International Journal of Humanities and Social Science Research
ISSN: 2455-2070; Impact Factor: RJIF 5.22
Received: 07-11-2019; Accepted: 08-12-2019
www.socialsciencejournal.in
Volume 6; Issue 1; January 2020; Page No. 25-29

Cyber crime in India: A theoretical study

Dr. Sumathi
Assistant Professor Department of Commerce and Management Government First Grade College, Kola, Karnataka, India

Abstract
Crime is a phenomenon correlated to the society we live in. The virtual world with all the advantages it has brought about has also led to the emergence of cybercrime more than ever before. The complexities arising from the cybercrime have been a concern with the policy makers. The description of Cyber Crime is still to be defined. The legal framework however needs a revisit and revision from time to time to equip the legal machinery to deal with the issues. The Cyber Crime in India is alarming as technology is reaching the normal households and the agencies now are facing the spread which is very extensive to cover. The present study is a theoretical study of Cyber Crime in Indian context and the statutory framework for the same.

Keywords: Crime, Legal machinery, Evidence

Introduction
The evolution of internet technology has given us so many advantages to deal with future problems and grow with rapid rate but also it has provided the scope for criminals to commit their crime with least chance of detection. The cyberspace has proved a boon to the deviant behaviour in the society. The concept of Cyber Crime has gained speed and we are facing great threat of its impact on world society. The human society is become vulnerable to Cyber Crime due to more and more dependence on technology. Cyber Crime becomes a global phenomenon and hence the nationwide generalization of crime cannot workable in present scenario. Our understanding and regulation of Cyber Crime cannot be national but has to be international. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even DOS or DDOS) are all technologies and per se not crimes, but falling into the wrong hands with a criminal intent who are out to capitalize them or misuse them, they come into the gamut of Cyber Crime and become punishable offences.

Definition of Cyber Crime
The Indian Legislature does not provide the exact definition of Cyber Crime in any statute, even the Information Technology Act, 2000 which deals with Cyber Crime does not define the term Cyber Crime. However, in general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers. Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes 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)"

Review of Literature
(Nayak, 2013) iterate that the facilities of computer technology have not come out without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber Crime' without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals Restriction of Cyber Crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. The researcher gives a systematic understanding of Cyber Crimes and their impacts over various areas like Socio-eco-political, consumer trust, teenager and the like with the future trends of Cyber Crimes.(Annual, 2014) feels that the Cyber Crime and ensuing victimization is not individual incidence. It is conjointly hampered or inspired by the group of people within which it is located. The author examines the Cyber Crime activities within the perspective of augmentation. The methodology employed analysis of historical information and its relationship with structural characteristics of the communities that are exposed to Cyber Crime. Further they discover that Cyber Crimes are increasing in context of years, however targeted towards specific age group. The ensuing policy insight is for creating public awareness campaigns in upcoming years. (T.C.Panda, 2012) [10] examine that in the current era of online processing, maximum of the information is online and prone to cyber threats. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the Cyber-attacks. Cyber-attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed

knowingly can be considered as the Cyber Crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense and the like. Restriction of Cyber Crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, the researcher provides the understanding of Cyber Crimes and their impacts over society with the future trends of Cyber Crimes. (Sunakshi Maghu, 2014) [9] feel 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 author 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. The article reviews the current solutions to deal with the alarming rise in these criminal activities. Hi-tech technologies that need to be adopted to prevent one from getting webbed have been recommended. (Animesh Sarmah, 2017) [1] contend that as we all know that this is the era where most of the things are done usually over the internet starting from online dealing to the online transaction. Since the web is considered as worldwide stage, anyone can access the resources of the internet from anywhere. The internet technology is used by few people for criminal activities like unauthorized access to other's network, scams etc. These criminal activities or the offense/crime related to the internet is termed as cybercrime. In order to stop or to punish the cyber criminals the term "Cyber Law" was introduced. Cyber law as a part of the legal systems that deals with the internet, cyberspace, and with the legal issues.

Some highlights of the Act

Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference. The said chapter also details the legal recognition of Digital Signatures.

Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

Chapter-IX of the said Act talks about penalties and adjudication for various contraventions. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000/- to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred.

Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking. The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Precautions to Fight with Cyber Crimes

Some precautions for fight with Cyber Crimes are described below:

1. One should not give out your personal information like password, user id and the like.
2. Protection must be ensured by installing basic security programmers.
3. Non-response to unknown E-Mail of offering lotteries, prize gift and the like.
4. Ensuring the secured connection.
5. Secure connection using the password which is very difficult to predict.

Reasons for Cyber Crime

The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace it can be said that computers are vulnerable so rule of law is required to protect and safeguard them against cybercrime **(**Dashora, 2011) [3]. The reasons for the vulnerability of computers may be said to be.

1. Capacity to store data in comparatively small space

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive

information either through physical or virtual medium makes it much easier.

2. Easy to access
The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers and the like. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

3. Complex
The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

4. Negligence
Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

5. Loss of evidence
Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

Preventive Measures to Avoid Cyber Crimes

- **Cyber Forensics** can be used to detect cyber Evidence
- To make necessary amendments not to suppress the criminal activity, this act has defined certain offences and penalties to smother such omissions, which is understood to come within the characterization of Cyber Crimes. From this it can be inferred that the law cannot afford to be static, it has to change with the changing times and viz. cyber space this is all the more required, as there many application of the technology that can be used for the betterment of the mankind, similarly it equally true that such application can also be used for the detriment of the mankind as has been demonstrated by the Spy–cam case. The bottom–line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development. Cyber cell of the law enforcement agencies have started operating in metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc. in Indian laws to control on Cyber Crimes (Yougal Joshi, 2013) [11].

Causes for 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 cyber terrorists.

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 **(**Mohanaprakash, 2005) [5].

Avoiding Cyber Crimes

- Know How To Recognize Phishing. Your bank won't send you an email telling you that your account has been compromised and asking you to provide sensitive account and personal information like password, PIN etc. it already has. These are obviously phishing attempts (Rajarshi Rai Choudhury, 2013) [7].
- Recognize that your Smart-phone is really a pocketsize computer and is prone to the same types of attacks directed at your laptop and desktop. Take steps to protect it, such as keeping your operating system current and creating a strong password.
- Keep your personal information to yourself. For instance, don't put your entire birth date, including the year, on Facebook. Think about the security questions normally posed by your bank and other secure locations: "first school you attended," "name of favorite pet" and the like.
- Know the pitfalls of public Wi-Fi. CreditCards.com says, "Avoid public wireless Internet connections unless you have beefed-up security protection."
- Beware of public computers, too. For instance, Kiplinger says, "Don't access your accounts or personal information on public hotel computers, which could have software that logs keystrokes and records your passwords and account numbers."
- Use credit cards, rather than debit cards, when making purchases online. In case of fraud, you'll get much better protection from liability with a credit card.
- Purchase only from reputable websites (and look for "https" in the Web address). "It is really easy to create a fake online store or to create a store that sells stuff, but its real purpose is to collect credit card information," former identity thief Dan DeFelippi told CreditCards.com.
- Check your accounts and your credit reports regularly. Some experts recommend that you check bank account and credit card activity every day. You can pull a free credit report every four months from AnnualCreditReport.com to verify that fraudulent accounts have not been created in your name.
- Avoid suspicious E-mails. Don't click on links in msuspicious emails, even those that appear to be from friends. Emailed viruses and malware are the most prevalent cyber threat of identity theft. Just think of

how many emails you've gotten in the last year that appeared to be from friends whose email accounts were hijacked.

Importance of Cyber Law

Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views (Animesh Sarmah, 2017) [1].

Need for Cyber Law

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are as below.

1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.
2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a banks electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.
3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
4. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.
5. Cyberspace offers never-seen-before economic efficiency. Billions of dollars‖ worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.
6. Electronic information has become the main object of cybercrime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.
7. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.
8. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. **(**Gurjar, 2015).

Different Types of Cyber Crime against Individual

1. E-Mail Spoofing

This means a spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging. The main goal of the attacker in this case is to interrupt the victim's e-mail service by sending him a large number of emails.

2. Phishing

Phishing means 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. The criminal then has access to the customer's online bank account and to the funds contained in that account. The customers click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred.

3. Spamming

Spam is the abuse of electronic messaging system to send unsolicited bulk messages indiscriminately.

4. Cyber defamation

It involves any person with intent to lower down the dignity/image of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

5. Cyber stalking and harassment

The use of Internet to repeatedly harass another person group, or organization. This harassment could be sexual in nature, or it could have other motivations including anger.

6. Computer sabotage

The use of the internet to halt the normal functioning of a computer system through the introduction of worms, viruses, or logic bomb is referred to as computer sabotage.

7. Malware

Malware is any software that infects and damages a computer system without the owner's knowledge or permission and takes control of any individual‘s computer to spread a bug to other people‘s devices or social networking profiles. Such software can also be used to create a _botnet‘— a network of computers controlled remotely by hacker to spread spam or viruses.

Cyber Laws

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 Information Technology.The Information Technology 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:

1. Cyber Crimes under the IT Act

- Tampering with Computer source documents - Sec.65
- Hacking with Computer systems, Data alteration - Sec.66
- Publishing obscene information - Sec.67
- 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 IPC and Special Laws

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC

- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

3. Cyber Crimes under the Special Acts

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

Conclusion

The preamble of the Information Technology Act 2000 provides that the act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce, further the act has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act 1934 for facilitating legal recognition and regulation of the commercial activities. The police, the judiciary and the local administration must be cyber-friendly and more well-equipped to handle evidences judiciously.

References

1. Animesh Sarmah RS. A brief study on Cyber Crime and Cyber Law's of India. International Research Journal of Engineering and Technology, 2017, 1633-1640.
2. Annual IA. Cyber Crime Investigations in India: RenderingKnowledge from the Past to Address the Future. V.K. Agarwal, Sharvan Kumar Garg, Manoj Kapil, and Deepak Sinha, 2014, 593.
3. Dashora K. Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences, 2011, 240-299.
4. Gurjar LR. Vardhaman Mahaveer Open University,. Cyber Crimes, 2015, 1-277.
5. Mohanaprakash MT. Cyber Criminology. Journal of International Management, Elsevier, 2005, 1-6.
6. Publishers SB. (nd) Cyber Laws in India. Source: Book on "IT" Security of IIBF Published by M/s TaxMann Publishers, 1-19.
7. Rajarshi Rai, Choudhury SB. Cyber Crimes-Challenges & Solutions. Rajarshi Rai Choudhury *et al*, (IJCSIT) International Journal of Computer Science and Information Technologies, 2013, 1-4.
8. Shaw D. Cyber Crime in India – A Challenge to Growth of E-Commerce. Ray: International Journal of Multidisciplinary Studies, 2016; 76-83.
9. Sunakshi Maghu S. Inside of Cyber Crimes and Information Security: Threats and Solutions. International Journal of Information & Computation Technology, 2014, 836-839.
10. Panda TC, H S. Cyber-Crimes and their Impacts: A Review. Hemraj Saini, Yerra Shankar Rao, T.C.Panda / International Journal of Engineering Research, 2012, 202-209.
11. Yougal Joshi AS. A Study on Cyber Crime and Security Scenario in India. International Journal of Engineering and Management Research, 2013, 13-18.