Paper 12

A Study on the Cyber Crimes in the Technological Era

Pradeep M. D[1]
[1]Assistant Professor, College of Social Sciences & Humanities, Srinivas University,
Mangaluru, Karnataka, India.
Email: mdpradeepnair767@gmail.com

ABSTRACT

Advancement in Technology facilitated cybercrimes and created fear among netizens. Information Technology widened communication sphere making it Borderless and Transnational. Any criminal act committed over the internet for monetary and non monetary gains is considered as Cyber Crimes. Cyber offenders indulge in misusing confidential information for committing illegal activities. The most prominent offences are stalking, hacking, phishing, online frauds, identity thefts, distributing viruses etc. These crimes cause damage to personal identity, fraud, forgery, threat, monetary losses etc. Through the Information Technologies (Amendment) Act, 2008, government tried to bring beneficial changes to ensure cyber security in the country. Cybercrimes cause severe damages in the developing countries driving towards cashless economy. Compared to traditional crimes, Cybercrimes requires special regulations. Combating Cyber violations has become the prime consideration for the Criminal Justice Administration System in developing economy. The laws dealing with Cybercrimes become inappropriate to deal with new offences committed by using new technologies. There is a need for Universal Criminalization of Cyber Offences under International laws and treaties. This paper highlights about cybercrimes, laws, policies, prevention and cyber security.

Keywords: Technology, Cyber Space, Cyber Crimes, Cyber Laws, Cyber Security.

1. Introduction

The present world is driven through technology and the imagination of world without IT in the 21st Century is impossible[1]. Cyber space is the electronic medium of computer network used for interaction, exchange, information, social support, business, directing, art, games and discussions etc. Computer network is the collection of computers connected through communication channels such as cables, fiber optics to share data, hardware and software. Any criminal activity taking place on or over the medium of Computers or Internet or other Technology recognized under the Information Technology Act is known to be Cyber Crime. Cyber crimes are new classes of crimes rapidly growing due to the extensive use of internet and Information Technology enabled services. Cyber Technology started to pose threat over social wellbeing by offering avenues to the fraudsters and offenders to commit crimes by using computers and internet technology. Cyber Criminals hide their identities and commit offences causing devastating damage with different magnitudes. Growing menace of Cyber Crime is posing challenge before the Business and legal systems. Indian Legal system and Institutional framework is falling short in meeting the challenges of Cyber Crime. It has become difficult to initiate measures to control Cyber Crimes as the impact of such crime can be realized only after its commission. Healthy usage of information technology requires secure environment with adequate legal and enforcement mechanism [2].

2. Features of Cyber Crimes

Cyber crimes have gained serious and unfettered attention compared to conventional crimes hence it is required to examine peculiar feature of these offences.

- It is committed by people with specialized knowledge on internet and networking.
- With zero geographical constraints, cyber criminals are operating across the borders posing geographical challenges to combat cyber crimes.
- Crimes are committed over the virtual world.
- The collection of evidences to present before the court is difficult due Non traceability.
- Magnitude is unimaginable with potential monetary and non monetary losses.
- These offences are presumed to involve low risk and high rewarding ventures.
- People lack with adequate skills and know how to trace cyber violations.
- Crimes are committed from far distances without involving the perpetrators physical presence.
- Investigating agencies lack with hi tech skills to detect and prevent cyber crimes.
- Cyber violations are not reported due to the fear of adverse publicity or loosing public trust.
- It may be the outcome of greed, mischief and exploitation over attempt to commit violence.
- Cyber crimes are becoming more complex along the boundary less existence.
- Easy access and openness allows anybody to indulge in cyber offences.
- Cyber Crimes has wider ramification causing harm to socio-economic and legal rights of the people.

3. Targeted Cyber Attacks

Cyber crimes are illegal activity committed by using any computer network or against some computer systems causing damages to the netizens. Difficulty in determining jurisdiction in transnational online transaction causes unmanageable ambiguity to the judiciary to decide cases on cyber crimes. It is very difficult to determine the 'Men's Rea' and 'Actus Reus' in Cyber Crimes as the entire act is committed in intangible surroundings.

(a) Hacking: An act of accessing others computer without permission for destroying, deleting, altering and diminishing the value of information. It even includes acts of introducing computer virus, causing damage, disruption or denial and causing cyber terrorism.

(b) **Cyber Pornography: U**sing the cyberspace to create, display, distribute, import or publish pornography or obscene materials. The internet is highly used by the abusers to abuse children sexually worldwide. The pedophiles win the confidence of children to exploit them online since parents and teachers does not tell them about right and wrong over the internet.

(c) Cyber Stalking: Constant harassment or threatening via internet or electronic medias including chats box, e-mail, spam, fax, buzzer or voice-mail. It also includes following a person, appearing at someone's house or workplace, making harassing phone calls, leaving written messages or objects, vandalizing someone's property etc.

(d) **Cyber Defamation: A**n intentional false communication, either published or publicly spoken which injures another's reputation or good name. The gist of defamation is actual or presumed damage to reputation flowing from publication.

(e) Cyber Terrorism: Unlawful attacks and threats against computers, networks and stored information done to intimidate or coerce a government, people in furtherance of political or social objectives.

(f) **Malware or Malicious Computer Codes:** Any code including viruses, Trojan and worms designed to cause damage to the normal functioning of the computer.

(g) **Phishing & Vishing:** Acquiring private, personal and financial by masquerading as a trustworthy person through electronic communication is phishing whereas, vishing is the usage of social engineering and voice over IP (VoIP) to gain access to such information.

(h) **Denial of Service Attack: A**n explicit attempt by the attackers to deny service by flooding a computer resource with more requests than it can handle to consume the available bandwidth to result server overload.

(i) Data Theft: Stealing of Business Secrets, Technical Knowhow, Designs, Music, Films, Books, Personal Data including Usernames, Credit Card Numbers & Passwords etc.

(j) **Data Diddling:** Data diddling involves changing data prior or during input into a computer.

(k) Salami Attack: Salami Slicing Attack is a technique by which cyber criminals steal money or resources a bit at a time so that there is no noticeable difference in overall size.

(l) E-mail Bombing: It is a net abuse by sending huge volumes of email to cause the overflow in the mail box or server thereby crashing the email server.

(m) E-mail spoofing: It is a fraudulent e-mail activity where the sender's address of the e-mail header is altered so as to appear that e-mail has been originated from a different source.

(n) Logic Bombs: A logic bomb is a computer instruction that codes for a malicious act.

(o) Internet Time Theft: Unauthorized usage internet hours of others.

(p) Web Jacking: Hacker takes control of a website fraudulently so as to change its content or redirecting the user to a fake similar looking webpage controlled by him.

(q) Software Piracy: Unauthorized use and distribution of computer software.

(r) Intellectual Property Violations: Electronic breach of patented designs, copy rights and trademarks or usage of domain for illegal activities.

(s) Cyber Fraud: It is obtaining dishonestly money or property or services or evading debt or liability by means of fraudulent usage of computer networks.

(t) Cyber Trespass: Crossing the cyber boundaries into other computer systems having right of ownership so as to cause its damage.

4. Conclusion.

The user of computer system and internet are increasing worldwide in large number day by day[3]. Cyber attacks have been more specialized and concentrated targeting organization and individuals[4]. The society is highly vulnerable to cyber crimes committed with greater along with the higher dependence over technology [5]. During 2016, maximum number of cases under cyber-crimes were reported in Uttar Pradesh (2,639 cases) with 21.4% followed by Maharashtra (2,380 cases) with 19.3% and Karnataka (1,101 cases) with 8.9%. Among the reported crimes 48.6% of cyber-crime cases reported were for illegal gain (5,987 out of 12,317 cases) followed by revenge with 8.6% (1,056 cases) and insult to the modesty of women with 5.6% (686 cases) [6]. Enactment of new laws and preventive mechanisms will protect our society from such crimes. Use of Internet and unfamiliarity with internet usage may lead for fraud and cyber crime. The Customer protection through the education on security risks may check the reputation risk of the banks[7]. Government of India formulated IT Policy as per United Nations Commission on International Commerce in 1996. Indian Parliament enacted IT Act, 2000 [IT Amendment Act 2008] for India which provides legal recognition for electronic communication. Provisions were incorporated in Indian Evidence Act, 1872, Indian Penal Code (Post Criminal Law Amendment Act, 2013), Protection of Children from sexual offences act, 2012, Bankers Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, The Indecent Representation of Woman Act, 1986, Indian Technology Act, 2000. Cyber Crimes defy quantification the estimation of such instances based on its prevalence, cost and other measures is quite difficult [8]. Harmonized approach to jurisdictional issues, including careful consideration of the universality principle, would also play a critical role in combating cyber crime [9]. Enhancing cyber security and protecting critical information infrastructures are essential to safeguard the National security and economic wellbeing [10].

5. References

[1] Pradeep M.D., (2015). 'Impact of Information Technology in Banking- Cyber law and Cyber Security in India' , *International Journal of Management, IT and Engineering*, 5(7), 411-428.

[2] Economic & Political Weekly (1999). 'Dithering Over Cyber Laws', 34(20), May 15, 11-51.

[3] Alpna & Sona Malhotra, (2016). ‘Cyber Crimes- Its types, analysis and prevention techniques’, *International Journal of Advanced Research in Computer Science and Software Engineering,* 6(5), 145-150.

[4] KPMG, (2017), Cyber Crime Survey Report Insights and Perspectives, 1-26.

[5] Sumanjit Das & Tapaswini Nayak, (2013). ‘Impact of Cyber Crime: Issues and Challenges’, *International Journal of Engineering Sciences & Emerging Technologies*, October, 6(2), 142-153.

[6] Crime in India (2016). ‘National Crime Records Bureau’, Ministry of Home Affairs, Government of India. xxii.

[7] Yang, Z.; Jun, M. & Peterson, R.T. (2004). ‘Measuring Customer Perceived Online Service Quality’, *International Journal of Operation and Production Management*. 24(11), 5-10.

[8] Peter Grabosky, (2000). ‘Cyber Crime and Information Warfare’, Paper presented at the Transnational Crime Conference, Australian Institute of Criminology in association with the Australian Federal Police & Australian Customs Services, Canberra, March, 9-10.

[9] New Challenges for International rules against Cyber Crime (2004). Springer Netherlands, 10(1), March.

[10] Marco Gercke, (2012), ‘Cyber Crime: Phenomena, Challenge and Legal Response, International Telecommunication Union, Telecommunication Development Bureau, September, Geneva, Switzerland, 2.