

ANALYSIS OF CYBER CRIME AND ITS IMPACT IN INDIA

Y.Karali*

S.Panda*

C.S.Panda*

Abstract

In this age of information and technology, Internet plays the pivotal role for the exchange of huge amount of information. It influences not only all spheres of human life but also all age groups of man. Even if the internet has changed our society fundamentally, the information over internet is not free from any illegal access or harm. Thus the security and safety of information has become the major challenge of the present time. With the rapid growth of users, the cyber crime cases are also increasing and are not restricted by any geographical limitations or national boundaries in the world. Over the past few years India has witnessed many cyber crime cases. And it is a matter of great concern as it has direct negative impact on economic and social lives of people. Our research work is based on the quantitative analysis of cyber crime cases of last four years under the IT Act and Indian Penal Code in top vulnerable states and cities in India. And further we include the description of different motives of cyber crime activities and the offences along with some important remedial measures to minimize the cyber crime cases.

Keywords: Cyber crime, IT Act, Indian Penal Code, Offences.

* P.G. Department of computer science and application, Sambalpur University, Sambalpur, Odisha-768019, India

1. INTRODUCTION

Today, world is undergoing second revolution. Every aspect of human life is being touched by Information Technology. Everyday's activities are affected in form, content and time by computer. Computerization is replacing human tasks [2]. But the information over internet is not free from any illegal access or harm. It is found that in the current decade, there is a remarkable increase of crime rate on internet. Thus the security and safety of information has become the major challenge of the present time. The crime on internet is termed as cyber crime and in simple meaning cyber crime is unlawful acts wherein the computer is either a target or a tool or both. A crime committed or facilitated via the internet is a cybercrime. Cyber Crime is any criminal activity involving computers and networks [1]. Cyber crime is regulated by cyber laws or internet laws. The criminal activities that are traditional in nature such as theft, fraud, forgery, defamation and mischief are subject to the Indian Penal Code whereas the abuse of computers such as hacking, phishing, Email Spoofing, Email spamming, Email bombing etc. are addressed by the Information Technology Act 2000.

2. Cyber Laws: Indian Penal Code and IT Act2000

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the internet, the World Wide Web and Cyberspace. Cyber laws are meant to set the definite pattern, some rules and guidelines that define the different business activities going on through internet and categorize the activities as legal and illegal. The activities which are illegal are punishable as per the laws. Cyber crimes can involve criminal activities that are traditional in nature such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code.

In the Year 2000, India enacted its first law on Information Technology which is called Information Technology act 2000. The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. The preamble to the IT Act 2000 indicates three fold objectives [3]. Firstly, to provide legal recognition for transactions carried out through electronic means. Secondly, to facilitate the electronic filing of documents with government agencies, and thirdly, to amend certain Acts, inter alia ,the Indian Penal Code 1860, Indian Evidence Act 1872.

The IT Act 2000 provides legal validity and recognition to electronic documents and digital signatures and enables to draw conclusion of legally valid and enforceable e-contracts. It also provides a regulatory regime to supervise the certifying authorities issuing digital signature certificates and created civil and criminal liabilities for contravention of the provisions of the IT Act 2000. It also conferred the power on the central government to appoint Adjudicating Authority to adjudge whether a person has committed a contravention within the meaning of the Act. But with the advancement of technology, many loopholes of the Act were noticed that led to the passage of the Information Technology (amendment) Act 2008 which was made effective from 27 October 2009[3].

3.Types of cybercrime most prevalent in India:

3.1. Cyber crime under IT ACT-

- Tampering with computer source documents-sec.66
- Hacking with computer systems, data alteration-sec.66
- Publishing obscene information sec 67
- Unauthorized access to protected system sec70
- Breach of confidentiality and Privacy-sec.72
- Publishing false digital signature certificates Sec.73

3.2. Cyber crime Under IPC –

- Sending threatening messages by email-Sec.503
- Sending defamatory messages by email-Sec.499
- Forgery of electronic records-sec.463
- Bogus websites, cyber fraud-Sec420
- Email spoofing-Sec383
- Web Jacking-Sec383
- Email abusing –Sec500
-

3.3. Cyber crime under special Act-

- Online sale of drugs under Narcotic Drugs and Psychotropic substances Act
- Online sale of arms Act

4. Statistical Report on Cyber Crime in India

Table-1(Cyber crime cases registered under both IPC and it act 2000 in top ten states of India)

STATE	2010	2011	2012	2013
MAHARASTRA	246	443	561	307
ANDHRA PRADESH	171	372	454	651
KARNATAKA	176	160	437	533
KERALA	156	245	312	383
WEST BENGAL	60	57	309	342
UTTAR PRADESH	41	114	249	682
MADHYA PRADESH	35	103	197	342
RAJASTAN	55	146	154	297
PUNJAB	68	79	78	156
ASSAM	18	31	28	154

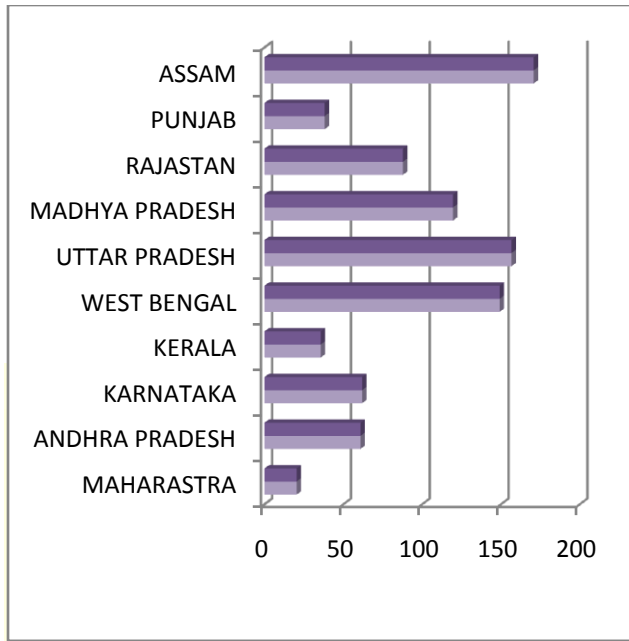


Fig-1(Percentage variation of Cyber crime cases registered under both IPC and its act 2000 in top ten states of India)

Table2 (Cyber crime cases registered under both ipc and its act 2000 in top ten cities of India)

CITY	2010	2011	2012	2013
BENGALURU	49	121	349	417
VISHAKHAPATANAM	31	126	154	175
PUNE	58	83	108	100
DELHI	41	99	80	150
JAIPUR	27	96	73	131
KOLKATA	13	22	68	96
KOCHI	10	37	65	37
HYDERABAD	56	67	42	160
MUMBAI	49	33	35	132
CHANDIGARH	0	0	33	11

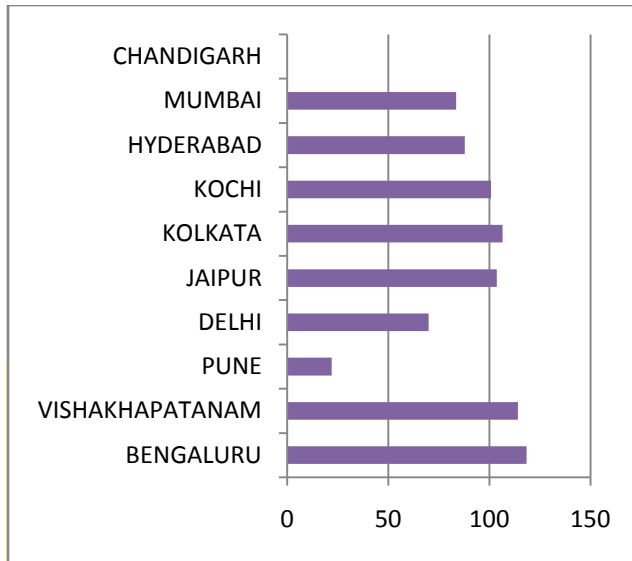


Fig2(Percentage variation of Cyber crime cases registered under both IPC and IT Act 2000 in top ten cities of India)

Table3 (Cyber crime cases registered under both IPC and IT Act 2000 in top ten Metro cities of India)

METRO CITY	2010	2011	2012	2013
MUMBAI	49	33	105	150
DELHI	41	99	80	132
KOLKATA	13	22	68	96
CHENNAI	25	17	15	13

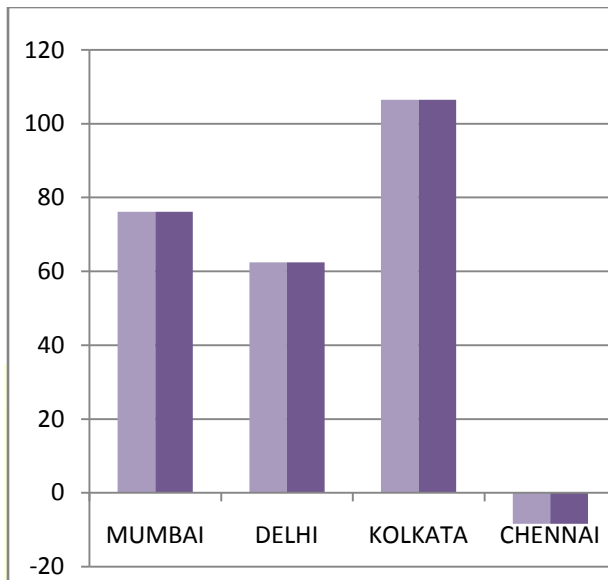


Fig3(Percentage variation of Cyber crime cases registered under both IPC and IT Act 2000 in top ten Metro cities of India)

ANALYSIS OF FIGURES

The data have been taken from the national crime record bureau govt. of India. Here in this study, we have analyzed the cyber crime cases registered under both Indian penal code and IT act 2000 together since 2010 to 2013. In our study, we have considered the top ten vulnerable states, cities and four metropolitan cities separately. From the above figure-1, it is observed that the rate of increase of cyber crime cases is highest for Assam although the number of crime cases registered for the state of Maharashtra is highest. The Figure-2 reveals that the percentage variation of the cyber crime cases registered in the top ten cities of India from 2010 to 2013 is highest for the city Bengaluru whereas the city Pune shows lowest among them. Similarly, from figure-3, it is vivid that the metropolitan city Kolkata shows highest percentage variation of cyber crime cases even if Delhi shows maximum number of cyber crime cases registered but Chennai is the only metropolitan city which shows decrease in number of cyber crime cases registered.

CONCLUSION

The primary objective of the research undertaken has been to shed light on the evolution of the dominance of cyber crime cases throughout India. This paper concludes that many types of cyber crime prevailing in this technology based age. It is observed that in the current decade there is a steady increase in the number of cyber crime cases in different states and cities of India. The

cyber crime cases registered from 2010 to 2013 in different states and cities in India show a consistent increase. So, it becomes clear that our cyber frameworks as well as Indian cyber laws have still some issues to be solved as our Information Technology Act is unable to provide complete protection to our cyber world. Thus it requires proper implementations of cyber laws combined with the awareness and proper policy making.

References:

1. National Crime Prevention Council, Subcommittee on crime and Terrorism, Washington, D.C., April 12, 2011.
2. M. Narang, G. Jain, Cyber Crimes : Problems of Investigation and Solutions, Indian Journal of Applied Research, vol.3, issue 11, pp.73-76, 2013.
3. Wow essay (2009), Top Lycos Networks, Available at: <http://www.wowessays.com/dbase/ab2/nyr90.shtml>.
4. A. Cruz, Cyber Crime and How it affects you, Cyber security tips, vol.7, issue1, January 2013.
5. K. Seth, IT Act 2000 VS 2008-Implementation, Challenges, and the Role of Adjudicating Officers, National Seminar on Enforcement of cyber law, New Delhi, 8th may 2010.
6. National Crime Records Bureau, Ministry of Home Affairs, Government of India, Crime in India 2012 Statistics.
7. Z. Mohiuddin, Cyber laws in Pakistan-a situational analysis and way forward, Ericsson Pakistan (Pvt.) Ltd, June 24, 2006.
8. H. Saini, Y. S. Rao, T. C. Panda, cyber crime and Their Impacts: A Review, International Journal of Engineering Research and Application, vol.2, Issue2, pp.202-209, 2012.
9. N. Nain, S. Batra, Preliminary study of cyber crime ,its impact and remedial acts in India, International journal of computer science and communication engineering, special issue, pp.223-227, 2013.
10. M. Olusola, O .Samson, A. Semiu, A. Yinka, Impact on cyber crime on Nigerian Economy, The International journal of Engineering and Science, Vol.2, Issue4, pp.45-51, 2013.

11. .R. P. Kaur, Statistics of cyber crime in India: An overview, International journal of Engineering and Computer Science, vol.2,issue 8, pp.2555-2559,2013.
12. Faye Misna, Alan Mc Luckie and Michael Saini Real world dangers in an online Reality: a quantitative Study Examining online relationship and cyber abuse”33 social work research2,june 2004.
13. Dr. Ken Rigby, Children and Crime: Victims and Offenders, Conference convened by the Australian Institute of Criminology and held in Brisbane, 17-18 June 1999.
14. Children prey to cyber-crime; majority of parents don't feel so, press trust of India, New Delhi, June 15, 2014.
15. Adv Prasanth Mali, IT act 2000, Types of Cyber Crimes & Cyber Law in India, Security Corner, part-II.
16. Bantek I, Nash S, international criminal law 2/e, Rutledge, Cavendish: London, 2003, ISBN-1859417760.
17. Hume m, child porn is being normalized by panic merchant the times jan12, 2004
18. Wolak j , Finkehor d, Mitchell k, Y Berra m, Online predator and their victims: American psychologist 2008;63(2);111-128.
19. Shaheen Shariff , Dianne L. Hoff Cyber bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace Mc Gill University, Canada, 2008;1;1
20. Richard Donegan ” bullying and cyber bullying: history, statistics, law, prevention and analysis” the Elon journal of Undergraduate Research in communications vol3,no1,spring 2012 .