International Journal of Multidisciplinary Education and Research
ISSN: 2455-4588; Impact Factor: RJIF 5.12
Received: 01-09-2019; Accepted: 03-10-2019
www.educationjournal.in
Volume 4; Issue 6; November 2019; Page No. 01-06

A study of prospects and legal frame work of cyber-crime in India

Krupamani
Assistant Professor, Department of Psychology, Maharani Women's Arts, Commerce and Management College, Seshadri Road Bengaluru, Karnataka, India

Abstract
Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber Crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds. The present research paper brings about the facts and the form in which cybercrime is done in the normal usage. The legal framework for the Information Technology is definitely a concern.

Keywords: cracking, fraud, law

Introduction
The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber-apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious. The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programs will only affect a percentage of possible victims. The others need to be automatically protected through measures that are really effective.

Cyber violence is undoubtedly the new emerging form of violence in the 21st century and cybercrimes the most challenging crimes of recent times. Emerging in the 21st century, cyber violence has fast become the most severe issue challenging our security and privacy. It is serious in case of states like India where information technology facilities are widespread but legal awareness in general is low. The legal structure of India and the law enforcement agencies are not yet well-equipped to deal with cyber violence or cybercrimes. Crimes against women form a crucial part of cybercrimes in India and the online platform is now the new platform where women's dignity, privacy and security are increasingly being challenged every moment. Trolling, abusing, threatening, stalking, voyeurism, body-shaming, defaming, surveillance, revenge porn and other forms of indecent representation of women are rampant in the cyber world. In cyber-crimes against women the effect is more mental than physical while the focus of the laws ensuring women's security is more on physical than mental harm (Cyber, 2018).

Statement of the Problem
In India each and every minute one person become internet users. its convergence with digitally supported platforms and gadgets, safeguarding the parents as well as students from the cybercrimes is becoming a challenging task. In addition to, the pinching reality is that the internet users are not getting updated on the vulnerable cyber threats and security issues, at the pace they are getting updated with the usage of internet enabled tools and apps (Shah, 2016) [10].

Need for the study
Cybercrime is evolving at an astounding pace, following the same dynamic as the inevitable penetration of computer technology and communication into all walks of life. Whilst society is inventing and evolving, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it. To avoid giving cybercriminals the initiative, it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements so that they can adjust their methods appropriately **(**Yougal Joshi, 2013) [13].

Review of literature
Shah (2016) [10] iterates that in India Cyber Crime case are registered under Information Technology Act, 2000 and Indian Penal Code. Information Technology Act, 2000 signifies legal recognition for transactions carried out by means of electronic data interchange and electronic communication commonly termed as "electronic commerce", which involve the use of alternatives to traditional paper based methods of communication and storage of information (Shah D., 2016) [10].

Dashora (2011) [4] propounds that the world of internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for

millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind (Dashora, 2011) [4].

Kumar (2017) [8] feels that the technology has made us a global community in the literal sense of the term. Mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Ideas will flee from manipulation or onerous regulation of its value or use and no government can restrain it for long. Human experience has shown that every technological change brings with it some unforeseen problems, taking advantage of which the law breakers explore new techniques to perpetrate their criminal activities. Internet is one such gray area, which has given rise to the menace of cybercrimes. The computer based global communication system has crossed the territorial borders thus creating a distinct field for online activity warranting global attention (Kumar, 2017) [8].

Mohanaprakash (2005) [9] propagates that with the rapid technological developments, our life is becoming more digitalized. Be it business, education, shopping or banking transactions everything is on the cyber space. There are some threats posed by this incredible rise in digitization which is creating a new set of global concern called as Cyber Crime. It is easy to fall prey to such unethical way of hacking and penetrating into personal life which is feasible at a click of a button. Cyber Crimes thereby take place in many forms like illegal access and theft of data, intrusion into devices and fraud which is a big concern amongst all the users. The researcher identifies the importance of being acquainted with the effects of Cyber Crime keeping in mind the recent activities that have taken place and offering solutions to protect oneself from it. Moreover, highlighting the need of being cyber safe and how such illegal activities can be a problem for us (Mohanaprakash, 2005) [9].

Desai (2016) [5] feels that the Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of Internet. Dishonest and greedy people take advantage of easy and free access to Internet and perform any acts to satisfy their needs. The need could be physiological or psychological in nature. Online shopping and wide use of “social media” are root cause of Cyber Crimes. Much awareness created for Cyber Crimes and users were educated. But still people do not complain it to authorities. Even somebody do it then also police or crime branch unable to clear such complains in reasonable time period. Delay in justice will lead to NO registration of complain. This is not healthy situation in free democratic India (Desai, 2016) [5].

Alpana (2016) [1] observes that the user of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a base of communications around the world. There has been tremendous growth in use of Internet. Due to this cybercrimes increases day by day. Cyber Crime is technology based crime committed by technocrats. This paper deals with Variants of cybercrime like terrorist attack, cyber extortion, crimes against individuals, crimes against property, and crimes against organization. It also includes impact on the real world and society, and how to handle Cyber Crimes (Alpna, 2016) [1].

Definition of Cyber Crime

The term Cyber Crime may be judicially interpreted in some judgments passed by courts in India, however it is not defined in any act or statute passed by the Indian Legislature. Cyber Crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark sides too. Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber-defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or internet (Cyber Crime and its Classification).

Cybercrime, or computer crime, is crime that involves a computer and networks. Cyber Crime 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 and mobile (Mohanaprakash, 2005) [9].

Kinds of cyber crime

The Internet space or cyber space is growing very fast and as the Cyber Crimes (T.C.Panda, 2012) [12]. Some of the kinds of Cyber-criminals are mentioned as below.

- **Crackers**

These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

- **Hackers**

These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

- **Pranksters**

These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.

- **Career criminals**

These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude

capture".

- **Cyber terrorists**

There are many forms of cyber terrorism. Sometimes it is a rather smart hacker breaking into a government website, other times it is just a group of like-minded Internet users who crash a website by flooding.

Categories of Cyber Crime

In general, a Cyber Crime can be classified into the following three categories: In general, a Cyber Crime can be classified into the following three categories:

1. *Target Cyber Crime:* It is a crime wherein a computer is the target of the offence.
2. *Tool Cyber Crime:* It is a crime wherein a computer is used as a tool in committing the ffence.
3. *Computer incidental*: It is a crime wherein the computer plays only a minor role in the commission of the offence.

According to the Information Technology Act, 2000 a Cyber Crime can be defined as "an act or omission that is punishable under the Information Technology Act, 2000". This however is not an exhaustive definition as the Indian Penal Code also covers certain cyber-crimes, such as email spoofing and cyber defamation, sending threatening emails, etc (INDIA, 2016) [7].

Cyber Crime Variants

There are a good number of Cyber Crime variants. A few varieties are discussed for the purpose of completion. The following is the list of Cyber Crime variants.

Cyber stalking

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year.

Phishing

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. F-Secure Corporation's summary of 'data security' threats during the first half of 2007 has revealed that the study found the banking industry as soft target for phishing scams in India.

Cross Site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private. personal and financial Information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymitcontact details and telephone numbers as these could be misused.

Magnitude of Cyber Crime

Nearly 69 per cent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information. Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability. y for the billpayer. Vishing is typically used to contact details and telephone numbers as these could be misused. Nearly 69 per cent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information. Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability (Goyal, 2012) [6].

Cyber Laws in India

Cyber Crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview Cyber Crimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

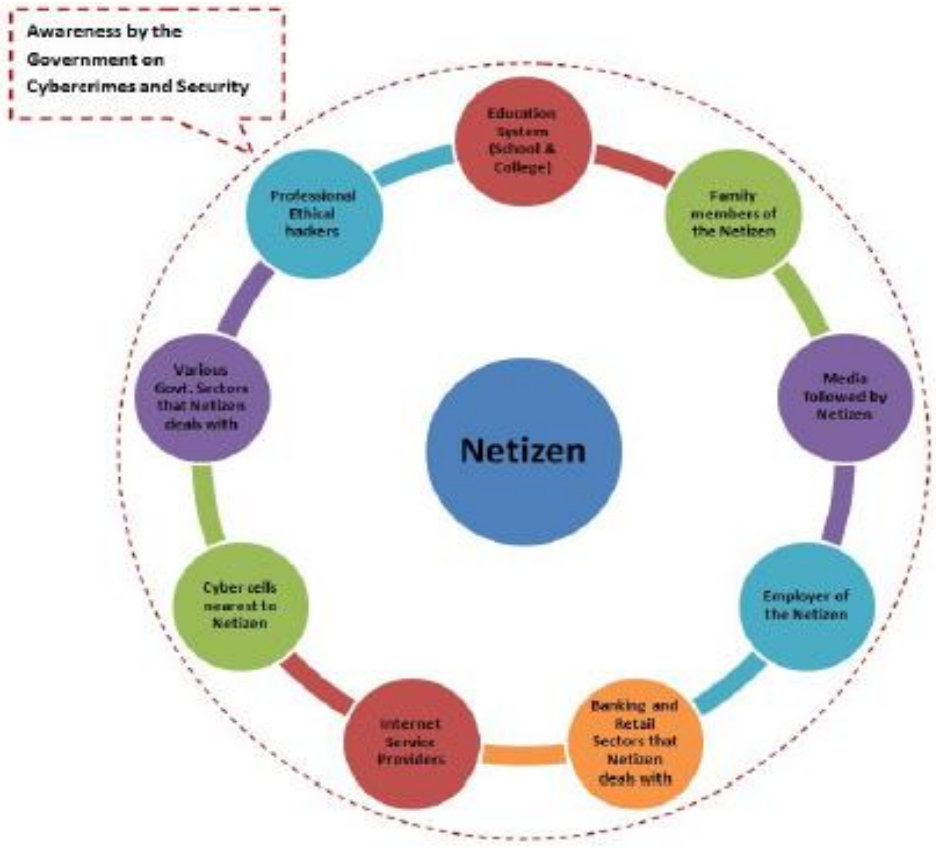

Fig 1: Conceptual model for creating awareness on cybercrimes

As the dotted red line indicates, the Government can take initiative of creating awareness among netizens and stakeholders at various levels, with multiple approaches, like o Inform and educate all the stakeholders on cybercrimes and security measures as they deal with general public on a larger scale through internet (Shah, 2016) [10].

- Informing, educating and altering the netizens through those stakeholders that he deals with by using Internet for various transactions. For instance, the bank can take the responsibility to alert the customer through personal counselling or by providing information whenever required.
- Encouraging cross-flow of knowledge and information between media, cyber cells, ethical hackers and education sectors to reach the netizen in easiest and appropriate way.

Controlling Cyber Crimes (Role of Technology)

Steps to prevent Cyber Crime:-

1. Never disclose your personal information publicly on websites. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Never enter your credit card number to any site that is not secured, to prevent its misuse.
4. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children
5. Always use latest and updated Antivirus software to guard against virus attacks.
6. To prevent loss of data due to virus attacks, always keep back up of your data.
7. It is advisable to use a security program that gives control over the cookies and send information back to the site, as leaving the cookies unguarded might prove fatal.
8. Use of firewalls proves beneficial.
9. Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers will serve the purpose. Capacity of human mind is profound. It is not possible to eliminate cyber-crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties and to guard ourselves so that crime has no effect on us

Causes of Cyber Crimes

1. Ease of access

The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of violating the technology by stealing access codes, recorders, pins, retina imagers etc. that can be used to fool biometric systems and bypass firewalls to get past many a security system.

2. Cyber Hoaxes

Cyber Crimes can be committed just to cause threats or damage one's reputation. This is the most dangerous of all causes. The involved believe in fighting their cause and want their goal to be achieved. They are called cyberterrorists.

3. Negligence: There are possibilities of not paying attention in protecting the system. This negligence

gives the criminals control to damage the computer.

4. **Revenge or Motivation:** The greed to master the complex system with a desire to inflict loss to the victim. This includes youngsters or those who are driven by lust to make quick money and they tamper with data like e-commerce, e-banking or fraud in transactions.
5. **Poor law Enforcing Bodies:** Due to lack in cyber laws of many countries, many criminals get away without being punished.
6. **Cyber Crimes committed for publicity or recognition:** Generally committed by youngsters where they just want to be noticed without hurting someone's sentiments.

Suggestions

Based on the overall conclusions of the study, and the analysis of the inputs given by experts in cybercrime, few suggestions are observed that can help all the potential victims to safeguard from cybercrimes.

1. Every internet user has a right to be aware of the consequences of its threats and misuses. Hence educating them is on high priority on the issues like:-
   a. Uses and misuses of Internet
   b. Importance of Internet security
   c. Awareness about cyber law and regulations
   d. On crime Impact of technology
   e. Hardware & software requirements to protect the data from exploitation and pilfering.
   f. Knowledge on internet policies at the organizations.
   g. Right to protect the personal data from sharing with others
2. Now a days, Internet users are as young as 8 years old. Hence educating them right from the school has to be accorded importance. Workshops can be conducted in schools for both kids and parents for better understanding on 'Safe Surfing' of Internet.
3. The same strategy can be adopted even in colleges. Colleges should take special initiative to incorporate a course work or a paper on "Cyber Crimes and Security" for a professional outlook and can allot credits for clearing the same.
4. Workshops and orientation form experts and ethical hackers are to be encouraged 5 Owner of website should have a through watch on traffic & check for any irregularities are on the site to avoid the scope of malfunctions.
5. Owner of Website should be made aware of their minimum responsibilities in order to adopt some policy for preventing cybercrimes as no of internet user are growing day by day.
6. Web server functional open sites must be physically singly protected from internal corporate network. In order to safeguard the information and data on sites, the corporate authorities can use sophisticated security programmes. Government should bring out more awareness campaigns in various places where the potential net users are high.
7. Mainstream media like television, newspapers, radio and New media platforms like face book can be utilized to the fullest to make all the netizens aware of various kinds of cybercrimes.
8. Government can collaborate with Ethical hackers to bring out more practical solutions for the prevailing problems.
9. Rules and regulations that deal with cybercrimes should be implemented strictly to make sure that no one is taking the security issues for granted. Strict governance is required so that no one is inculcating the habit of indulging in illegal download and data theft.
10. Number of cyber cells can be increased even in small towns. Every organization should be made aware of the procedure to reach these cyber cells, their roles and responsibilities.
11. A complete justice must be provided to the victims of cyber-crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber-crime.
12. As Cybercrime is an internationally threatening issue, and there is more scope for cross border crimes, certain steps should be seized at the planetary even for preventing the cybercrime and coordination between the governments is encouraged.

Conclusion

Cyber Crime reporting in India is still in its nascent stage though cyber violence is fast growing. The Information Technology laws need to be changed to make them cyber-sensitive as well as gender-sensitive. Words like lascivious and prurient should be dropped from the concerned Act to make them better secure women's equality and dignity. Cyber Crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel.

The perspective of the laws should be to ensure dignity of human beings irrespective of the gender and not being in a paternalistic role. Laws are still inadequate and the IT Act needs to be amended to make it well coordinated with IPCs. More IPC provisions need to be amended to make them cyber-friendly. There should be a single comprehensive law covering all aspects of Cyber Crimes. The police, the judiciary and the local administration must be cyber-friendly and more well-equipped to handle evidences judiciously. Cyber Crimes need a holistic approach with change in laws, change in approach of officials and more intense sensitization campaigns involving different sections of society (Cyber, 2018) [3].

References

1. Alpna DS. Cyber Crime-Its Types, Analysis and Prevention Techniques. Alpna *et al*., International Journal of Advanced Research in Computer Science and Software Engineering, 2016, 145-150.
2. Cyber Crime and Its Classification. (n.d.). 24-130.
3. Cyber, N. D.-b. Introspecting the Gaps between Cyber Crimes against Women and Laws: A Study of West Bengal. National Dialogue on Gender-based Cyber, 2018, 1-6.
4. Dashora K. Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences, 2011, 240-299.
5. Desai S. Study of Online Cyber Crimes in India. American Journal of Computer Science and

Engineering Survey, 2016, 1-4.
6. Goyal M. Ethics and Cyber Crime in India. International Journal of Engineering and Management Research, 2012, 1-3.
7. INDIA TI. Cyber Crime Law and Practice. The Institute Of Company Secretaries of India, 2016, 1-152.
8. Kumar J. Cyber Crime in India: An Overview. Imperial Journal of Interdisciplinary Research (IJIR), 2017, 963-967.
9. Mohanaprakash MT. Cyber Criminology. Journal of International Management, Elsevier, 2005, 1-6.
10. Shah J. A Study of Awareness about Cyber Laws for Indian Youth. International Journal of Trend in Scientific Research and Development, 2016, 10-16.
11. Shaw D. Cyber Crime in India – A Challenge to Growth of E-Commerce. RAY: International Journal of Multidisciplinary Studies, 2016, 76-83.
12. Panda TCHS. Cyber-Crimes and their Impacts: A Review. Hemraj Saini, Yerra Shankar Rao, T.C.Panda / International Journal of Engineering Research. 2012; 202-209.
13. Yougal Joshi AS. A Study on Cyber Crime and Security Scenario in India. International Journal of Engineering and Management Research, 2013, 13-18.