International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 12, December-2017, Impact Factor: 3.578

Cyber Crimes and the Cyber Law in India: An Overview

Dr. G. Mallikarjun*

*Asst. Professor of Law, NALSAR University, Hyderabad (India)

I. INTRODUCTION

Cybercrimes are offences which are generally committed with a criminal intention to harm either the individual reputation or the reputation of any organisation or it may even cause physical or mental abuse to the victim directly or indirectly. In India 'Cyber Crime' is not defined officially in Information Technology Act 2000 (IT Act) or in any other legislation and thus it can be said that it is just a "combination of crime and computer"[1] Anyone who has an Email-id or Face book account or who is a member of a social networking website or even one who is doing on-line transaction to carry on day today business can become a victim of cybercrime. Cybercrimes not only affects the privacy of an individual but it is also harmful or threat to the security and integrity of the state or organisation. The cybercrimes in India, though on rise, mostly go either unreported because of lack of knowledge about the cyber law.

II. CYBER-CRIME: THE DEFINITION

Cyber-crimes are the crimes committed with the use of computers or relating to computers, especially through the internet. Cyber space crimes may be committed against persons, property, government and society at large. Thus, the Cyber Crimes is a term that refers to all criminal activities done by using the computers or computer networks or by using other devices like mobile phones, tablets[2] etc. It also covers the traditional crimes in which computers networking are used to enable the forbidden activity. Cyber Crimes can be categorised in three ways[3]:

1. **The computer as a target** – attacking the computers of others.
2. **The computer as a weapon-** Using a computer to commit "traditional crime" that we see in the physical world.
3. **The computer as an accessory-** Using a computer as a "fancy filing cabinet" to store illegal or stolen information.

III. SIGNIFICANT CYBER OFFENSES IN INDIA

List of offenses given below is not exhaustive and would include many other offenses that would be committed through a computer or against a computer in the future.

Unauthorized Access (Hacking): it is an unauthorized control/access in to the computer system or network[4]by which destroys the complete data. Hackers write or use ready-made computer programs to attack the target computer to destruct or otherwise to steal the credit card information, bank account information and other confidential information.

Cyber Stalking: Repeated acts of expressed or implied harassment or physical threat towards the victim by using internet services. Even they use very filthy and obscene language to invite the interested persons. If the stalker is able to access the telephone of the victim, repeated calls will be made to the victim to threaten, harass, or intimidate them. Stalkers, generally, have desire to control the victims life. Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female[5].

---

*Asst. Professor of Law, NALSAR University, Hyderabad.

[1] Lionel Faleiro**,** **"**IT Act 2000 – Penalties, Offences With Case Studies", http://niiconsulting.com/checkmate/author/lionelfaleiro/

[2] Kanika Chhabra and Gunjan Chhabra, A Study on Emerging Issue on Cyber Law, Advances in Computer Science and Information Technology (ACSIT), Volume 1, Number 3; November, 2014, Krishi Sanskriti Publications pp. 112-116, http://www.krishisanskriti.org/acsit.html

[3] R. M. Johri **,** Principal Director (information Systems)Cyber Security – Indian Perspective**,** Office of CAG of India, seefor further detailswww.intosaiitaudit.org

[4] It is a kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network (section 66 of IT Act 2000).

[5]See http://www.nandedpolice.in/cyber.php, (Accessed on 13-12-2017)

Web Jacking – The term refers to forceful taking of control of a web site by cracking the password[6].
Cyber Squatting: More than one person claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously[7]

Denial of service Attack: This is an attack in which the criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic[8].

Child Pornography: Depicting children engaged in sexually explicit act, creating text or digital images or advertising or promoting such material depicting children in obscene or indecent manner etc[9]

Cyber Pornography: This would include pornographic websites; pornographic magazines produced using computer and the Internet (to down load and transmit pornographic pictures, photos, writings etc.)[10]

Virus attacks: Viruses are the programs that will have the competency to infect other programs and make copies of it and spread into other programmes, which will multiply like viruses but spread from computer to computer are called as worms.

Trojan Attack: A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing[11].
Software Piracy: Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kinds of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

Salami Attacks: This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed[12]. E.g. a bank employee inserts a program, into the bank's servers, that deducts a very minimal amount of money may be single digit amount from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

Phishing: The act aims at stealing confidential information and other important details by sending an e-mail to a user falsely claiming to be an established enterprise in an attempt to get private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as username, passwords and credit card details and bank account numbers that the legitimate organization already has[13].

Email spoofing: Sending offensive messages through an electronic communication so as to cause annoyance or sending an email to mislead or deceive the recipient about the origin of such messages are commonly known as IP or email spoofing[14].

Investment Frauds: An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site[15].
Cyber Terrorism: Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization[16].Cyber terrorism is nothing but targeted attacks on military installations, air traffic control, schedule

[6]See http://technohacks.in/cyber-protection-threats/cyber-threat/web-jacking/, (Accessed on 13-12-2017)
[7] See https://en.wikipedia.org/wiki/Cybersquatting
[8]See https://en.wikipedia.org/wiki/Denial-of-service_attack, (Accessed on 12-12-2017)
[9] Child Pornography has been exclusively dealt with under Section 67B.
[10] See http://www.cidap.gov.in/documents/cyber%20Crime.pdf, (Accessed on 12-12-2017)
[11]Ibid.
[12]Parthasarathi Pati, "CYBER CRIME", http://www.naavi.org/pati/pati_cybercrimes_dec03.htm, (Accessed on 12-12-17)
[13] M.Usha , Phishing - A Challenge in the Internet, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1) , 2014, 260-263.
[14]Section 66A of IT Act 2000.
[15] See http://www.cyberlawsindia.net/index1.html, (Accessed on 13-12-2017)
[16] Section 66F of IT Act 2000.

banks and telecommunication networks. It is an attractive option for terrorists for the reason that anonymous can be maintained than traditional terrorist methods.

Data Diddling: This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed. For instance, the NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances[17].

IV. CYBER CASES IN INDIA: AN ANALYSIS

Genpact BPO Case (Cyber stalking/cyber bullying)[18]: Female employee of Genpact was repeatedly harassed by the erstwhile employee of the same company with absence mails. She filed a complaint along with email copy consisting of email header by which IP address of the sender was traced and with that email address of the accused was found to be from rediffmail.com to send the said mails. A case was booked against him for Cyber stalking.

The Bank NSP Case[19]: Where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

Sony.Sambandh.Com Case[20]: A complaint was filed by Sony India Private Ltd, which runs a website called www.sonysambandh.com, targeting Non Resident Indians. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. After one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation. The court convicted Arif Azim for cheating under Section 418, 419 and 420 of the Indian Penal Code. This was the first time that a cyber-crime has been convicted. The judgment is of immense significance for the entire nation.

Bazee.com case (Auction Fraud case)[21]**:**www.Baazee.com.10 Sony Ericsson P900 mobile phones were put up for auction by one seller. By mentioning offer price as Rs/-15,000/- when actual market price was 40,000/-. And in that he mentioned himself as Sony Ericsson Importer. Many users placed bids. Seller supplied his bank a/c to bidders, asked to deposit money in his account. Bidders deposited money, mobiles never delivered. This fraud was done by a final year MBBS student at Bangalore, who is from affluent family of Malaysia. He did it for sake of pocket money as a alternative source of income.

Citi Bank Spoofing Case (Phishing case)[22]**:** Many E-mails are in circulation asking the receivers to update their CITI Bank account information. The mails are purported to be from Customer Service Department of the Bank. The mails also contain a link to CITI Bank website. The fact the link is not genuine. It comes with an extension … e.g.www.citibank.com/5%ac8%/login.asp. The link actually takes the person to a mirror of actual site. The information punched in there never goes to the Bank but to another computer and gets stored which can be used by the person for operating the accounts.

ONGC Cyber fraud case (Identity theft)[23]**:** The Oil and Natural Gas Corporation Limited (ONGC) lost Rs 197 crore after cyber criminals duplicated the public sector firm's official e-mail address with minor changes and used it to convince a Saudi Arabia-based client to transfer payments to their account. The fraud was committed on the promise that the company making the payment would not notice a minor change in the e-mail address of the ONGC representative, with whom they had been communicating. While ONGC communicated with the company from

[17]Rajkumar Dubey, Cyber Crimes -An Unlawful Act Where in the Computer is Either a Tool or a Target or Both", http://www.mondaq.com/i_article.asp_Q_articleid_E_28603, (Accessed on 13-12-2017)
[18] See http://gurgaon.haryanapolice.gov.in/case-studies.htm, (Accessed on 13-12-2017)
[19] See http://www.indiancybersecurity.com/case_studies/the_bank_nsp_case.html, (Accessed on 12-12-2017)
[20] See http://www.indiancybersecurity.com/case_studies/sony_sambandh_case.html ((Accessed on 12-12-2017)
[21] See http://gurgaon.haryanapolice.gov.in/type_cybercrime.htm, (Accessed on 12-12-2017)
[22] See http://gurgaon.haryanapolice.gov.in/case-studies.htm, (Accessed on 13-12-2017)
[23] Ibid.

patel_dv@ongc.co.in, the fraudsters deceived the company by communicating with them from patel_dv@ognc.ac.in, which is dubious created an e-mail ID for the transfer of a large sum of money to their credit.

V. CYBER LAW IN INDIAN: AN ANALYTICAL OVERVIEW

To check and to deal with the cybercrime theInformation Technology Act (IT Act) was enacted in the year 2000[24]by Indian parliament based on the United Nations Commission on International Trade Law UNICITRAL model of Law on e- commerce 1996. Subsequently[25], the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003, and the Information Technology (Security Procedure) Rules, 2004 were passed[26]. They prescribe provisions relating to secure digital signatures and secure electronic records.

Further the Act also amended 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 Act. The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000 and to regulate and control the affairs of the cyber world in an effective manner.

However, The Act thoroughly amended in the year 2008 aimed to provide for comprehensive legal framework so cover all activities[27] conducted on line apart from providing the legal sanctity to all electronic records and other activities[28]. Further it provides for the constitution of the Cyber Regulations Advisory Committee which has been advising the government as regards to any rules or for any other purpose connected with the Act. The Act[29] also deal with the unauthorised access, unauthorised downloading, virus attacks or any contaminant, causes damage, disruption, denial of access etc. And who ever involved in the said acts will be fined up to Rs. 1 Crore[30] as a remedy, but it is not a full protection for the online transfers. Even Act under section 72 talks about the Breach of confidentiality or privacy , but does not prevents the violations caused in the cyberspace[31] Tamper with computer source documents will invite the imprisonment for that is up to 3 years or fine[32]. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine. Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs[33].

Territorial jurisdiction which has been mentioned in sec 46, 48, 57 and 61in IT Act is not satisfactory in context of adjudication process and the appellate procedure connected with and again in sec 80 and a part of the police officer power to enter, search a public place for a cybercrime etc. However, Jurisdictional issues like extraterritorial jurisdiction extradition are being sorted out through international negotiations and through bilateral treaties.

VI. CONCLUSION AND SUGGESTIONS

Cyber-crime is not only a problem to India but it is a global problem and thus the world at large should strive together to curb this menace. In India as of now the existing cyber laws are not stringent enough to cover all forms of cyber related crimes as they were enacted long back based on the political, social, economic, and cultural scenario of that relevant time when there was no thought of internet regime as today. It is also to be noted that the Copyright and Trademark violations do occur on the net, but the laws[34]which are specifically deals with the issue are silent on that. Further, transmission of e-cash and related transactions online are not given protection either under Negotiable Instrument Act or under IT Act[35]. Likewise the Internet Service Providers (ISP) who transmits some third party

[24] On 17th May 2000 and subsequent developments are: on 17th October 2000 the Information Technology (Certifying Authorities) Rules, 2000 and Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 came into force.
[25] On17th March 2003
[26] However, they came into force on 29th October 2004
[27] Like, Electronic and Digital Signatures, Intellectual Property, Data Protection and Privacy etc.
[28]The Act also amended 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 Act. The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000 and to regulate and control the affairs of the cyber world in an effective manner.
[29] Chapters IX and XI of the IT Act of 2000
[30] Section 43 of the IT Act of 2000
[31] See ttps://www.kpmg.com/in/en/industry/publications/fs_cybercrime_booklet.pdf
[32] Section 65 of the IT Act of 2000
[33] The Gazette of India, Extraordinary part -2 http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf
[34] Copyright Act, 1976 or the Trademark Act, 1994
[35] See ttps://www.kpmg.com/in/en/industry/publications/fs_cybercrime_booklet.pdf

information without human intervention is not made liable under the IT Act. Therefore, India needs to update the Law by amendments having holistic approach towards internet related crimes with effective enforcement mechanism.

VII. SUGGESTIONS

To ensure effective prevention and control of the cyber-crimes, the following suggestion are recommended

1. To make cyber law more efficient, the necessary amendments to be carried out in tune with the ever changing nature of cyber-crimes.
2. It is always to be ensured that the proper procedures are being followed while collecting and handling the digital evidence or potential digital evidence so as to rule out the acquittals due to lapses in following the procedure
3. Though judiciary is well equipped to comprehend the nature and technicalities involved in the commission of cybercrimes, yet it is better to establish a special tribunal consisting of scientific experts who will advise the judicial officer (presiding officer) in dealing with cyber-crimes.
4. Cyber-crime is a concern of every country as it is a global problem and therefore international cooperation and co-ordination by entering into bilateral or multilateral treaties with the help of international organizations, like UNO, OECD and G8 etc., to curb this menace.