law that deals with legal issues related to use of the internet. In simple terms, cyber law is the law governing computers and internet.

Cyber law is important because it deals with all the transaction and activities relating to the internet and cyberspace. Cyber law includes laws relating to – cybercrimes, electronic and digital signatures, intellectual property and data protection and privacy. In the present technological environment, the world is becoming more and more digitized and even the crimes. And only cyber law deal with all legal issues related to the internet and computer. The need for cyber law is increasing because of an increase in the number of internet users. Cyber law is necessary to provide safety and assurance to the internet users. Cyber law ensures that law is there to provide justice to the victim of cybercrimes. Cyber law is essential because in today’s world, almost everything is digitalized such as online shopping, government forms are now filled in electronic form, billing by shopkeeper etc. Cyber space generates moral, civil and criminal wrongs activity.

In India cyber law is needed because of several reasons. In India there are so many laws. Numerous laws have been enacted and implemented. But these existing laws were enacted by keeping in mind the relevant social, political, economic and cultural scenario of that time.

But now the time has been changed and means of crimes also became faster. At that time no one visualized about the computers and internet. The existing laws cannot be interpreted in the light of emerging cyberspace and cannot include all aspects of different activities in cyberspace and if it does, the law will include perils and pitfalls. And no existing law gives any sanction to the activities involved in cyberspace. Internet requires the legal infrastructure which can be provided by relevant cyber laws. Therefore in India there is need of separate law for cyberspace i.e. cyber law which can exclusively deal with its matter.

CYBER LAWS IN INDIA were officially born on 17th October 2000, when the Information Technology Act, 2000 came into force. This act is the primary source of cyber law in India. This act deals and regulates the use of computer, internet, systems, networks and data. The following act was amended by Information Technology Amendment Bill, 2008 which came into effect from 27/10/2009. The Amendment was created to address issues that the original bill failed to cover. It accommodates the further development of IT and related security concerns since the original law was passed. Before the act was passed IPC was dealing with the cases of cybercrimes. Some section under IT act deals with the types of cybercrime which are discussed above.
<table>
<thead>
<tr>
<th>S No.</th>
<th>Offences</th>
<th>Section under IT Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Tampering with computer source Documents</td>
<td>Sec. 65</td>
</tr>
<tr>
<td>2.</td>
<td>Hacking with computer systems , Data Alteration</td>
<td>Sec. 66</td>
</tr>
<tr>
<td>3.</td>
<td>Sending offensive messages through communication service, etc</td>
<td>Sec. 66A</td>
</tr>
<tr>
<td>4.</td>
<td>Dishonestly receiving stolen computer resource or communication device</td>
<td>Sec. 66B</td>
</tr>
<tr>
<td>5.</td>
<td>Identity theft</td>
<td>Sec. 66C</td>
</tr>
<tr>
<td>6.</td>
<td>Cheating by personation by using computer resource</td>
<td>Sec. 66D</td>
</tr>
<tr>
<td>7.</td>
<td>Violation of privacy</td>
<td>Sec. 66E</td>
</tr>
<tr>
<td>8.</td>
<td>Cyber terrorism</td>
<td>Sec. 66F</td>
</tr>
<tr>
<td>9.</td>
<td>Transmitting or publishing obscene material in electronic form</td>
<td>Sec. 67</td>
</tr>
<tr>
<td>10.</td>
<td>Publishing or transmitting of material containing sexually overt act, etc. in electronic form</td>
<td>Sec. 67A</td>
</tr>
<tr>
<td>11.</td>
<td>Punishment for transmitting or publishing of material depicting children in sexually explicit act, etc. in electronic form</td>
<td>Sec. 67B</td>
</tr>
</tbody>
</table>

Figure.2 cyber law under IT Act

The Indian Penal Code (as amended by IT Act) penalizes several cybercrimes some of them are as follows-

<table>
<thead>
<tr>
<th>Offences</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending threatening messages by e-mail</td>
<td>Sec. 503 IPC</td>
</tr>
<tr>
<td>Word, gestures or intentional act to insult the modesty of a woman</td>
<td>Sec. 509 IPC</td>
</tr>
<tr>
<td>Sending defamatory messages by e-mail</td>
<td>Sec. 499 IPC</td>
</tr>
<tr>
<td>Bogus websites, Cyber Frauds</td>
<td>Sec. 420 IPC</td>
</tr>
<tr>
<td>E-mail Spoofing</td>
<td>Sec. 463 IPC</td>
</tr>
<tr>
<td>Making a false document</td>
<td>Sec. 464 IPC</td>
</tr>
<tr>
<td>Forgery for purpose of cheating</td>
<td>Sec. 468 IPC</td>
</tr>
</tbody>
</table>
The law should cover all types of cybercrime. The present law is difficult to apply.

PREVENTING CYBERCRIME

How one can deal with the entire cyber problem. The government took the initiative and enacted a law on cybercrime to tackle it. FBI sets up Cyber Division in addition to counterterrorism, counterintelligence and the criminal division. The FBI has further partnered with local states and other Federal agencies in the divine to combat cybercrime. And they also enacted laws which put stiff penalties on criminals.

Various programs are introduced by government to tackle this problem, because of the rising use of computer and information technology in different features of daily life and at a point when there are rising discuss about Internet security. Recently University Grants Commission (UGC) has issued an announcement to colleges to set up cyber security and information security as a matter. Students of different technical courses at the undergraduate and postgraduate degree will now have to study a new subject: cyber security and information security. As a many commercial business actions were online and the instances of fraud were growing, there was a need to generate more human resources in cyberspace.

Apart from the measures taken by government, individual also needs to take measures for his/her safety. Prevention is always better than cure. Internet users must take blocking measures to tackle the cybercrimes. Internet users must keep in mind the following things

1) To stop cyber stalking avoid revealing any information about you. This is as good as revealing your identity to strangers in public areas.
2) Always avoid transfer any photograph online mostly to chat friends and strangers as there have been many incidents where photographs are wrongly used.
3) Use newest and update antivirus software to protector against virus attacks.
4) Maintain backup volumes so that one might not lose data in case of virus contamination.
5) Keep in mind never send your credit card number to every site that is not protected, to guard against deceits.
6) Always keep a watch on the websites that children are accessing to avoid any kind of stalking or depravation in family.
7) It is improved to use a security program that gives manage over the cookies and forward information back to the plot as leaving the cookies unguarded might prove lethal.
8) Web site owners must watch traffic and check every wrongdoing on the site. Putting host-based intrusion observation devices on servers may do this.
9) Always use of firewalls may be helpful.
10) Web servers managing public sites must be physically divide protected from internal corporate system.
CONCLUSION

Cybercrime is one form of crime which is done through computer and internet. In one type of computer crime is used as a tool to commit crime. In another type of computer crime is used as target for crime. Both types of crime are increasing in society. Fear is increasing in society because the cyber criminals target the people of society. The victims of cybercrime are those people who are innocent, easy to deceive and trustworthy. Most common cybercrime in which girls and women are targeted is cyber stalking. Girls who are using the internet are most targeted by cyber criminals. For example recently actress Mona Singh morphed video leaked on the internet. Victim of cyber-stalking are mostly girls. And after being victim of such crime, they become isolated from society. They cannot move freely or exercise their rights because there is always fear that someone is watching you.

The truth is that the criminals have changed their method and have started relying on the advanced technology, and in order to deal with them the society the legal and law enforcement authorities, the private corporations and organizations will also have to change. Therefore, India enacted cyber law i.e. IT Act. And in every city there is cyber- crime cell investigation which deals with the problem of cybercrime. But still there is need of separate law for cybercrime which should deal with all types of cybercrime. People use internet and social networking site for the social purpose, to interact with people and to become socially active. People should be social but also should beware. The capacity of the human mind is difficult to measure. It is not possible to eliminate cybercrime from the cyberspace. This is quite probable to check. History is the witness that no enactment has succeeded in completely killing wrongdoing from the globe. That only probable step is to make people awakes of their rights and duties. People should report crime as a combined duty in the direction of the people. The law should be more stringent to check the crime. There is also need to make changes in the IT Act. It does not include half of the crime such as cyber stalking, cyber harassment.”

REFERENCES

2. J. Griffith, The idea of sociology of law and its relation to law and to sociology, 51.
3. Websites