An Analysis On Recent Trends Of Cyber Crimes In India

Srinivas Katkuri
Research Scholar (UGC-NET in Law), Faculty of Law/University College of Law, Osmania University, Hyderabad, Telangana.

Abstract- *Cyber crimes are a new class of crimes which are rapidly increasing due to extensive use of Internet and I.T. enabled services. Several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC with the legal recognition of electronic records and the amendments made in several sections of the IPC vide the IT Act, 2000. Cyber offences may appear to be an urban phenomenon, and Towns India turns out to be hub of cybercrime. Cyber crimes in India have cost a whopping about Rs 24,630 crore ($4 billion) in 2013 alone as criminals used sophisticated means, says a Delhi High Court-commissioned report. According to NCBR2015, most of the cyber crimes were registered for greed/financial gain accounting for 33.3% followed by fraud/illegal gain (9.6%), insult to the modesty of women (5.2%), sexual exploitation (5.1%) and causing disrepute (3.3%). In this paper, I would explore various cyber crimes and Cyber Law in India. The present study has been conducted through secondary sources.*

Keywords- Information Technology, cyber crimes, Cyber Law

I. INTRODUCTION

Cyber crimes are a new class of crimes which are rapidly increasing due to extensive use of Internet and I.T. enabled services. The internet provides the means to link up the many and diverse networks already in existence. Since commercialization of the internet during the mid 1990s, it has grown manifold. Even though majority of worldwide total internet connections are located in developed countries, the fact is that these are growing at a very fast rate in developing countries too. An Unequal access also follows along existing lines of social exclusion within individual countries and factors such as employment, income, education, ethnic disability are reflected in the patterns of internet use.[i]

"Cyber Crime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations".[ii] Examples of cyber crime include denial of service attacks, cyber-theft, cyber trespass, cyber obscenity, critical infrastructure attacks, online fraud, online money laundering, ID fraud, cyber terrorism, and cyber extortions. It is evident that organized criminal organizations use cyber crime extensively to collaborate and connect with their vast network which is spread across globe. The synergy between organized crime and the internet has thus increased the insecurity of the digital world.

Every nation should have in place laws addressing abuses of a computer or network that result in loss or destruction to the computer or network, as well as associated losses. The law should also provide the tools and resources needed to investigate, prosecute, and punish perpetrators of cyber crimes.[iii]

II. CRIME IN INDIA

'Crime Rate' is a standard yardstick for crime comparison among various States/UTs. 'Crime Rate', which is defined as number of crimes registered per 1,00,000 population, is universally taken as a realistic indicator since it balances the effect of growth in population and size of State.[iv]

Delhi (916.8), Kerala (723.2), Madhya Pradesh (348.4), Assam (321.8), Haryana (310.4), Telangana (290.7), Rajasthan (273.9) and Tamil Nadu (271.2) have reported high crime rate as compared to the national average of 234.2.[v] There were 815 police districts in the country (including railway police & special police cell) during the year 2015. Out of 815 police districts, 597 districts have reported more than 1,000 cases of IPC crimes during 2015. [vi]

The police districts which have registered more than 15,000 IPC crimes during 2015 are; Mumbai Commissionerate has reported the highest incidence of IPC crimes (42,940 cases) followed by Bengaluru city (35,576 cases), Malappuram (24,447 cases), Kolkata (23,990 cases), West District of Delhi (23,839 cases), South District of Delhi (23,379 cases), Indore (23,195 cases) and Kottayam (23,000 cases) during the year 2015. [vii]

III. CYBER CRIMES

"Cyber-crime," which refers to any criminal activity committed with the aid of or in the arena of the Internet and similar telecommunications, is both a new incarnation of old

crimes through a new medium, and a unique entity all its own. It differs from physical or "terrestrial" crime in four main ways: being easy to commit, requiring minimal resources for great potential damage, being committable in a jurisdiction in which the perpetrator is not physically present, and often, not being entirely clearly illegal.[viii]

a. Information Technology Act, 2000

The Information Technology (IT) Act, 2000, specifies the acts which are punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have been included in 2008 in the amended Act. Several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC with the legal recognition of electronic records and the amendments made in several sections of the IPC vide the IT Act, 2000.

In year 2015 a total of 8,045 cases were registered under this Information Technology (IT) Act, 2000. The State of Uttar Pradesh (2,161 cases) and Karnataka (1,414 cases) have accounted for 44.4% of the total such cases registered in the country during the year 2015. [ix]

Maximum cases under the Information Technology Act were registered in Bengaluru (1041 cases) followed by Jaipur (459 cases) during the year 2015. Cyber crime Rate was 2.6 in 2015. Bengaluru was top in incidence of cases registered under cyber crimes in states/UTs during 2012 & 2013, followed by Vishakhapatnam, Pune, Jaipur, Kolkata, Hyderabad in incidence of cases registered under cyber crimes in states/UTs during 2012 & 2013.[x]

Information on the cases registered under the IT Act relating to cyber crimes was 8,045 at all India level during the year 2015 in comparison to 7,201 cases during the previous year (2014), showing an increase of 11.7% in 2015 over 2014. 81.6% (6,567 cases) of the total 8,045 cases under IT Act were related to computer related offences (under section 66 & 66A, 66B, 66C, 66D and 66E of IT Act) followed by 10.1% (816 out of 8,045 cases) under publication/transmission of obscene/sexually explicit content (under section 67 & 67A, 67B and 67C of IT Act).[xi]

The age-wise profile of persons arrested in Cyber Crime cases under IT Act, 2000 showed that 62.5% of the offenders were in the age group 18 yrs. – below 30 years (3,188 out of 5,102 persons) and 30.8%(1,573 out of 5,102 persons) of the offenders were in the age group 30 yrs. – below 45 years. 98 juvenile offenders (below 18 years) were apprehended under IT Act during 2015.[xii]

b. Incidences of Cyber Crimes Registered under IPC

Information on the cases registered under various sections of IPC which were considered as cyber crimes. A total of 3,422 cyber crime cases were registered under various sections of IPC during the year 2015 as compared to 2,272 such cases during 2014 at all-India level, thus showing an increase of 50.6% over the previous year. 65.9% (2,255 cases) of the total 3,422 cases registered under different sections of IPC were related to cheating followed by 2.5% (84 cases out of 3,422 cases) under data theft.[xiii]

Out of total persons arrested under the cyber crimes, 35.3% (2,867 out of 8,121) were arrested in connection with cases relating to different sections of IPC during 2015. Out of 2,867 persons arrested under IPC cases relating to cyber crimes, maximum persons have been arrested in cases of criminal breach of trust/fraud (1,292 out of 2,867 persons) accounting for 45.1% of total such persons arrested under IPC crimes followed by 754 persons arrested under cheating cases accounting for 26.3% during the year 2015.[xiv]

The age-wise profile of persons arrested in cyber crime cases under different sections of IPC showed that 55.2%(1,583 out of 2,867 persons) of the offenders were in the age group 18-30 years and 36.1%(1,035 out of 2,867 persons) of the offenders were in the age group 30-45 years. 52 juveniles (below 18 years) were apprehended under cyber crimes related IPC cases during 2015.[xv]

c. Cyber Crimes – Cases of Various Categories under Special and Local Laws (SLL)

A total of 125 cases were registered under various sections of SLL during the year 2015. 90.4% (113 out of 125 cases) of the total cases registered under different sections of SLL were related to the Copyright Act, 1957. Out of 208 cases for investigation, investigations were completed for 112 cases under different sections of SLL during 2015. Cases under the Copyright Act has highest pendency rate (51.8%) during 2015. [xvi]

The age-wise profile of persons arrested in cyber crime cases under different sections of SLL showed that 62.5%(95 out of 152 persons) of

the offenders were in the age group of 30-45 years and 23.3%(43 out of 152 persons) of the offenders were in the age group of 18-30 years. 2 juveniles (below 18 years) were apprehended under SLL crimes during 2015.[xvii]

4 foreign nationals and 8,117 Indian nationals were arrested under cyber crimes. Among foreign nationals, one person was cracker/hacker and has been arrested in Chhattisgarh. Similarly among Indian nationals, most of the persons arrested under cyber crime were 'Business Competitor' with 19.6%(1,594 out of 8,121 persons) of total such persons followed by neighbours / friends & relatives' with 14.7%(1,195 out of 8,121 persons) of total such persons, professional computer geeks/hackers/crackers with 13.5% (1,095 persons), student with 10% (814 persons), sexual freak with 5.1% (415 persons) and employees/disgruntled employees 3.1% (249 persons).[xviii]

IV. CYBER LAW

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace".[xix] It is less of a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction.[xx] In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet.[xxi] Cybercrimes in purview of Cyber law are (i) Software Piracy ,(ii) Hacking,(iii) Data Theft,(iv)Identity Theft,(v)Spreading Virus Or Worms, (vi)Phishing, (vii)Violation Of Privacy, (viii)Cyber Terrorism, (ix) *Child Pornography*. *Apart from* Cybercrimes, *Cyber Squatting* is interdisciplinary crime of in purview IPR and copyright law. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law.[xxii] It has a separate chapter XI entitled "Offences" in which various cybercrimes have been declared as penal offences punishable with imprisonment and fine.

V. REASONS AND MOTIVE FOR CYBER CRIMES

Crimes are much higher in mega cities compared to either small cities or rural areas. High incidents of crimes in mega cities may be due to various factors like high density of population, greater information availability/flow, greater degree of anonymity in big cities, social milieu of urban slums etc. [xxiii]

Motive

Most of the cyber crimes were registered for greed/financial gain accounting for 33.3% (3,855 out of 11,592 cases) followed by fraud/illegal gain (9.6%) (1,119 cases), insult to the modesty of women (5.2%) (606 cases), sexual exploitation (5.1%) (588 cases) and causing disrepute (3.3%) (387 cases).[xxiv]

VI. PROTECTIVE MEASURES

In every mega city there was a cyber wing, established with in the Crime Investigation Department (CID) to look after for cyber crime in Cities. It services not only limited to cities but providing help in catching the criminals. Police commissionarate equipped with advanced technological equipments to catch the cyber criminals. Best example to be Hyderabad city, where advanced cyber tools available with the police department apart from this there was electronic surveillance (CC camaras) with Command Control chamber. Mumbai, Delhi, Bengulure and all other cities were more focusing on cyber crime incidences.

Computer crime, or *cybercrime*, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.[xxv] These categories are not exclusive, and many activities can be characterized as falling in one or more categories. The term cybercrime has a connotation of the use of networks specifically, whereas computer crime may or may not involve networks. [xxvi]

Indian Computer Emergency Response Team is carrying out mock drills with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. These drills have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations.[xxvii]

National Cyber Security Policy-2013(NCSP-2013) was released by Government in August 2013 for public use and implementation with all relevant stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

VII. CONCLUSION

Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cyber criminal. Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime.

The real issue is how to prevent cyber crime. For this, there is need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary. The challenge in cyber crime cases includes getting evidence that will stand scrutiny in a foreign court. [xxviii]

The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC.[xxix]

Cyber crime has serious impact on society in the form of psychological disorder, social disorganization and economic losses. Even though all people suffer from its ill effects, the most vulnerable group is adolescent and youth.[xxx]

Digital technology these days includes much more than just computers.[xxxi] The Communication Technologies (ICTs) and the substantial innovation in the sector have resulted recent evolution of Information and in a significant increase in productivity as well as the emergence of a wealth of new goods and services. The work of ICTs is done at microsecond speed, carrying information invisible to the naked eye, under the control of software developed by people, so harmful intentions in this environment are often carried out rapidly, invisibly, and are difficult, if not impossible, to trace.[xxxii]

Cybercrimes are inherently complex by their very nature. Computers which are complicated machines, the operation of which is really understood by very few people always play a key role in every cybercrime case. Despite the many obstacles that stand in the way of effectively prosecuting cybercrime cases including the difficulty of even defining the crime in the first place, the jurisdictional nightmares that arise when suspect and victim are in different geographic locations, and the attitudes and lifestyle differences that make it difficult for police and IT professionals to work together it is possible to overcome all these challenges and put together a case that will stand up in court.[xxxiii]

Law enforcement agencies can work with prosecutors to clarify definitions and ensure that they understand the elements that must be proven to arrest and convict in a cybercrime case. IT personnel who anticipate working with law enforcement on cybercrime cases must learn the basics of how the criminal justice system operates, and both must know how civil, criminal, and regulatory laws differ and which specific acts fall under which bodies of law in their jurisdiction.[xxxiv]

Law enforcement officers and IT professionals can learn to work together on cybercrime cases, resulting in much more effective investigations than either could conduct alone. Police officers need to learn technical terminology, and IT personnel need to become comfortable with the language of law and police jargon so the two can better understand one another. A successful prosecution is based on the work of many people and on many factors. An important element in building a solid case hinges on proper implementation of the investigative process.

.

REFERENCES

[1] Castells, Manual and Pekka Himanen (2002), The Information Society and the Welfare State: The Finnish Model.), Pg 208-23, Oxford UP, Oxford

[2] Kshetri, Nir (2010), The Global Cybercrime Industry, Springer, New York. Pg.3

[3] George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, Alan Schwartz , Information Technology Security Handbook, , The International Bank for Reconstruction and Development / The World Bank, 2003, pg.89

[4] "Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India

[5] Ibid,

[6] Ibid,

[7] Ibid,

[8] HAWKI, MOHAMED. "A CRITICAL LOOK AT THE REGULATION OF CYBERCRIME." COMPUTER CRIME RESEARCH CENTER. RETRIEVED FROM HTTP://WWW.CRIME-RESEARCH.ORG/ARTICLES/CRITICAL/ A CRITICAL LOOK AT THE REGULATION OF CYBERCRIME (LAST ACCESSED ON 12.09.2017 AT 13:18)

[9] "Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India

[10] " Crime India 2013" National Crime Records Bureau, Ministry of Home Affairs, Government of India

[11] "Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Ibid
[16] Ibid
[17] Ibid
[18] ibid
[19] CYBER LAWS, retrieved from http://infosecawareness.in/cyber-laws-india(Last Accessed on: Feb 12, 2017 08:48 PM)
[20] CYBER LAWS retrieved from https://notesmilenge.files.wordpress.com/2014/08/cyber-mod-3.doc (Last Accessed on: 12.09.2017 12:48 PM)
[21] CYBER LAW retrieved from http://www.leintelligensia.com/cyber-law-services-india(Last Accessed on: 12.09.2017 12:48 PM)
[22] Pradeep Mishra, "Types of Cyber Crimes & Cyber Law in India" retrieved from https://www.linkedin.com/pulse/20140828035155-72824304-types-of-cyber-crimes-cyber-law-in-india (Last Accessed on: 12.09.2017 14:48 PM)
[23] "Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India
[24] ibid
[25] This definition is from the New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement (information-retrieval.info/cybercrime/index.html).
[26] William Stallings , Cryptography and Network Security Principles and Practice, Prentice Hall, New York,2011, pg.843
[27] Dr. Gulshan Rai, "Securing Cyber Space", retrieved from http://www.pib.nic.in/newsite/mbErel.aspx?relid=98163((Last Accessed on: 12.09.2017 14:48 PM)
[28] Talwant Singh, Addl. Distt. & Sessions Judge, Delhi "Cyber Law & Information Technology"
[29] Ibid
[30] India Digital Future in Focus, ,Retrieved from www.comscore.com/content/India-Digital-Future-in-Focus-2013(August 22,2016)
[31] George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, Alan Schwartz , Information Technology Security Handbook, pg.15, The International Bank for Reconstruction and Development / The World Bank, 2003
[32] Ibid. Pg.1
[33] Debra Littlejohn Shinder, Michael Cross, Scene of the Cybercrime: Computer Forensics Handbook,Pg.655, Syngress - 2008
[34] Ibid

---

[i] Castells, Manual and Pekka Himanen (2002), *The Information Society and the Welfare State: The Finnish Model.*), Pg 208-23, Oxford UP, Oxford
[ii] Kshetri, Nir (2010*), The Global Cybercrime Industry*, Springer, New York. Pg.3
[iii] George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, Alan Schwartz ***, Information Technology Security Handbook,*** , The International Bank for Reconstruction and Development / The World Bank, 2003**,** **pg.89**
[iv]"Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India
[v] Ibid,
[vi] Ibid,
[vii] Ibid,
I. [viii] CHAWKI, MOHAMED. "A CRITICAL LOOK AT THE REGULATION OF CYBERCRIME." COMPUTER CRIME RESEARCH CENTER. RETRIEVED FROM HTTP://WWW.CRIME-RESEARCH.ORG/ARTICLES/CRITICAL/ A CRITICAL LOOK AT THE REGULATION OF CYBERCRIME (LAST ACCESSED ON 12.09.2017 AT 13:18)
[ix] "Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India
[x] " Crime India 2013" National Crime Records Bureau, Ministry of Home Affairs, Government of India
[xi] "Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India
[xii] Ibid.
[xiii] Ibid.
[xiv] Ibid.
[xv] Ibid
[xvi] Ibid
[xvii] Ibid
[xviii] ibid
[xix] CYBER LAWS, retrieved from http://infosecawareness.in/cyber-laws-india(Last Accessed on: Feb 12, 2017 08:48 PM)
[xx] CYBER LAWS retrieved from https://notesmilenge.files.wordpress.com/2014/08/cyber-mod-3.doc (Last Accessed on: 12.09.2017 12:48 PM)
[xxi] CYBER LAW retrieved from http://www.leintelligensia.com/cyber-law-services-india(Last Accessed on: 12.09.2017 12:48 PM)
[xxii] Pradeep Mishra, "*Types of Cyber Crimes & Cyber Law in India*" retrieved from https://www.linkedin.com/pulse/20140828035155-72824304-types-of-cyber-crimes-cyber-law-in-india (Last Accessed on: 12.09.2017 14:48 PM)
[xxiii] "Crime in India-2015", National Crime Records Bureau, Ministry of Home Affairs, Government of India
[xxiv] ibid
[xxv] This definition is from the New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement (information-retrieval.info/cybercrime/index.html).
[xxvi] William Stallings , *Cryptography and Network Security Principles and Practice*, Prentice Hall, New York,2011, pg.843

[xxvii] Dr. Gulshan Rai, "*Securing Cyber Space*", retrieved from http://www.pib.nic.in/newsite/mbErel.aspx?relid=98163((Last Accessed on: 12.09.2017 14:48 PM)

[xxviii] Talwant Singh, *Addl. Distt. & Sessions Judge, Delhi "Cyber Law & Information Technology"*

[xxix] Ibid

[xxx] India Digital Future in Focus, ,Retrieved from www.comscore.com/content/India-Digital-Future-in-Focus-2013(August 22,2016)

[xxxi] George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, Alan Schwartz , ***Information Technology Security Handbook,*** **pg.15**, The International Bank for Reconstruction and Development / The World Bank, 2003

[xxxii] Ibid. Pg.1

1) *[xxxiii] Debra Littlejohn Shinder, Michael Cross, Scene of the Cybercrime: Computer Forensics Handbook,Pg.655, Syngress - 2008*

[xxxiv] Ibid.