International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 3; Issue 1; January 2018; Page No. 640-644

Indian cyber law

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

Abstract
A rapid increase in the use of computer and internet has given rise to new forms of crimes. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes. 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. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. The information Technology Act was enacted in the year 2000.Threats emanate from a wide variety of sources, and their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole. The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Threat actors can operate with substantial impunity from virtually anywhere. Many malicious tools and methodologies originate in the efforts of criminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions. The legal defense to prevent and control of the Cyber Crime under Information Technology ACT, 2008, Indian Penal Code 1860 and some suggestions are to be explored in this Research paper.

Keywords: cyber crime, computer resources, network, offence

Introduction

"This world cyberspace is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history."

President Barack Obama, May 29, 2009

The Indian Law has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the Information Technology (amendment) Act 2008. The term 'Cyber Crime' is combination of two words 'cyber' and 'crime'. Crime is a legal wrong that can be followed by criminal proceedings which may result into punishments [1]. *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 [2]. 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 [3].

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace" [4]. 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 [5]. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet [6].

Scope and Methodology

Information Technology (IT) Act, 2000, 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, Indian Evidence Act, 1872, Criminal Procedure Code, Information Technology (Certifying Authorities) Rules, 2000, Information Technology (IT) Security Guidelines and Cyber Security policies of Government of India, treaties and convention on cyber security, need of cyber forensic standards, cryptographic law will be covered and my methodology of research is doctrinal approach.

Research Objectives

The Research objectives (i) to train and engage more cybercrime investigation professionals and cyber warriors (ii) to legislate cyber security law, enhance cyber crime law and (iii) to establish more efficient cyber forensic labs in India.

Cyber Crimes

In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law [7]. It has a separate chapter XI entitled "Offences" in which various cybercrimes have been declared as penal offences punishable with imprisonment and fine.

The some of the Cybercrimes to be: (a) Software Piracy, (b) Hacking, (c) Data Theft,(d)Identity Theft,(e)Spreading Virus Or Worms, (f)Phishing, (g)Violation Of Privacy, (h)Cyber

Terrorism, (i) Child Pornography (j) Cyber Squatting.

a. Software Piracy

Theft of software through the illegal copying of genuine programs or Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force. Such act shall be punishable with imprisonment up to 3 years, or with fine which may extend up to Rs. 2,00,000/-, or with both under section 65 of IT (Amendment) Act, 2008.

b. Cyber Stalking

Cyber stalking refers to the use of the Internet, e-mail, or other telecommunication technologies to harass or stalk another person. It is not the mere annoyance of unsolicited e-mail. It is methodical, deliberate, and persistent. The communications, whether from someone known or unknown, do not stop even after the recipient has asked the sender to cease all contacts, and are often filled with inappropriate, and sometimes disturbing, content. Cyber stalking is an extension of the physical form of stalking. Cyber stalkers may initially use the Internet to identify and track their victims. They may then send unsolicited e-mails, including hate, obscene or threatening mail [8]. Cyber stalking is offence under Sec.66A clause (b) of IT Act shall be punishable with imprisonment up to 3years and with fine.

c. Hacking

'Hacking' is a term used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the public or that person. Section 66 provides that a person who commits hacking shall be punished with a fine up to Rs.2 lakhs or with imprisonment upto 3 years, or with both. The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications. Under Information Technology (Amendment) Act, 2008, Section 43(a) [9], 43(i) [10] read with section 66 is applicable and Section 379 [11] & 406 [12] of Indian Penal Code, 1860 also are applicable.

d. Data Theft

If any person without permission of the owner or any other person, who is in charge of a computer, computer system of computer network - downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, then it is data theft, this may be punishable with imprisonment up to 3years or fine up to Rs.5,00,000/- or with both. Under Information Technology (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable and under Section379 [13], 405 [14] & 420 [15] of Indian Penal Code, 1860 also applicable.

e. Identity Theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft. Under Information Technology (Amendment) Act, 2008, Sec.43 (j) [16], Section 66-C and Section 417A [17] of Indian Penal Code, 1860 also applicable.

f. Spreading Virus or Worms

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network. This is crime under Information Technology (Amendment) ct, 2008, Section 43(c) [18] & 43(e) [19] read with Section 66 is applicable and under Section 268 [20] of Indian Penal Code, 1860 also applicable.

g. Phishing

Phishing email messages, websites, and phone calls are designed to steal money. Cyber criminals can do this by installing malicious software on your computer or stealing personal information off of your computer. Cyber criminals might call you on the phone and offer to help solve your computer problems or sell you a software license. Once they've gained your trust, cyber criminals might ask for your user name and password or ask you to go to deposit money. Common practices in Phishing are Spelling *and Bad Grammar, Links in Email, Threats, Spoofing Popular Websites or Companies* [21]. Under Information Technology (Amendment) Act, 2008, Section 66-D [22], 43(h) [23] of IT Act and Section, 417A [24], 419A [25] & 465 of Indian Penal Code, 1860 also applicable.

h. Violation of Privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 years or with fine not exceeding Rs.2,00,000/-, or with both, this has been inserted vide Sec.66E in IT Act, provides punishments in IT Act 2008, and in Indian Penal Code section 502A inserted to provide Privacy.

i. Cyber Terrorism

This may said to be a Cyber crime against Government. Cyber Terrorism which intended to threaten the unity, integrity, security or sovereignty of nation. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. *According to Sec 66Fof IT(Amended) act 2008,* Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

j. Child Pornography

The emergence of Internet facilitated sex crimes, including child pornography, has raised crucial questions regarding the use of the Internet by offenders and the law enforcement

challenges in addressing these offenses. The problem of child pornography possession was thought to have been minimized prior to the emergence of the Internet. However, there is a general consensus that the Internet has made child pornography more accessible and available to collectors and distributors. Child pornography can be obtained and traded on the World Wide Web, using Internet and via other online sources. Child pornography possession cases involve the use of the Internet or computer technology to possess and/or collect electronic images of child pornography. These investigations present challenges for law enforcement agents around the world [26].

According to Section 67-B, Information Technology act, 2000 Whoever,- publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to 5 years and with a fine which may extend to Rs.10,00,000/- and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to Rs.10,00,000/-

k. Cyber Squatting

Cybersquatting is generally bad faith registration of another's trademark in a domain name [27]. If someone registered a domain name in a generic top-level domain (gTLD) operating under contract with ICANN similar to your trademark, you may be able to file a Uniform Domain Name Dispute Resolution Policy (UDRP) proceeding [28]. Cybersquatting means using somebody's name and creating a website for one's benefit. There are no cybersquatting laws in effect India but, the law of Patents, Law of Copy rights may help to prevent it. Cyber squatters around the world have begun to use the suffixes at the end to promote their businesses.

Findings

"Cyber Security" is defined under Section 2-D *(nb)* means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. Cyber Security policy and IT Act explains that there should be a Indian Computer Emergency Response Team to look over Cyber Security and emergency. Here we have Section 69 in IT act (Substituted Vide ITAA 2008), which provides Powers to central Government or a State Government or any of its officer specially authorized to issue directions for interception or monitoring or decryption of any information through any computer resource, in the interest of the sovereignty or integrity of India, defense of India, security of the State, for preventing incitement to the commission of any cognizable offence relating to Cyber Security.

According to Section 69, A Power to issue directions for blocking for public access of any information through any computer resource, Where the Central Government in the interest of sovereignty and integrity of India, defense of India, security of the State. Whereas Section 69B of IT Act enumerates Central Government may authorize to monitor and collect traffic data or information through any computer resource for Cyber Security, by notification in the official Gazette.

As reported in titled "Responding to cyber crime incidents in India" report, employees are the second-largest source of risk after unknown hackers. "Employees post extensive details regarding their work profile on social networking websites. These social media platforms act as a gold mine for cyber criminals to identify and target key individuals for a successful breach," it said. The report quoted a McAfee study to say that India is estimated to be losing 0.21% of its gross domestic product (GDP) to cyber crime and the numbers of incidents were increasing each year. About two-thirds of businesses were unable to detect a cyber incident in real time due to insufficient understanding of the motive behind the attack. While 55% of respondents said that cyber security laws need to be strengthened, 34% said regulations in the cyber law space need to be clearer, the report revealed. The report is based on more than 160 interviews with senior and middle management executives. Over 50% of the respondents are employed in listed companies. A majority of 72% of the respondents believe their company's IT security teams lack specialists to deal with cyber crime incidents, while just 40% believe their techniques around proactive monitoring of cyber crime are adequate. 40% of respondents plan to spend more on investigation and forensic capabilities in their organisations. The report identifies five key sectors affected by cyber crime technology, media and telecommunication (26%), financial services (24%), automotive and transportation (8%), government and public sector units (8%) and real estate, construction and hospitality (8%) [29]. According to National Cyber Security policy there is need of more than 5,00,000 *cyber security professionals* in the coming 5 years, but India lacks the plans to meet the target. All it has now is just 22,000 identified trained security experts. Though the UGC asks universities to offer a course in cyber security, there is hardly any idea among them on how to go about it [30].

More than 12,000 incidents of cybercrime were reported in 2016, but nearly the same number of such crimes carried forward from the previous years had not been investigated, the data released by the National Crime Records Bureau (NCRB) said. Only in 30% cases reported in 2016, the police or the investigating agency filed a charge sheet. In absolute numbers, 7,990 persons were arrested for the crimes, which included 147 women and charge sheets were filed against 4,913 accused. Illegal gain (5,987 incidents) and revenge (1,056) were the two top motives that accounted for cybercrimes. Sexual exploitation (686), insulting the modesty of women (569) and causing disrepute (448) constituted 13% of the crimes [31].

Maximum number of cases under cyber-crimes were reported in Uttar Pradesh (2,639 cases) (21.4%) followed by Maharashtra (2,380 cases) (19.3%) and Karnataka (1,101 cases) (8.9%) during 2016. During 2016, 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) [32].

Recommendation

Cyber Insurance reduce the Cyber vulnerability mitigate the economical loss. Cyber-insurance is enormously beneficial in the event of a large-scale security incident. Insurance provides a smooth funding mechanism for recovery from major losses, helping businesses to return to normal and reducing the need for government assistance.

At a time when cyber threats are on the rise for banks for increasing cashless transactions and effects of demonetization, insurers see rise in demand for cyber insurance and cyber liability insurance, in particular [33]. Cyber insurance is a tailor made insurance offering providing comprehensive cover for liability and expenses a business may incur arising out of unauthorised use of, or unauthorised access to, physical and electronic data or software within an organisation's computer network or business. Cyber insurance policies can also provide coverage for liability, costs and expenses arising from network outages, the spreading of a virus or malicious code, computer theft or extortion. Traditional business insurance policies have tended to only cover "tangible" assets such as PCs, lap tops and other mobile devices [34].

Conclusion

Cyber Criminals may from outside India and inside India easily escaping due advancement in Technology, they might using fake Internet Protocol (IP) Address, doing crimes using foreign country servers and using fake physical addresses. Then it is difficult to catch and punish the Cyber Criminals. There should be a huge need to create cyber warriors [35], because there is the lack of adequate trainable talent in the country.

Our law enforcement agency is not ready to tackle the issues of Cyber crimes. The law Enforcing authority in India not well equipped to prevention and detection of cyber crimes. The progress in the law is slower than the progress in the Information Technology. To enforce Cyber Law especially all Judges, Judicial Officer and Investigating officers have to fully aware about Cyber crimes. Cyber Law has both technical and legal aspects to understand widely. Some cyber crime investigations require considerable computer processing power, communications capacity, and storage capacity, which may be beyond the budget of individual jurisdictions.

References

1. Granville Williams, Britain's Media: How they are Related - Media Ownership and Democracy (Campaign for Press and Broadcasting Freedom, with support from Unison and the Row tree Trust 1996)
2. This definition is from the New York Law School Course on Cybercrime, Cyber terrorism, and Digital Law Enforcement (information-retrieval.info/cybercrime/index.html).
3. William Stallings, 'Cryptography and Network Security' (Prentice Hall, New Delhi, 2006) 843
4. Cyber Laws, <retrieved from http://infosecawareness.in/cyber-laws-india(Last Accessed on: Feb 12, 2017 08:48 PM)>
5. Cyber Laws <retrieved from https://notesmilenge.files.wordpress.com/2014/08/cyber-mod-3.doc (Last Accessed on: 12.09.2017 12:48 PM)>
6. Cyber Law <retrieved from http://www.leintelligensia.com/cyber-law-services-india(Last Accessed on: 12.09.2017 12:48 PM) >
7. 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)>
8. <docshare03.docshare.tips/files/12161/121613192.pdf>
9. Sec 43of ITAA2008,If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -(a) Accesses or secures access to such computer, computer system or computer network or Computer resource
10. If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network (i) Destroys, deletes or alters any information residing in a computer resource or diminishes.
11. IPC Sec.379 Punishment for theft —whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
12. IPC Sec.406. Punishment for criminal breach of trust — Whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
13. IPC Sec.379 Punishment for theft
14. IPC Sec. 405Criminal breach of trust —Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or willfully suffers any other person so to do, commits "criminal breach of trust".
15. IPC Scc.420 Cheating and dishonestly inducing delivery of property —Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
16. If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network - (j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008).
17. IPC Sec.419A. Punishment for cheating by personation —whoever by means of any communication device or computer resource cheats by personation shall be punished with imprisonment of either description for a

term which may extend to three years, or with fine, or with both.
18. If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network - (c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
19. If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network - (e) Disrupts or causes disruption of any computer, computer system or computer network;
20. IPC Sec.268. Public nuisance —A person is guilty of a public nuisance who does any act or is guilty of an illegal omission which causes any common injury, danger or annoyance to the public or to the people in general who dwell or occupy property in the vicinity, or which must necessarily cause injury, obstruction, danger or annoyance to persons who may have occasion to use any public right.
21. <https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx Last Accessed on 10.05.2017 at 16:23)>
22. [Section 66D] Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008): Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
23. If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network - (h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.
24. 417A.Punishment for Identity Theft-Whoever Cheats by using the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for term which may extend to two years and shall also be liable to fine.
25. IPC Section.419A. Punishment for cheating by personation
26. Wells, Melissa, Finkelhor, David, Wolak, Janis *et al*. Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession 1. Police Practice and Research. 2007; 8:269-282. 10.1080/15614260701450765.
27. Evaldas Cerkesas. The Right to a Domain or How to Prevent a Cybersquatting. <retrieved from https://www.linkedin.com/pulse/right-domain-how-prevent-cybersquatting-evaldas-cerkesas (accessed on 12.09.2017 at 04:42pm)>
28. <http://www.icann.org/en/resources/compliance/complaints/ip/cybersquatting>
29. Rozelle Laha. 90% firms see social media as a big risk area for cyber crime: EY report, <retrieved from http://www.livemint.com/Industry/iakqEYUGMz939tftJBVyxI/90-firms-see-social-media-as-a-big-risk-area-for-cyber-crim.html accessed on Fri, May 05 2017. 01 46 AM IST>
30. Kaushik Deka. The new battlefield is online. Is India prepared? <retrieved from http://indiatoday.intoday.in/story/cyber-crime-cyber-attack-malware-cyber-security/1/1037598.html last accessed on 12.09.2017 at 17.00 IST)>
31. Vijaita Singh. Many Cybercrime Cases Not Investigated, The Hindu, New Delhi, 2017
32. Crime in India 2016, NCRB
33. Banks rush to buy cyber security cover as digital payments rise PTI Feb 12, 2017, 04.23 PM IST, Mumbai, <http://timesofindia.indiatimes.com/business/india-business/banks-rush-to-buy-cyber-security-cover-as-digital-payments-rise/articleshow/57109647.cms accessed on 22.05.2017 @12.45 pm>
34. Cyber Insurance Research Paper, Centre for Internet safety, Sponsored by American International Group, Inc. (AIG)
35. Cyber warriors are Cyber Forensic professionals, Cyber or Information Security Professionals and Cyber law enforcing professionals.