CYBER CRIME & CYBER TERRORISM IN INDIA

Dr. Sumeet Pal Singh Brar, Visiting Assistant Professor, Department of Law, Punjabi University, Patiala, Punjab

ABSTRACT

As the need for the internet increases, so does the need for the protection of information and data. Whether you are a company owner, a business owner or just a regular internet user, you should know how to minimise threats, risks and cybercrime, as well as how to be proactive, cautious and stay informed about Cyber-criminals. With the development of technology, people have become dependent on the internet for all their needs. The internet has made it possible for people to access everything at any time from any location. Social networking sites, online shopping sites, data storage sites, gaming sites, online education, online job sites, you name it, everyone can do it through the internet. The internet is used in nearly every sphere. The internet and its advantages have also led to the development of cybercrime.

I. Introduction

The world is indeed, undergoing a new information revolution today. It not only touches every aspect of life but also makes the way extensively to perform the industrial and economic function of the society. New communication system and digital technology have made dramatic changes in the way we live. A revolution has been occurred due to technological progress.[1] Almost everybody is making substantial use of computers and the internet's are becoming an essential part of our daily life. They are being used by individuals and societies to make their life easier. They use them for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and almost all aspects of life.

Computers and the Internet continue to pervade human life in everything from automobiles to kitchen appliances. With the invention of computers, its increasing use and human dependency over Internet, while we have gained manifolds in terms of efficiency and management, it has also brought to the front many negative effects and disadvantages.[2]

Individuals or groups can now use Cyberspace to threaten International governments, or terrorize the citizens of a country. The crime of "cracking" can escalate into terrorism when an individual "cracks" into a government or military-maintained website. Cyber terrorism could be hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage for an act of revenge.[3]

Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe.[4]

II. Evolution, Nature and Scope of Cyber Crime

Cybercrime is the deadliest epidemic confronting our planet in this millennium. At present when everything from microwave ovens and refrigerators to nuclear power plants are

[1] Shalhoub Karake, and Lubna Al Qasimi, *Cyber law and cyber security in developing and emerging economies* 134 (Edward Elgar Publishing, London, Reprint edn., 2010)
[2] *Ibid.*
[3] Jatin Patil, "cyber laws in India: an overview." 4.01 *Indian journal of law and legal research* 139 (2020)
[4] Neal Kumar Katyal, "Criminal law in cyberspace" 149.4 *University of Pennsylvania Law Review* 103 (2001).

being run or computers cybercrime has assumed rather sister implication.[5]

It has raised its head as multi headed hydra. Where if one is being cut other and newer kinds of crimes appear or develop suddenly cyber-crime can involve criminal activities that are traditional in nature, such as theft, fraud forgery, defamation and mischief. The above of computer has also providing an scope of new age crime such as hacking, web defacement cyber stalking, web jading etc.[6]

Cyber-crime is a twentieth century fetus of technological development, now which grown up like as epidemic and has become uncontrollable in the twenty-first century.[7]

There are different categories of cybercrimes they are as follows

A. Data Interception

An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker in attempt to initiate the establishment of a data stream or influence the nature of the data transmitted.[8]

B. Data Modification

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites.[9]

In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing

[5] Shrikant Pajankar, "Cyber-crimes and cyber laws in India." 7.1 *Delta National Journal of Multidisciplinary Research* 25 (2020).
[6] *Ibid.*
[7] *Available* at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3122318 (visited on June 2, 2023).
[8] CAPEC-117:Data Interception Attacks, *Available* at http://capec.mitre.org/'data/definilions/l 17.htral (Visited on February 24, 2023)
[9] Oracle (2003), Security Overviews, *Available* at: http://docs.oracle.com/cd/B13789_01/ network.lOl/ bl0777/overview.htm, (Visited on February 24, 2023)

the dollar amount of a banking transaction from $100 to $10,000.

C. Data Theft

Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.[10]

D. Unauthorized Access

"Unauthorized Access" is an insider's view of the computer cracker underground. The fihiiing took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality.[11]

E. Virus Dissemination

Malicious software that attaches itself to other software like virus, worms, Trojan Horse, Time bomb, Logic Bomb, are examples of malicious software that destroys the system of the victim.[12]

F. Computer-Related Forgery and Fraud:

Computer forgery and computer-related fraud constitute computer-related offenses.[13]

G. Content-Related Crimes

Cyber-sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses.[14]

---

[10] Iqbal Juneed and Bilal Maqbool Beigh "Cybercrime in India: trends and challenges." 6.12 *International Journal of Innovations & Advancement in Computer Science* 187 (2017).
[11] *Supra* note 10 at 188.
[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid.*

III. Legal & Technological Measures To Combat Cyber Crime

In India, the Information Technology Act 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President Assent on 9 June and was made effective from 17 October 2000.[15] The Act essentially deals with the following issues:

1. Legal Recognition of Electronic Documents
2. Legal Recognition of Digital Signatures
3. Offenses and Contraventions
4. Justice Dispensation Systems for cyber-crimes.[16]

Amendment Act 2008: Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA.[17]

The Information Technology Act, 2000 together with Indian Penal Code have adequate provisions to deal with prevailing Cyber Crimes. It provides punishment in the form of imprisonment ranging from two years to life imprisonment and fine / penalty depending on the type of Cyber Crime. However, the Government has taken following steps for prevention of Cyber Crimes[18]:-

[15] *Available* at: http://www.iibf.org.in/ (Visited on February 25, 2023).
[16] *Supra* note at 15.
[17] Nir Kshetri, "Cybercrime and cyber security in India: causes, consequences and implications for the future." 66 *Crime, Law and Social Change* 313 (2016).
[18] *Ibid.*

i. Cyber Crime Cells have been set up in States and Union Territories for reporting and investigation of Cyber Crime cases.[19]

ii. Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.[20]

iii. In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bangalore, Pune and Kolkata for awareness creation and training.[21]

iv. Programs on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber-crimes for judicial officers.[22]

v. Training is imparted to Police Officers and Judicial officers in the Training Labs established by the Government.

Thus the IT Act 2000 tries to amend obsolete laws and offers new techniques to handle cyber-crimes. As a result, the IT (Amendment) Act, 2008 formed which is effective since 27 October, 2009 and made marked amendments in IT Act, 2000.[23] IT Act 2008,[24] introduced corporate responsibility in S. 43A, important definitions are added, legal validity of electronic documents has been re-emphasized, critical information infrastructure has been signified and much more recent amendments.

Thereby it could be well said the legal enforcement against the cyber-crime & cyber terrorism is uphill and confronting these crimes at forefront saving & preserving civil society at large.

[19] *Ibid.*
[20] *Ibid.*
[21] *Ibid.*
[22] *Supra* note at 17.
[23] The Information Technology Act, 2000 (Act 21 of 2000)
[24] The Information Technology (Amendment) Act, 2008 (Act no 10 of 2009)

IV. Conclusion

To sum up, though a crime-free society is Utopian and exists only in dreamland, it should be constant Endeavour of rules to keep the crimes lowest. Especially in a society that is dependent more and more on technology, crime based on electronic offences are bound to increase and the law makers have to go the extra mile compared to the fraudsters, to keep them at bay. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even DoS or DDoS) are all technologies and per se not crimes, but falling into the wrong hands with a criminal intent who are out to capitalize them or misuse them, they come into the gamut of cyber-crime and become punishable offences.

Hence, it should be the persistent efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes. It should be the duty of the three stake holders:-

i) The rulers, regulators, law makers and investigators.

ii) Internet or Network Service Providers or banks and other intermediaries.

iii) The users to take care of information security playing their respective role within the permitted parameters and ensuring compliance with the law of the land.