EMERGENCE AND DEVELOPMENT OF CYBER SPACE JURISPRUDENCE IN INDIA: A SOCIO-ANTHROPOLOGICAL STUDY

A DISSERTATION TO BE SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF MASTER OF LAWS

Submitted BY

VIBHU BANERJI
UNIVERSITY ROLL NO. 1200997059
School of legal studies

UNDER THE GUIDANCE OF

Dr VATSLA SHARMA
ASSISTANT PROFESSOR
School of legal studies

BBD UNIVERSITY

Session: 2020 – 2021

Certificate of Supervisor

This is to certify that the dissertation titled, "*Emergence and Development of Cyber Space Jurisprudence in India: A Socio-Anthropological Study"* is the work done by *Vibhu Banerji* under my guidance and supervision for the partial fulfilment of the requirement for the Degree of **Master of Laws** in School of Legal Studies Babu Banarasi Das University, Lucknow, Uttar Pradesh.

I wish her/his success in life.

Date_____

Place-Lucknow

Dr Vatsla Sharma
Assistant Professor
School of Legal Studies
Babu Banarsi Das University
Uttar Pradesh, India

DECLARATION

Title of Dissertation **"Emergence and Development of Cyber Space Jurisprudence in India: A Socio-Anthropological Study"**

I understand what plagiarism is and am aware of the University's policy in this regard.

VIBHU BANERJI

I declare that

(a) This dissertation is submitted for assessment in partial fulfilment of the requirement for the award of degree of **Master of Laws.**

(b) I declare that this **DISSERTATION** is my original work. Wherever work from other source has been used i.e., words, data, arguments and ideas have been appropriately acknowledged.

(c) I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off as his or her own work.

(d) The work conforms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Date_____

Place- Lucknow

Vihu Banerji
University Roll No. 1200997059
LLM (2020-2021)
Criminal and Security Law
Uttar Pradesh, India

Acknowledgement

I would like to express my sincere gratitude to my teacher and supervisor **Dr Vatsla Sharma** ma'am, who gave me the golden opportunity to do this wonderful research on the topic 'Emergence and Development of Cyber Space Jurisprudence in India: A Socio-Anthropological Study'.

Her valuable guidance, help, support and patience has been categorical in completion of this dissertation. This opportunity also helped me in doing a lot of research and I came to know about so many new things. I would like to thank my parents who helped me a lot in gathering different information, collecting data and guiding me from time to time in making this dissertation. They gave me different ideas in making this dissertation unique. I am really thankful and deeply indebted to them.

Thanking you,

Vibhu Banerji

LLM (CSL),

School of Legal Studies,

Babu Banarsi Das University

Contents

Table of Cases

Chapter 1: Introduction

"We are approaching the New Era with 21st-century Technologies with 20th-century governing processes and 19th-century governance structures" Harold A. Linstone, Professor Emeritus, Portland University, Oregon USA

There has been a rise in the number of internet users all over the world. Like India internet usage and first-generation users seems to be on the rise. In India according to a report, the internet percentage per year is at a rise of 34.8% which is around 13.5 % of the total world internet user percentage. According to another report by 2016, there were 4,62,124,989 internet users in the country of India.[1] Internet safety user data protection is crucial as the increasing internet penetration rises is of prime importance for good governance for any developing country. According to the National Crime Records Bureau in India, there has been a categorical rise in the cases of Cybercrimes over the years, 2015 cybercrime grew by 20% in India while there has been an increase of 2458% in the last decade according to a report conducted by Times of India in 2016. According to the National Crime Record Bureau, one-third of the total crime committed in India is related to Cyber jurisprudence. In 2014 the total number of Cybercrimes in India were reported to be 9622 whereas it dropped two 11592 in 2015. While there has been a consistent rise in the rate of Cybercrimes in India the cyber laws are yet to be modified to that extent where it can be effective to curtail the rising cases in this country.

The technology of the internet is bringing the world together. The amalgamation of convenience and various other services and platforms makes the user consistently use the technology. The recent increase in the number of mobile phone users in India shows that this axiom is correct to an extent. Today is the world of cyberspace includes services as education and pharmacy; Telecom has reduced the power that can be controlled from the palm of the hand. According to a report in 2016 in India[2], 24.3 % of the population accessed the internet from mobile phones this figure of mobile phone

[1] Internet Society (2015). ―Global Internet Report 2015: Mobile Evolution and Development of the Internet‖. Geneva, Switzerland

[2] Visited www.cbi.nic.in

users with internet access is supposed to grow 230% by 2021. This rise in internet users in India is a boon and a bane as well. It is a boon because it will bring employment to the people, it will connect individuals across different platforms, it would bridge the gap between communities but this comes to the challenge as data privacy and data security are the foremost challenges and hurdles in this process of making the world more accessible. Today we are dependent on our mobile phones for banking news, relationships, health and fitness, share and the stock market, entertainment, social network connectivity and other information including office sources but little did we know how much data is secured which is shared over the internet. We can upload, download Google and share anything that we like but in a country like India where rumours can be spread through fake news, sharing anything at the fingertips becomes quite a challenge. We have seen in the recent cases where rumours have been spread regarding covid-19 vaccines over Twitter and other fake news are spread especially during sensitive times where the country goes through such as elections pandemics in cases of mob violence a mob lynching. It would be wrong to say that the very smart phone which makes life easier and has become a part of every household is also the source of Cybercrimes in India[3].

Before we understand the evolving jurisprudence of Cyberspace it is important to understand the definition of cyber laws. The term cyber law is very popular as we have heard it multiple times during seminars, workshops and even during classroom discussions. It is important to know the nature and scope of Cyber Law.[4] Cyber law is popularly known as the law of the internet. Whether it is a glamorous word or a part of law response mechanism in itself this needs to be established. There is a direct relationship between unemployment rate in demography and subsequent Cyber crime in that society/state. This is explained through the figure 1.

[3] Source: "Cyberstalking rears its head in the workplace," *MSNBC*, 24 April 2001.
[4] T. Gregorie. Cyberstalking: Dangers on the Information Superhighway, 2002. Available from: http://www.ncvc.org/src/help/cyberstalking.html.

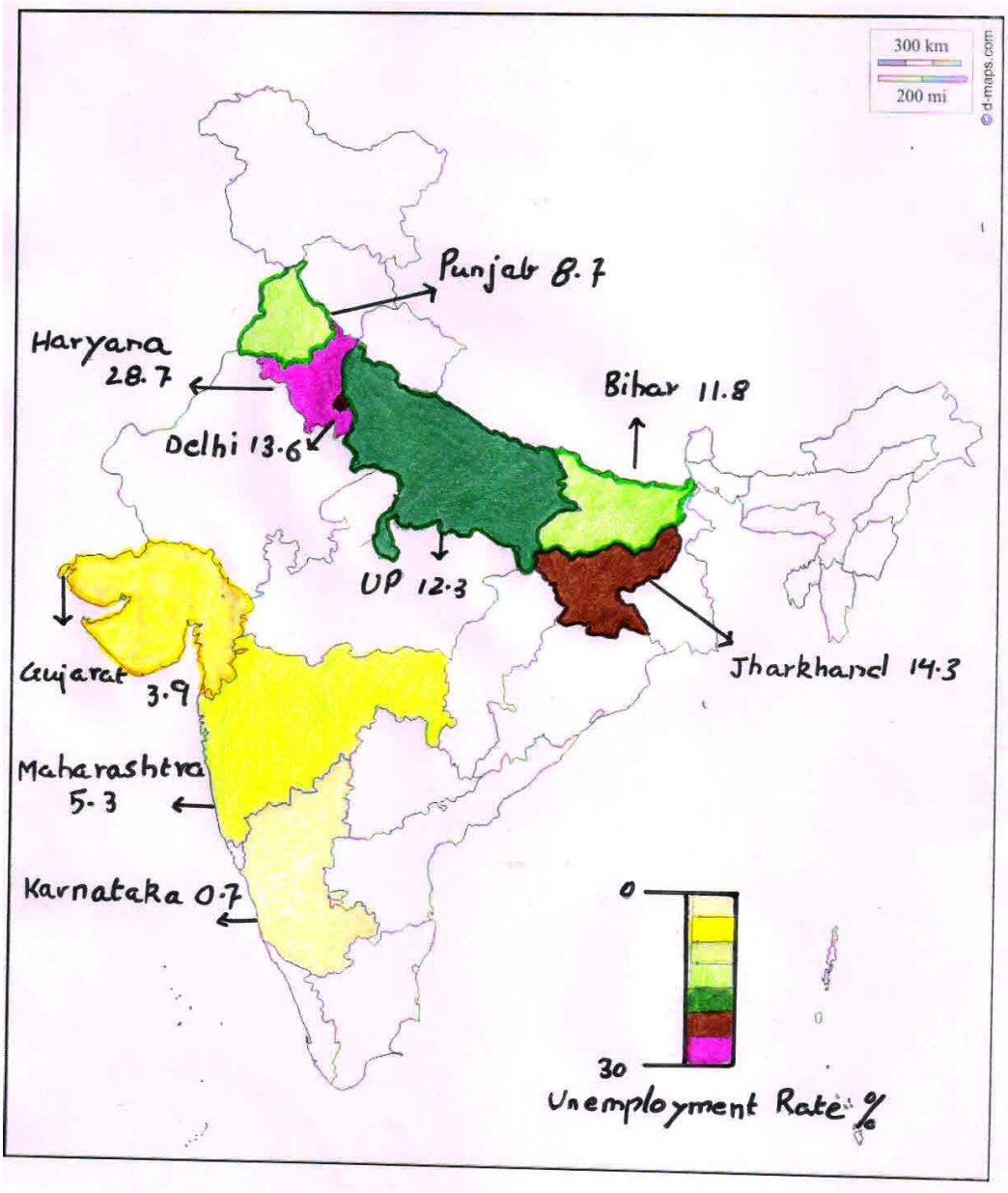

Figure 1: Unemployment in India and Hotspots of Cyber Crime (August 2019)[5]

It is to be noted that in a country like India where there is a disparity in communities, where education is not prevalent, and where there is a lack of awareness regarding issues related to finance, morality and ethics; cyber breaching is possible very easily. Awareness and education are to be kept as fundamentals to stop this breaching.

[5] Centre for Monitoring Indian Economy, https://unemploymentinindia.cmie.com

The word cyberspace was coined by novelist **William Gibson**[6] which states that it is a space without any man-made walls or measurable dimensions rather cyberspace is an abstract universe that has the potential to connect individuals across the globe in a short span of time. The rate of growth of internet users in itself is a cause of concern. It is very important to bring about the interface of Technology and law and to update cyber jurisprudence to the 21st century where it can take care of data and privacy.

What one can make out of the branch of Cyber Law is that it is continuously evolving and it interacts with other constitutional provisions various statutes of Indian law with a traditional in nature such as the Indian Penal Code, Indian Contract Act, the intellectual property rights and various other cases involving juristic individuals, and Institution who use the internet as a mode of transaction and communication. Search description of jurisprudence would include internet service telecommunication educational services pharmacy radio and broadcasting television and media service Stock Exchange and Finance, Artificial Intelligence, Service popular entertainment and even with the onset of a pandemic now even the judicial services have all come under the ambit of Cyber jurisprudence and they expect further evolution in the near future. Cyber law has a wide scope as the aforementioned small facet of this jurisprudence is described; it is essential to concentrate on the core issue which makes the operation of the very jurisprudence. There is no hard and fast rule which states the presence of Cyber jurisprudence on a particular subject matter, however whether it can be comfortably said that if the subject matter is influenced by law or regulated by law then there is a great possibility that a certain portion of Cyber jurisprudence applies on the subject matter as well.[7]

To state an example between the interlude of Cyber jurisprudence and one of the most traditional law which is the criminal jurisprudence, it is observed that the modern crimes of digital stalking, voyeurism using technology as a medium or motive to take advantage of an individual or to spread rumours in form of slander or libel, are just examples when one can observe the convergence of the two jurisprudence. Internet frauds and sexual exploitation are especially targeted against children and females, are

[6] Source: https://www.theguardian.com/books/2020/jan/11/william-gibson-i-was-losing-a-sense-of-how-weird-the-real-world-was

[7] Rick Sarre, Laurie Yiu-Chung Lau and Lennon YC Chang, Responding to cybercrime: current trends, Police Practice and Research, 19, 6, 2018, pp 515–516

other crimes which are rising in India. The people who commit crimes by using cyberspace take advantage of the emotionally weak and vulnerable communities especially those people who are not educated and are not aware of the dos and don'ts of cyber security.

Table 1: Factors of Increase in Cybercrimes in India[8]

Cybercrime in India
A Perfect Storm of Anger and Frustration

Mobile-phone ownership encouraged
Mobile telephony was greatly boosted in the 2010s, allowing a glimpse of Western consumerism. These new digital users are not necessarily security smart, making them easy targets.

Labour over supply
One million people in India become age-eligible to join the labour force each month. Due to poor quality training, up to 94% of IT graduates may be unemployable.

Insufficient law enforcement
By late 2018, an average of one cybercrime attack was reported every 10 minutes in India. Overworked and understaffed police solve only an infinitesimal proportion of offences.

Domestic population shifts
Every two seconds, a rural migrant arrived in an urban area looking for work. Up to 60% of Indians now reside in urban areas, many unemployed.

Exposure to racist vitriol
Call-centre employees were often mocked, called racist terms, or accused of stealing jobs. Political and economic grievances mutated into criminal schemes to defraud Westerners.

[8] Source:https://globalinitiative.net/wp-content/uploads/2020/04/India-Cybercrime.10.04.web .pdf

The 21st century is mostly data-driven. Data controls social media trends, it controls markets in finances, and in other words, data controls consumer behaviour. Therefore data becomes one of the most sought-after commodities for any company dealing specially in developing countries with the scope of development is higher and the possibility of exploitation as well. An example of how data works in finance is that when we download an app from Google Play Store or Apple equivalent, it asks us for various permissions such as to access the camera microphone and other saved files on the mobile. Now while you're using the app it records whatever you are speaking therefore if you are talking about the weather, how rainy the week has been and the forecast tells that they will be a thunderstorm in the following weeks subsequently when you have stopped using that particular application but you are browsing something else over the internet you will see much to your amazement that by Cyber wizardry the browsing application is showing you advertisement of products you can use during thunderstorm such as an umbrella. While this form of artificial intelligence is permissible one wonders to what extent ICF personal information is used by these commercial giants[9].

In this dissertation thesis, the writer is going to attempt to understand the various forms of Cybercrimes prevalent in the world, we're going to attempt to give a concrete dimension to the already abstract cyber jurisprudence, following which the author is going to touch upon the various statues in India which are in place to manage, curb and protect Cybercrimes. The discussion of Cyber jurisprudence would be incomplete without judicial pronouncements and policy recommendations that can make cyberspace more user-friendly, secure and safe.

Chapter 2: Types of Cybercrime

As elucidated in the previous section Cybercrime seems to be multifarious which touches many aspects of an individual's life. Preliminary studies reveal that

[9] Source: "Cyberstalking rears its head in the workplace," *MSNBC,* 24 April 2001

Cybercrimes broadly can be divided into two categories. One type of crime is termed **cyber-enabled crimes** and the other type of crime is **cyber dependent crimes**[10].

Cyber dependent crimes happen when a person's personal computer or network of series of computers is breached by a technical person. In other words, such a crime cannot be conducted by a layman. The word person denotes an individual, group of individuals, company, e-corporation, society and juristic person. Therefore, in other words, crime happens when a person with a certain amount of acumen in information and technology uses his knowledge to breach confidential and sensitive information without the consent of the individual being breached. Over the years there has been a rise in cyber dependent crime as internet usage has gone up but it has to be noted that the dependent criminals who had prior knowledge of Information and Technology are less in number. Traditional scammers who use the internet as a medium to scam come under this category of criminals. It is also being seen that in countries where the literacy rate is better and economies are thriving there we see high levels of Cyber dependent crimes. It is contrary to the popular opinion that awareness towards cyberspace creates fewer Cybercrimes. In such countries where the economy is better and there is proper prior wireless about cyberspace, online scams which are haphazard in nature are almost impossible to be executed.[11]

Therefore, to give a geographical viewpoint to this pattern of crime it can be stated very comfortably that developing countries such as India, Western African countries are more prone to Cyber-enabled crimes rather than cyber dependent crimes. Cyber dependent crimes are managed by a small set of sophisticated White Collar criminals, it is to be noted that although in numbers they might be less but the potential to harm is greater. One such example of Cyber dependent crimes is in the recent tweet by an online tribal group that tweeted and tagged entrepreneur billionaire Elon Musk. Threatening that if Elon continues to tweet about cryptocurrency they will hack his space x company. This particular tweet is not a one-off as Elon Musk is a pioneer when

[10] Ayeshea Perera, Why India's financial system is vulnerable to hacks, BBC, 15 November 2019, https://www.bbc.com/news/world-asiaindia-50401008

[11] Jaskiran Bedi, China never had to learn English like India because its economy relied on manufacturing, The Print, 7 February 2020, https://theprint.in/ pageturner/excerpt/china-never-had-to-learnenglish-like-india-because-its-economy-relied-onmanufacturing/361198/

it comes to artificial intelligence, data and security, whereas 5 independent criminals who have prior knowledge of Information and Technology have gone on board and threatened the very pioneer of this jurisprudence.

In contrast to that cyber dependent crimes happen in countries where the economy is dwindling, where opportunities for employment it is less or negligible and where people are illiterate. There is a lack of awareness. In countries like this cyber dependent crimes are undertaken by criminals who are not sophisticated. The criminals take advantage of the lack of awareness and vulnerability of the citizens at large. The apathy of the situation is not limited to citizens only but rather to the criminal justice administration system, which is also complementing as the same system is laxative to recognise and take expedient cognizance of Cyber dependent crimes. It is estimated that online transactions in India would be worth 1 trillion US dollars by 2023.[12] While this figure is great as it indicates the booming economic opportunities in India at the same time this figure of one trillion US dollars is daunting as well as because Indians are or not aware of the new trends and technologies used by cyber abusers. Unless that there is a categorical improvement in statutes which are then complemented by a proactive legal administration system, the South Asian Nations will become a top contender as the capital of the world's cybercrimes.

India has the potential to quadruple cybercrimes in near future because of foreign direct investment and information and technology. In the near future, there would be devices used in India which are essentially marketed and manufactured by foreign companies, therefore, making India and Indians at large vulnerable to International cyber rackets.

In comparison between India and China, it can be said easily that the Chinese Government has taken steps to build pre-existing surveillance systems as well as forming an information and technology giant using Mandarin as the core language communication. Here is the stark comparison between India and China. While they both have a great amount of population, Indians rely on the technology curated and manufactured by International companies, therefore, English is the standard language used while most Indians are not proficient in the English language. We can make

[12] Dominic Casciani, Briton who knocked Liberia offline with cyber attack jailed, BBC, 11 January 2019, https://www.bbc.com/news/uk-46840461.

cyberspace more secure if we use Hindi, which is the local language of India, for most businesses and communication while using information and technology.[13]

To sum up cybercrimes there are levels of complications. The complications define whether the crime is cyber dependent or cyber-enabled. There is small niche of cyber dependent crimes which do not even require a human being at the helm to execute a crime; therefore, artificial intelligence has evolved itself to such an extent that its creator - the human is no longer required to conduct the crime. These types of crimes are executed remotely by Malware and the targets are mostly research and development organisations of corporate and government likewise. Such crimes which require human intervention come under the category of cyberespionage and may have links with governments or organisations working against the government such as Taleban or ISIS. According to a news report, a hacker hailing from the United Kingdom took the internet down from the country of Libya. This was an attempt to vindicate the government of Libya by stalling all communication and transactions which were internet dependent. The power of Cyber dependent crime is that one person can stop the use of the internet of a whole country[14].

While we are on the subject of Cyber dependent crimes it is important to mention the hackers from Eastern Europe who were predominantly active with the preaching of cyberspace in the late nineties. These hackers are alleged to have backing from the Russian Federation and the main purpose of their job was to create interstate conflicts. The Eastern European hackers can be claimed to be the first-ever organised set-up targeted towards particular sovereignty in view of cyber warfare. These hackers try to get confidential information such as nuclear codes, governmental development in the area of security and defence information. To put it simply the purpose of these hackers are to gain access to computer networks of high-profile government offices. According to a report it is claimed that there were seven groups of Cybercriminals that targeted the Western developed countries in the late nineties. Contrary to the opinion of cybercrime which is less dependent on individuals or a lone person working against a government,

[13] Soumyo D Moitra, Cybercrime: Towards an assessment of its nature and impact, International Journal of Comparative and Applied Criminal Justice, 28, 2, 2004, p 106.
[14] Soumyo D Moitra, Cybercrime: Towards an assessment of its nature and impact, International Journal of Comparative and Applied Criminal Justice, 28, 2, 2004, p 210.

nowadays it is more related as an organised network of criminals; back in 1990 it was still rudimentary[15].

Nowadays cybercrime is extremely organised and almost can be compared to a corporation or a corporate company where there are levels and individually different people work in different levels, whereas the landscape of such crime was extremely different in the late nineties. While there might be an organised set up such as the terrorist organisations back in 1998, every individual who was part of the criminal activity in cyber crimes was broadly termed as hackers. Nowadays with the prevalence of computer education in the urban population, it is very easy to learn about coding and the language of computers, therefore there is a predominance of people who can breach into another computer system, therefore, can act like hackers. It can be comfortably said that on the internet today's time people indulge in hacking as a recreational activity[16].

Part of crime committed under cyberspace that becomes extremely difficult to define for law enforcement agencies because of the fact that a certain degree of victim involvement is there in the commission of cybercrime. To put it differently, there is a breach in the victim's personal computer based on some shortcomings on the part of the victim and the victim had not done his due diligence in order to protect his security and privacy. Therefore, it is extremely difficult for law enforcement agencies to distinguish between cyber-enabled crimes and cyber dependent crimes because both involve a certain degree of victim participation. It is to be noted here that the victim's participation is willingly obtained due to his lack of awareness and knowledge of cyberspace[17].

To put it in the broadest terms possible, a cyber dependent crime would be a crime committed against a victim who is well off in society and is a high profile well-protected target; therefore, relying only on technical parameters cannot guarantee the breach of his personal computer, confidential information and privacy. Therefore a

[15] Sramana Mitra, The death of Indian outsourcing is imminent, Huffpost, 6 May 2017, https:// www.huffpost.com/entry/the-death-of-indianoutsourcing-is-imminent_b_59357886e4b06c469 3fb770a/

[16] Snigdha Poonam, Dreamers: How Young Indians Are Changing Their World. Gurgaon: Penguin, 2019, p 247

[17] Ayeshea Perera, Why India's financial system is vulnerable to hacks, BBC, 15 November 2019, https://www.bbc.com/news/world-asiaindia-50401008

cyber dependent crime is not solely dependent on the technical aspects of hacking etc. But it encompasses other aspects of more traditional crimes and such cyber dependent crimes are conducted and executed against people who are in power and of certain importance to the sovereignty such as politicians, businessmen and film stars. On the contrary, if during the execution of the crime there is human to human interaction either virtually or physically then it can be said that the level of security is less thereby the crime conducted in such a manner is Cyber-enabled[18].

The majority of offences committed in India are cyber-enabled in nature. It involves the basic common denominator that is the common man as the target and hackers manipulate them by talking to them over the telephone or reaching out to them via email. The level of sophistication can be low but the human to human interaction creates a link of similarity which makes the common man believe the criminal who is stalking or communicating with them on the other hand. This also explains that a cyber dependent crime is conducted in a society that is well connected, which has a high level of digital awareness and literacy. In other words of society is technological aware. Whereas the demography of India is quite the opposite, therefore, the majority of the crimes committed in India a cyber-enabled in nature, not cyber dependent.[19]

Such types of crime usually involve a person communicating with the other person who is in need of resources such as money. They try to make the other person believe in a story followed by asking for details as the bank account number. After the primary conversation, the other person takes confidence in the other person speaking over the phone and thereby shares the confidential information and thereby commits a mistake.

ITE elucidates the aforementioned point that a certain amount of victim participation is required in order to fulfil the crime. Such types of grains are not only extremely tech savvy or sophisticated but they involve playing the human emotion and breaking of trust. Such criminals are psychologically trained more than their technical IT acumen. It is well established that a society that is not advanced in levels of digitalization is easier to succumb, therefore to defraud people who are not technically sound to use

[18] Rick Sarre, Laurie Yiu-Chung Lau and Lennon YC Chang, Responding to cybercrime: current trends, Police Practice and Research, 19, 6, 2018, pp 515–516

[19] T. Gregorie. Cyberstalking: Dangers on the Information Superhighway, 2002. Available from: http://www.ncvc.org/src/help/cyberstalking.html

smartphones or computers and have little too low understanding of cyberspace are easily targeted and taken advantage off. In addition to that the laid back law enforcement and criminal justice administration service in India makes the hackers very difficult to be traced. Such defrauding activities take place over a catchment sample size of millions, therefore, to trace the hackers over a million telephone calls becomes extremely challenging for the law enforcement agencies. It is also to be noted that crimes committed by such organised groups focus on micro scams such as camping someone for an extremely low amount of money in that way the other person who has been scammed is discouraged to take his matter forward with the law enforcement agencies thus making such operations discreet and underground.

Categories of Cyber Criminals

Actor	Motive	Objective
Hacker	**Egotistical and technical**	**Demonstrates individual prowess by penetrating well-protected public and private-sector networks**
Spy	**Professional**	**Steals secrets from friendly and hostile countries for the purpose of helping own side gain a diplomatic, economic or military advantage**
Terrorist	**Ideological**	**Undermines government's credibility by disseminating hate messages and disrupting public life through interference with critical infrastructure**
Corporate raider	**Monetary**	**Steals information from a business entity that can be used by a rival firm for either product**

		improvement or to inflict reputational damage
Professional criminal	**Monetary**	**Steals information or takes control of a computer system for personal profit, either with the aim of conducting blackmail or perpetrating a fraud**
Vandal	**Egotistical and vengeful**	**Defaces or disrupts internet traffic to a website for the sole purpose of individual gratification**
Voyeur	**Egotistical and sexual**	**Breaches the privacy of another individual or several individuals to satisfy a personal obsession**

Table 2: Types of Cybercrimes and their Essential Ingredients

Hacking

Hacking is the activity by which the Intruder breaches the personal computer of the victim in order to harness confidential information without the prior knowledge or permission of the victim. Hackers are people who commit hacking. They are people who have a great amount of computer knowledge; they have training and education in information and technology and are proficient in more than one computer language. They are experts in that field and have a great amount of command on different software and other technical aspects of cyberspace. We see a transition in hacking while earlier hackers were primarily educated in computer science. Nowadays we are seeing that many individuals take up hacking as a hobby recreational activity and become backdoor hackers as they have learnt the craft over the internet. As far as the motive of hacking is concerned it varies from person to person; individual to individual. While there can be some who hack for the power dissatisfaction and the money there are others who hack computers just for the fun of using then knowledge

for that influence for the society. Some hacking involves harmless breaching of the profile of an individual and posting something ludicrous. For example, there are occasions when the social media profiles of the celebrities such as film stars, politicians are hacked and from their social media platforms and quotes such as tweets are shared stating they are going to give something valuable such as Bitcoin. Later the celebrities restore their social media platforms and communicate to their followers that their accounts were hacked. Another activity is when hackers use their knowledge for devious reasons. For example, recently in India, the personal data of customers from multinational companies such as Dominos and Big Basket were released by a group of hackers on the dark web. Personal information such as address details, telephone numbers, names and ages of customers are now available free on the dark web.[20]

Voyeurism or averice also promotes and fuels the minds of the hackers to conduct hacking on the person's home they feel threatened or violated. There have been instances in the past to where banking details, Corporation, financial data of individuals web reach are shared openly. Hackers have the potential to take command of the personal system and execute commands from the computer of official in such a way that the official himself was in command of the computer and therefore ordered the same. Hackers who have malicious intent behind such activities are called crackers and they're also known as Black hat hackers.[21]

There is a niche Variety of hackers who hack into multinational companies owned by popular and famous businessmen in order to get publicity. The basic reason is to breach the system in order to make the general public aware of malicious activities being conducted by the company-operation. Whereas others indulge in hacking in order to do get even on some terms, for example, if an employee has been fired by a company then the employee takes the termination on his ego and decides to expose and breach confidential information of the company in order to get even with them. An ambiguous space between ethical hacking and criminal hacking is popularly termed **grey hat**

[20] Source:https://www.researchgate.net/publication/271079090_ETHICAL_HACKING_Tools_Techniques_and_Approaches

[21] Survey on Ethical Hacking Process in Network Security, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, Murugavel, 3(7): July, 2014

hacking which basically refers to activities of hacking that are between black and white.

It is to be noted that the greatest minds who have contributed immensely in the fields of Information and Technology were hackers but they decided to use the knowledge for the betterment of society. Dennis Ritchie and Thomson, who are the creators of the UNIX operating system which is by far termed as the predecessor of Linux computing systems, went to such people who were formally involved in hacking but later decided to use the knowledge to create an evolution in personal computing, thereby helping the society. Mark Zuckerberg who is the founder of Facebook and Sean Fleming who was the developer of the Napster application are further examples of people who used knowledge in information technology and personal computing for the betterment of society.[22]

It is important to know how to control hacking in the first place. Experts say that in order to control hacking that is letting the intruder get access to your personal computer it is important to know how hacking is committed. Why it is extremely difficult to comprehend the various aspects of hacking we can discuss in brief regarding the various methods used by hackers to bridge the computer in the following section.

SQL Injections

Every software in the personal computer is run by a series of codes in a particular language of the computer. A hacker is said to have breached software by using SQL injection code thereby making a particular feature of software invalid void or incorrect. Usually, unprotected SQL databases are targeted for such strategic operations. Usually, SQL data sources are beacons that provide entry to the access of confidential information. In a personal computer SQL codes can be as common as username or password, which gives the hacker complete access to the personal computer. The hacker just needs to log-in from the username and password and thereby accessing confidential information related to the privacy and security of sought-after organisations. When the hacker logs-in, the sign-in process fields the information that

[22] Ethical Hacking, International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015

is transferred as an SQL command. This command is the checkpoint which resources that the hacker has placed, that is the right username and password in the computer. If the data which is inserted by the hacker matches from the SQL command then the same hacker is granted access, if the SQL command is the same there then an error 404 on the screen comes up which means that a wrong password or wrong username has been inserted. [23] So basically SQL database is the command section which consists of all the usernames and passwords of the victim home system which is about to be breached. The hacker decodes the SQL code and thereby uses his computer from a remote location, then types the username and password, thereby accessing confidential information. An SQL injection is a type of command with additional in nature, that means that when it is inserted into the world by the web it tries to convert the content from the database into the system it has been logged-in[24]. Therefore, by the successful interjection of an SQL command, the hacker can change vital information, data and Statistics from the victim's computer. This type of hacking can be used to harness information such as financial information, banking information and other important protected passwords and user IDs.

Theft of FTP passwords

This type of hacking is extremely common and it's the way to breach various websites on the internet. What happens is that there are many website owners who store confidential information about their websites such as login information, financial information, balance sheet, the number of stocks in the warehouse etc, on poorly protected personal computers. The hackers take advantage of the fact that the confidential important information is texted and stored in an average PC that does not have high levels of security features. The hacker looks out for the victim's FTP login details and theirby from those details he can hack into the system from his remote location using his own personal computer. Subsequently, he logs into the web, via the remote computer and then manipulates and modifies the web page as per his needs. Therefore to sum up the theft of FTP passwords is in a commercial setting where

[23] K. Spett (2003): Blind Sql injection. White paper, SPI Dynamics, Inc. http://www.spidynamics.com/whitepapers/Blind SQLInjection.pdf.
[24] *Ibid.*

websites are owned by owners who do not invest in computer security systems that by using average computers for additional computers to store confidential and sensitive information regarding their business this very same is then used by the hackers via FTP login, thereby they can access the website of the owner and harness aforesaid data/information[25].

Cross-Site Scripting

Cross-site scripting is highly technical for hacking into a computer. In popular fiction and journalism, the same is abbreviated and well known as XSS. In a typical xss intrusion, the hacker gets inside a website with a *mala fide* intention. In this what happens is that the hacker attacks the website and then tries to fix it with the virus, thereby when a common person who is not aware of such an attack downloads something from his browser, the downloaded file then corrupts his personal computer.[26] There is little to no victim participation in the execution of the cross-site scripting. Ideally, cross-site scripting abusers introduce various computer languages such as ActiveX, flash HTML, JavaScript, VBScript into an application in order to deceive the coding of the website and in this process it also makes the victim who is about to download the file with acceptable virus infliction in his own personal computer. It is important to protect an individual's personal computer from cross-site scripting. It is foremost for investing in a good firewall. It is important to note that the medium through which the hacking is conducted is the internet therefore a secure connection reduces the chance of cross-site scripting. It is advised to take an internet service provider reputed internet service provider in order to mitigate the chances of cross-site scripting.

Virus Dissemination

Virus dissemination is one of the most popular and common ways of breaching an individual's computer. Here the main cause of hacking or including a person's personal computer is not to get access to confidential and private information but to seize the

[25] Theft of FTP Password, Cyber Crime Chamber, https://www.cybercrimechambers.com/blog-theft-of-ftp-passwords-121.php
[26] KirstenS, Cross Site Scripting (XSS), https://owasp.org/www-community/attacks/xss/

application of the personal computer. Viruses are programs which are made in the language of the computer which attaches itself either by files which are uploaded through the system to the internet or can be transferred from one infected computer system to another by Local Area Network. The primary reason may not be to get access to confidential information but to infect the computer in such a way that it cannot proceed with its standard application. This type of hacking is done on a mass scale in order to reduce the productivity of an organisation or to get popular and famous by conducting a crime against a big corporation or company. It is to be noted that viruses are of multiple types, for example Trojan horses, worms and malware[27].

Malware is an acronym that comes from two particular words namely malicious and software. Therefore as the name suggests Malware is a type of software that is made with malicious intent. When the victim installs the software instead of doing the prerequisite activity which it was supposed to do it stops the normal functioning of the computer thereby making the system shutdown. Trojan horses are all different types of viruses and are used for their transport from one system to another by forms of files which look benign in nature as they are set as email attachments or any links of websites which are shared over the internet via email or social media but when the victim clicks or download the file or the link respectively the virus take command of the computing system. This type of infection of virus is extremely common these days as we are using internet mobile applications which send us codes and links quite often in order to avail better and enhance service. It is extremely important to download files from a trusted source and to protect the computer system alongside it is advised to have a good antivirus security system installed in the computer. There is a category of viruses which are called hybrid viruses which exhibit symptoms of both virus and malware. This unique type of virus is called worms. They can be transferred from one system to another through attachment files, links extra whereas they can be directed to

[27] Stallings, William (2012). *Computer security : principles and practice*. Boston: Pearson. p. 182. ISBN 978-0-13-277506-9.

enter a particular system why the hacker thereby does not host the computer as a mode of entrance to a known inflicted fresh computer.[28]

Logic Bombs

Logic bombs are similar to computer viruses but they are different in a few parameters. It is basically a malicious code made in a particular computer language, which is part of a software or computer program. It given directly by the Intruder already installed in the system, waiting for the trigger code to be initiated by the Intruder by his remote computer. In other words, logic bombs are malicious code(s) that is a part of software that is ready to be triggered when the desired action is sort from the software. It is like a bullet loaded in a gun waiting for the finger to press the trigger in order to be fired, till the time the desired command is not initiated by the victim the logic bomb/malicious code lies hidden and harmless as a part of the software, but as soon as the victim process the command for a specific feature in the software and the code is initiated and then it takes over the normal functioning of the computer. Thereby, the victim cannot access his computer for normal day to day functioning. In certain advanced versions of logic bombs, confidential information can be shared from the victim's computer to the system which created the malicious code in the first place[29].

It is important to note that the victim is unaware of the malicious code in the form of a logic bomb being installed as a part of the software used by the computer system. Logic bombs are of different types; they can be installed in a nuclear personal computer or can be installed in multiple computers working and connected to the local area network. Logic bombs can go off at a particular time or on a particular date, thereby, in popular culture it is called logic time bombs. For example, in America, it is said that the 13th day of the month falling on a Friday is considered to be unlucky for the financial market. There have been multiple instances when the computer systems of the stockbrokers of Wall Street have crashed on Friday the 13th, thereby; the hackers wanted the system to be down on a particular date. A cataclysmic explosion takes place one after another when a certain command is sorted from software which triggers the

[28] Éric Filiol, *Computer viruses: from theory to applications, Volume 1* Archived 2017-01-14 at the Wayback Machine, Birkhäuser, 2005, pp. 19–38 ISBN 2-287-23939-1

[29] "Man Indicted in Computer Case". *The New York Times*. 10 February 2000. pp. C.7

malicious code installed inside it and thereafter the computer fails to perform its normal basic functions[30].

It has also been seen that such malicious codes are installed by employees who have been terminated by an organisation. Such disgruntled employees take the designation of termination on the egos and use the knowledge for a malicious intention. Since they have contact with the computers which are used in the office, installing malicious code is often an insider's job. It is to be noted that the application of logic bombs are seldom unitary. Logic bombs are instilled and launched in a series of multiple computers with the logic behind that whenever the malicious code is triggered at a certain point either a certain by the hacker waiting to be triggered by a command invariably launched by the victim, ultimately IT results in an action of a Domino effect whereby the computer systems of the whole unit of a branch of the office is under the influence. The explosive nature of logic bombs slows down typing economies and it is a part of cyber-enabled crimes where a technical person conducts a crime against people who are well-off and cyberspace literate. In order to reduce the chances of logic bombs it is important to install and update a good antivirus program inside the computer, in addition to that conduct regular checks and updates of software. It is extremely important to use the internet from a source verified internet service provider. Furthermore it is extremely important to have trusted employees working in information and technology so that instances of coding such malicious codes are reduced.

Denial of Service Attack

As the name suggests, a denial of service attack is a type of hacking in which there is no actual intrusion by the hacker in order to invade the personal computer. A denial of service attack works in a way in which the victim is not able to access a desired service from the internet. This desired service can be accessing by someone over the internet by browsing a website that includes e-commerce or downloading software or a desired file from the internet.

[30] "Man Indicted in Computer Case". *The New York Times*. 10 February 2000. pp. C.15

A denial of service attack is basically targeted not towards the victim who is unable to access this service but to the big fish in the market, which is the service provider in itself. Usually, the service provider is a big corporation or a company that has an established reputation in the market. The customer, who is in Britain as a by-product, accesses the website in question. There are numerous popup that open up while downloading or using the service which ultimately affects the internet bandwidth thereby making the whole operation of service experience extremely slow even to that point when the computer gets bamboozled. Slow down of the server is the prime objective of denial of service attack. Big websites such as amazon.com, flipkart.com, ebay.com are prime targets of hackers as the traffic on these websites is significantly higher when compared to other websites. The hackers choose a particular day where there is a high number of 'traffic' on these websites. With a combination of different techniques including denial of service attacks, the hackers try to invade the personal computers of the victims and get confidential information such as financial information[31].

The main target in denial of service attack is the bigger consumer and goods provider support the multi-national giants mentioned above, but denial of service attack may not be only directed to 20 multinational companies (by using a combination of different methods of hacking/breaching of confidential information), on part of the common man who uses these websites may also be included under the ambit of the DOS attack. A type of denial of service attack is distributed denial of service attack, where the hackers geographically target various consumers at the same time. A denial of service attack can be initiated against big E-Commerce companies, financial institutions such as banks, educational institutes when it comes to annual admissions of students and even government organisations are also not immune from this type of hacking[32]. Awareness towards this type of hacking, using tools such as Google extensions in order to stop pop-ups being raised by the website are some of the ways to control denial of service attacks.

[31] *Encyclopaedia Of Information Technology*. Atlantic Publishers & Distributors. 2007. p. 397. ISBN 978-81-269-0752-6.

[32] Source: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Phishing

The system is the most common method used in India for Cybercrimes. This is a cyber-dependent crime that involves human intervention at its core. What happens under phishing is that a person who is a hacker primarily connects with the victim who comes usually from impoverished condition; thereby the hacker tries to manipulate the victim who is already vulnerable. In poor countries such as India and Sub-Saharan Africa, the hackers contact the victim by stating that they have won a certain amount of money in the lottery and thereby they seek confidential banking information such as account number and address of the victim in lieu that after sharing that the amount they would be transfer the lottery amount to the victim's bank account. They take advantage of the vulnerable condition of the individual, his lack of literacy and awareness of cyberspace and thereby executing such a crime. Another type of phishing crime is when hackers contact people on the telephone claiming to be bank employees and stating that a certain amount of money has been debited from the victim account thereby in a state of confidence to the person who has been calling and share confidential information in order to blocked accounts. Little they know that the information that they are sharing with the hacker would be one of the reasons that the accounts would be breached. Phishing as a crime can be controlled by awareness and cyberspace literacy.[33] There are countless advertisements made on behalf of the government and statutory organisations such as the Reserve Bank of India which highlight the various methods incorporated by the hackers in order to commit such crimes. These advertisements are broadcasted on radio and television for public awareness. It is crucial for those people who are aware and literate in cyberspace to inform and educate those who are not[34].

Email Bombing

As the name suggests, email bombing is a type of cyber intrusion where the abuser or the hacker sends multiple emails by different email ids to the victim's inbox. The main purpose of email bombing is to spam the inbox of the victim and to make the victim flummoxed and ultimately result in the crashing of the email website. Emails that are

[33] Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (eds.). *Handbook of Information and Communication Security*. Springer. ISBN 978-3-642-04117-4.
[34] https://www.forcepoint.com/cyber-edu/phishing-attack

sent in form of spam are usually from different email ids. Most of the emails are meaningless that can be of the same language as the mother tongue of the victim or incorporate any foreign language, most likely of the country from which the cyber abuser or the hacker resides. Email bombing is an older method of Cyber intrusion as the internet became popular in the last decade of the 20th century it was very common for people to have email ids. There have been occasions when the cyber bombing is of a nature of a more traditional crime thereby cost/ransom is asked byh the cyber abuser rather than crashing the parent website where the victim had the email account. Therefore, there have been occasions when emails have illustrated people for money from them, therefore, blackmailing them, if they do not give the money they would hack the computer systems and get private information which may include confidential details. In such a way more damage would be caused to the person in particular than given the ransom to the cyber abuser.[35]

Unsolicited bulk emails are the trademark of such type of crime. Email bombing is difficult to trace because the IP address which means the internet protocol address of the person who sends numerous emails keeps-on changing. Therefore, it is extremely difficult to trace the parent computer from which the attack was initiated. As mentioned above the attacks are usually made in different languages. The emails may consist links which upon opening or clicking may seize the activity of the computer and provide essential confidential information to the cyber abuser/hacker. Therefore such an attack is executed using multiple email accounts and uses multifarious methodologies in order to compromise the victim's computer. Therefore the email spamming can be complemented by Malware which when included in the email as an attachment or as a link (which upon opening or downloading may inflict denial of service attack or breaching of confidential information).[36]

Sending bulk emails as spam violates international norms of cybersecurity and is even against the domestic rules of internet service providers. Spammers are basically people who send bulk emails to the victims account in order to slow down the system on which

[35] Brenoff, Ann (2013-11-01). "Why Every Parent Needs To Know About Text Bombs". *Huffington Post*. Retrieved 2017-12-30.
[36] Silverbug. "10 Types Of Cyber Crimes... And Another 10 You've Never Heard Of". *www.silverbug.it*. Retrieved 2019-04-25.

they are working. That is the primary reason for email hacking, the other reason is a complicated reason in which the spam email is coupled with malicious software or a malicious code which upon downloading or clicking causes for the problems for the victim. Offences committed under email spamming are very difficult to be traced. Usually, the email spammers get the email address of the victim from open data sources. Open data sources are places where the victim had by his own volition updated his email ID, for example, in restaurants during reservations there is a form which is to be filled out by the person who is about to reserve a table, there are many internet websites which require email ID for the subscription of the newsletter, thereby the email ID is available on the open web. There are many websites which upon subscription tell that they are about to use the email id and will share others the information as well. It is quite common that the victim agrees to such a condition and then subject himself to email spamming attacks. Therefore due diligence before sharing the email ID either online or offline and cyber literacy are key factors to avoid email bombing[37].

Web Jacking

The crime of web jacking is extremely similar to the crime of hijacking. Now hijacking is a process in which the position of the vehicle or the aircraft is taken from the authorities responsible for the transit into the hands of the perpetrators. The processes of the transit, as a way to blackmail individuals, including coercing governments for certain undue favours or ransom collection are aspects of web jacking. Drawing a similar context in cyberspace, the unauthorised takeover by the cyber abuser/ hacker over a website in order to cause injury to the victim by posing the hijacked website as legitimate, thereby when the victim conducts its usual course of business with the website, he/she is basically transacting with the hacker[38]. The transition of possession and control of the website is so smooth and seamless that there are times when the owner of the website himself is not aware of the web jacking. There have been instances when the hacker has used this method to collect ransom, collect money as

[37] Source:https://www.techopedia.com/definition/1655/email-bomb
[38] Web Jacking, Cyber Crime Chambers, https://www.cybercrimechambers.com/blog-web-jacking-117.php

transactional fees, and there is no pecuniary interest; the hacker has even uploaded obscene videos and photographs of the victim online.

It is to be noted that a person who has gone on the website has no prior knowledge that the website has been changed or modified to that extent that now the version that the hacker is using is like the carbon-copy of the previous website. There is little to no victim participation during the execution of web jacking. The hacker has an advanced sophisticated knowledge about cyberspace and usually works secluded or in a team of hackers.[39]

Web jacking has to be differentiated from the traditional methods of hacking in which a link is shared and upon clicking the link the virus inflicts the computer. Here instead of a particular code being launched inside the victim's computer the whole website which is the medium that the victim is browsing itself is counterfeit. This requires elaborate planning and coding of the software so that the user who is well accustomed to the website, who uses the website every day, cannot even understand the difference. The difference can be extremely subtle, for example, google.com is the traditional and most sought after search engine but if it was under web jack attack the hackers would have a subtle change in the domain name of the website such as go0gle.com, and this would not come across as an anomaly for the victim who is the user of this website. The Subtle change of an alphabet resembling the letter O is the difference. Thereafter if the user is accessing and paying something, the money would directly go to the hackers rather than to the service provider[40].

There can be other types of cases involving web jacking where the domain name is taken by the hacker and the hacker applies for benefit under some scheme from the government or institution such as universities. Similar to email bombing it is extremely difficult to trace as the internet protocol address of the hacker keeps on changing. The sophistication required in conducting web jacking is extremely nuanced in nature. It is very difficult to protect yourself from web jacking. What can be the best advice is to go on a website that is highly secured for transactions and to share personal information on the website extremely sparingly. It was said that big websites for E-commerce

[39] Source:https://lawsisto.com/legalnewsread/NjQyNg==/DETAILED-OVERVIEW-WEB-JACKING
[40] *Ibid.*

companies are less likely to become counterfeit overnight and they have a highly secured network monitored by Information and Technology specialists. These specialists report and act against such breaching at the very instance.

Cyberstalking

Cyberstalking is similar to the stocking which is defined in the Indian penal code 1860 under Section 354 D where stalking means following a woman without her permission or consent in order to contact her, talk to her, or harass her. It is to be noted that the punishment for stalking in the traditional sense is a sentence for three years alongside a fine. This sentence is for the first time offenders, whereas for the second time offender the sentence is increased from a maximum term of three years to a maximum term of 5 years alongside a fine as deemed fit by the court. Cyberstalking is similar to the stalking defined under section 354 D of the Indian Penal Code. Here the stocking is conducted by the abuser in the virtual world through various applications and social media. With the rise of internet penetration in India, majority of Indians access the internet at extremely cheap rates, thereby they are also using social media but there is a catch-22 situation as the majority of users are not cyber literate and they lack the basic necessary etiquettes of cyberspace. Thereby they make themselves vulnerable by sharing information (data/pictures/videos) which was not supposed to be shared online in the first place.[41]

What begins as silent harmless stalking eventually becomes a toxic activity as the abuser starts to intimidate the victim. Here in this crime the technical acumen is not required on part of the abuser, in most of the cases there isn't any breach or intrusion in the personal computer of the victim and much to the traditional meaning of this offence, normal day today's stalking behaviour by men lead on to cyberstalking in the virtual online world as well. What this means is that if a girl is stopped by an individual or group of individuals living in a locality, it is quite likely that the same individuals are going to stalk the girl online in the virtual world as well. Criminal intimidation by threatening the girl for dire consequences if she requests a response in a constructive

[41] Smith, Kevin (2 September 2016). "Tougher California laws protect victims of digital harassment". San Gabriel Valley Tribune. Retrieved 3 July 2017

manner to their lewd comments is quite common in India[42]. The internet growth in India has caused another problem that was less prevalent in this country. Children who are not supposed to be on social media and should be given restricted access to cyberspace are using the same without any parental guidance or restrictions. While the parents cannot be totally blamed for this as they themselves are using the internet for the first time and they are not aware of the various nuances of cyberspace themselves, thereby they are exposed to cybercrime. The children are unfortunately exposed to even greater abuse. The abuse that I am elucidating is the crime of paedophilia on the internet. Children who are not supposed to be accessing various websites which are not secured, thereby expose themselves to paedophiles whom they would not have been in contact with had they been living in the natural environment without the internet and in presence of their parental guidance and supervision. Cyberstalkers take advantage of emotionally manipulating the victim and also his or her lack of knowledge of cyberspace by which they do not know how they can protect themselves from such stalkers[43].

Cyberstalking has now penetrated into every realms of cyberspace which includes social media, emails, blogs, general Google reviews, articles published online etc. It is extremely easy to trace a person these days with the internet around, for example, if a person uses social media such as facebook.com and due to his or her lack of awareness enables Facebook to know the location of an individual, thereby, if the individual has gone to someplace to have lunch, Facebook would show that this person is having his lunch at a certain restaurant and this piece of information would be shared without the permission of the social media account holder because he or she had already provided the permission while creating the account. Now the cyberstalker who was talking to the individual virtually knows the exact location of the individual, thereby, he can go to that place and intermediate or stalk the individual physically. In a globalised world, companies are being set-up and stalking takes place in a professional setting as well. Where if a person's computer isn't working and someone from the IT Department is

[42] Bocij, Paul (2004). *Cyberstalking: Harassment in the Internet Age and how to Protect Your Family*. Greenwood Publishing Group. pp. 12–13. ISBN 978-0-275-98118-1.
[43] Source:https://www.thebetterindia.com/45671/stalking-india-women-complaint-online/

called up to check the computer and thereby the malicious IT professional garners confidential information such as email id, birth dates, residential address, in order to conduct the offence of stalking.

Society and parental guidance and their significance in human life invariably define the life choices of an individual. With the prevalence of open relationships in urban India and the popularity of dating apps at an all-time high especially due to the pandemic covid-19 which has disabled normal practices of life, such as going to social places to hang out, people a cooped-up in their homes, and without physical contact the urge to meet new people in order to fulfil the socializing needs are quire common. People download such apps where they can make friendship online; that is virtual. But there is a problem with this type of social behaviour as the individual whom they are meeting online tends to stock them later when they share the social media handles. These types of relationships are shallow in nature and are devoid of human emotions. A person who is vulnerable and who desperately needs company, someone whom he or she can take confidence in and share a part of their life with are taken advantage of by the cold-hearted cyberstalkers. There are multiple forms of cyberstalking but for the purpose of this dissertation thesis cyberstalking can be broadly divided into two categories as following:-

Stalking over Internet

Stalking over the internet includes harassing the individual through emails or social media platforms. As mentioned above, the victim tends to share his or her details such as email id and other contact information without doing due diligence on social platforms. The technical aspect of the stalking isn't of great value and this can be broadly categorised as a cyber-enabled crime, where the individual is the main essential ingredient of the crime. However, if the stalker has a good amount of Information and Technology knowledge then he can also send a malicious software or malicious link via these social media platforms or even email and then it would be a combination of multiple types of Cybercrimes[44].

[44] Source:https://www.kaspersky.co.in/resource-center/threats/how-to-avoid-cyberstalking

Stalking by Hacking the Computer

Stalking by hacking the computer is slightly different from stocking over the internet while in both instances the medium of talking is the internet, here the place of the crime is committed is the software which runs the computer and not the application in particular used by the victim. In the aforementioned type of stocking the crime was committed on a platform that was used over the internet such as any social media website. Contrary to this stalking this nuanced method involves hacking the computer. When the hacker craps the operating system of the computer of the victim and in that process the hacker can access the webcam of the computer and the microphone of the computer which is inbuilt, thereby whenever the victim is sitting before the computer the hacker can see and hear him or her. This type of stalking is more serious in nature because it requires a high level of knowledge to execute. In the previous type of cyberstalking the crime is committed whenever the victim uses third party platforms and actively engages in conversation with strangers whereas this type of cyberstalking is conducted entirely under stealth which makes the victim highly vulnerable and compromised, as his or her privacy and security is breached by the hacker[45].

There is no one way to protect oneself from cyberstalking as the crime of cyberstalking originates from its predecessor in the traditional world. Apart from the usual checkpoints to protect oneself from cyber abuses such as awareness and due diligence before sharing vital confidential private information; the most pertinent aspects to control cyberstalking is parental guidance and constructive set-up of the society which discourages the practice of stalking[46].

Data Diddling

Data diddling is a type of cybercrime where information in the form of data (which can include numbers or any other vital information) is manipulated or altered by a person who is not authorised to do the same. The whole world today is driven by data and data is one of the most important commodities to conduct a successful business. To give an example of data diddling, when after the end of business transaction in the course of the

[45] Citron, Danielle Keats (October 2009). "Law's Expressive Value in Combating Cyber Gender Harassment". *Michigan Law Review*. 108: 373. SSRN 1352442

[46] Source:https://www.thebetterindia.com/45671/stalking-india-women-complaint-online/

day in a supermarket, the cashier records the transactions and prepares a balance-sheet which is to be submitted to the supervisor in order to maintain a roster which states the items which have been sold and items which are on the shelves. During this process, if the employee intentionally or unintentionally bundles certain numbers which illustrates us the amount of spending conducted by the supermarket then the erroneous blunder would amount to data diddling.[47] In order to commit the offence of data-diddling, the person/abuser need not be a hacker or technically trained in information and technology or any other technical branch of computer science. It is often seen that the offence of data diddling is committed by an insider who is either a former employee or a disgruntled current employee. The offence of data diddling is pretty basic in nature. Another popular and relevant example is where certain digits are misplaced and cause a huge amount of ruckus in social media. The incident in reference is when Reliance Electric Company provided electricity bills in the cities of Mumbai and Pune bearing egregious errors. The incident happened in 2020 when customers who brought service of electricity from the private company Reliance received bills in huge numbers pertaining to the amount to be paid by them in lieu of the electricity used/consumed by them. It was later found out that the customers did not consume the number of units of electricity claimed by Reliance electric company; thereby the company had to revise the bills. The data which in the aforementioned case was unit(s) of electricity consumed by the customers was erroneously altered by someone/cyber abuser. It could not be openly exposed as to who is responsible for such data diddling but the company received the flag on social media regarding the brazen attempt of taking advantage of their customers[48].

Identity Theft and Credit Card Fraud

Identity theft and credit card frauds are the most common methods of defrauding victims in India. In this type of offence, there is no participation of the victim in order of completion of the offence. Identity theft has been penalised in Indian statutes as well, for example, Section 66C of The information Technology Act, which states that if

[47] Parker, Donn B. (1989). *Computer Crime: Criminal Justice Resource Manual* (PDF) (2nd ed.). National Institute of Justice. pp. 12–13

[48] Source: https://fraudfighting.org/data-diddling/

an individual or a group of individuals, knowingly and dishonestly use the digital signature, or any other private and confidential platforms which can include emails, for an attempt to harm the individual then that would amount as identity theft which is punishable with the term exceeding maximum to 3 years alongside a fine which is decided by the discretion of the court. Credit card frauds are very common in India and there are multiple methods of getting the vital information of the credit card which enables the abuser to use the card in order to harm the victim.[49] The advanced methods of credit card fraud include card cloning technology whereby when the card is given to the service-provider in order to be swiped in the POS machine, the service provider takes the card and places it on the magnetic scanner which scans the metallic strip behind the card which is later printed through the 3D printer and then used via dummy cards.[50]

Another method of getting vital information from the credit card which does not involve a technical method to harness the information is the plain and simple call centre fraud technique[51]. Here the hacker or the cyber abuser contacts customers using credit cards and then they tell them that their card has been violated and some other place there is someone else who is trying to make a payment from the card and the bank employee is calling on behalf of the bank to verify the purchase. The card owner retaliates by saying that no such payment has been made and the card in question is in his possession. Baffled by this thought that there is someone who is having his card and using it for fraudulent purchase, the card owner requests the alleged bank employee on the telephone to block their card immediately. By this time the alleged bank employee who is fraudulently taking information has worked his charm on the credit card owner and the credit card owner takes confidence in the individual and shares his credit card number, its expiry date, and the most important CVV number which is written behind the card. In view of getting his credit card block the individual falls into the trap and what follows is predictable. The difference between quick payment from the card and when the owner of the card comes to know about the payment it is too

[49] Source: https://www.cnbc.com/select/credit-card-fraud/
[50] Olmos, David (6 July 2009). "Social Security Numbers Can Be Guessed From Data, Study Finds". Bloomberg. Archived from the original on 17 June 2013. Retrieved 4 January 2011
[51] Source: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/credit-card-fraud

late. Reserve Bank of India and many other popular banks in India always broadcast commercials stating that no bank employee on the telephone would ask for confidential and private information regarding the customer, his bank account or even credit cards. Despite that many educated and urban Indians fall under this trap. It is to be noted that credit card fraud is a type of fraud that is committed in category B and category A cities in India. This means that it is a crime that is committed against people who are literate and aware. But the rising number of credit card frauds indicates that somewhere down the line people come under pressure and provide vital information to the cyber abuser[52].

In order to secure ourselves from credit card fraud it is invariable to ask the bank for additional security features in the card such as the requirement of PIN or OTP in order to complete the transaction which requires the internet as the medium to conduct the transaction. The one-time password should come on the registered mobile number updated on behalf of the customer by the bank. The bank should make the employee aware at the time of issuing the credit card regarding the dos and don'ts of its usage. It is extremely important not to share the one time password with any stranger as it may lead to identity theft. In addition to that our smartphones have become our bank today therefore in any case where the victim loses his mobile phone it is imperative on his behalf to not only file an FIR in the police station for the stolen mobile but to go to the telecom service provider and block the SIM card and after that the story is still incomplete. He has to then go to his bank and request the manager to block the card which was linked with the mobile phone number.[53] This three-tier security and safety activity would ensure that the victim is not taken advantage of beyond the damage of the stolen mobile phone. It is to be noted that there are cards nowadays which do not require a One Time Password in order to process a payment that is of a lower denomination. Therefore, it makes it very difficult for the person who is the owner of the card to monitor the expenses incurred from the same. There have been cases where the vital information from the credit card is stolen and subsequently, a clone of the same

[52] Hoffman, Sandra K (2009). *Identity Theft : A Reference Handbook*. Santa Barbara, US: ABC-CLIO. pp. 42–44. ISBN 9781598841442

[53] Source: https://www.bajajfinserv.in/credit-card-fraud-in-india

card is made and then small payments are made by that card. As is the case with credit cards it takes roughly around 60 days in order to generate the bill and when the bill is presented to the owner of the credit card it is too late to track the payments. Since the bungling was made with small denominations it is extremely difficult to trace the cyber abuser[54].

Identity theft and credit card fraud apparently common in locations where there is a lot of tourism. When people hang out with their families they are in a different mindset whereby they are not conscious and let the guard down and the cyber abuses take advantage of this. A pretty common example is in hotel check-ins, when the customer walks in he shares his identity card for the purpose of the reservation and when during checkout he pays with his credit card, the information of his identity and the card number is shared to the reservation desk officer. Now if the reservation desk officer is a cyber abuser he can use the vital information and pose as the customer and use his card for payments and when the real owner of the credit card comes to know about the fraud it is often too late[55].

Salami Slicing Attack

A salami-slicing attack is an extremely nuanced method of defrauding an individual or group of individuals including institutions and societies. This type of cybercrime gets its name from a type of chicken cut made by the butcher which is called chicken Salami. This type of cut is known for a thin slice of chicken which is cut and usually served with different assortments which usually is a part recipe of a traditional sandwich. In the crime of Salami slicing attack, a small amount of money which is negligible in payment calculation is deducted from the victim's transaction account and transferred to an escrow account. It is to be noted that usually the small amount which is left is not transferred to the vendors' account but to the account of the cyber abuser. Salami slicing attack in simple words means the embezzlement of a small amount of money from the transaction between a vendor and a customer, where the bill is said to be round off but the difference in the amount of the round-off and the total expenditure

[54] Arata, Michael J. (2010). *For Dummies : Identity Theft For Dummies (1)*. Hoboken, US: For Dummies. pp. 43–45. ISBN 9780470622735

[55] Source: https://www.bankbazaar.com/credit-card/credit-card-fraudulent-transactions-in-india.html

of the bill does not go to the accounts of the vendor, rather it is directed to the account of the cyber abuser. It is extremely difficult to trace the Salami slicing attack as the embezzlement is of extremely low denominations. But these low denominations accrue over a long period of time and thereby constitute as a big number. Salami slicing attacks are conducted on a large scale therefore the amount embezzled by the cyber abuser is a significant number. This requires a technical person in order to conduct the crime; this person must have prior knowledge of Information and Technology and have the aid of a disgruntled employee working hand in hand with him in order to execute the Salami slicing attack. Therefore it is convenient to say that without any insider support and help it is extremely difficult to organise such mass-scale operation[56].

Salami slicing attack is popular laundering of money offence where it is executed in small amounts but it is not restricted to money only. There have been occasions when such attacks have also been used to breach information in small quantities over a long period of time. This information is confidential in nature and usually, such attacks are organised to access information and targeted against people who are in power, that is, they are in the government or run big companies or corporations. This information which is data in essence is collected from the website activities that he visits in his day to day life.[57]

Software Piracy and Cloning

Software piracy is extremely common in India because essentially software is developed in western countries and channelled by one or two market leaders in computer technology. That is either Windows or Apple computers. Therefore the software which has a tie-up with the aforementioned brands are provided free of cost but updating them or getting an alternate software cost a great amount of money. It is extremely difficult to procure software in remote areas or third world countries. In the wake of capitalism every company tries to make the most profit and in this business model what happens is that major computer making companies such as Hewlett Packard tie-up with windows and this causes the user to update the software in order to use the

[56] Voeten, Erik (3 December 2013). "'Salami tactics' in the East China Sea". *Washington Post*. ISSN 0190-8286. Retrieved 2020-11-23.

[57] Farley, Robert (26 December 2014). "A Holiday Primer on Salami Slicing". *thediplomat.com*. Retrieved 2020-11-23.

computer. This update comes with a big price. The consumer has no option but to update otherwise he will not be able to access the computer on a day to day basis. It is extremely difficult to develop software as it takes years of hard work by many engineers in order to develop software.[58] Therefore to use a pirated version of the same is morally and ethically wrong. People coming from impoverished backgrounds install software which is licensed by the manufacturing company on their personal computers, in this way they do not have to pay for a licensed copy of the same but they expose their system to many viruses and cyber-attacks through trojans. Installing a crack version of software breaches the safety standards of cyberspace and it also compromises the performance of the personal computer.

The section following would elucidate the various ways in which software piracy is conducted:-

1. Downloading software from illegal torrents through the internet
2. Installing a software that was supposed to be used on a single personal computer but rather than using it on one particular computer it is installed in multiple computers by tweaking the startup coding of the software
3. Applying a key generator to circumvent copy protection
4. Broadcasting software which was bought by a person for his personal use but later made available on the Internet to be downloaded and used by the general public

Software piracy is conducted by the method of cloning. By cloning what happens is that a replication of the codes which were incorporated to make the software are copied and the code which is required to start the software is removed from the pirated version. Therefore the pirated version can be opened on multiple computers by the same supply source. Software piracy not only dents the computer market but it also discourages ethical business practices. It harms the software developer and also does not ensure proper service for protection to the person who has downloaded or installed

[58] Cloning: The Rising Cases of Cyber Crimes in India, Hindustan Times, https://www.hindustantimes.com/business-news/cloned-the-rising-cases-of-cyber-crimes-in-india/story-yR8Emqv3SuzaGoCsYvpBJK.html

the crack version of the software.[59] There are multiple markets behind the high streets in popular cities when the crack version of the software is sold openly. It is imperative for the law enforcement agencies to crack down on these black markets in order to ensure that ethical business practices are restored and the software developers are not taken advantage of. It is to be noted that while the burden of controlling the offence lies on the criminal justice administration agencies, it is also imperative for the software developers and computer manufacturers who work closely with them to manufacture software that is pocket friendly and easy to use for developing countries. The crime of software piracy is promulgated by the pricing and user policies of the software developers themselves. Therefore they cannot walk away from the onus of their impartial involvement in the creation of this problem which has now taken the face of crime. Instead of cracking this disparity and lack of understanding of the markets especially in developing countries, the software developers have now evolved their security systems whereby they have included fingerprints which counter-proofs the hackers trying to make a crack version of their software[60].

It is an extremely sensitive offence as on the face of it seems to be an offence in which people convert proprietary software into crack version software which can be sold at a cheaper price and can be used by multiple people on multiple personal computer systems but in essence, this crime is extremely sensitive in nature as it is predominant developing countries where people are trying their best to use the internet as a constructive element in their life in order to away from crimes and try to make the best for their families.[61] In such a socio-economic setup it is extremely important not to add additional stress on individuals or families whereby they are forced to use illegal methods in order to make their ends meet. In such a scenario it is extremely difficult to point fingers at an individual who has committed the offence of piracy as the individual in question has been forced to take such a decision as he is a part of the general public and to whom he caters afford the proprietary software in the first position.

[59] Source: https://www.computerhope.com/jargon/s/softpira.htm
[60] Source: https://hypertecdirect.com/knowledge-base/software-piracy-facts/
[61] Source: https://www.geeksforgeeks.org/understanding-software-piracy/

Chapter 3: Jurisdiction of Cyber Crimes

United Nations Convention on Transnational Organized Crimes (UNTOC) and Jurisdiction of Cybercrimes

It is to be noted that the crimes which are committed against a country or through a strategic plan with the ulterior motive to harm the image of the country by virtue of targeting the common folk living in the country, these types of crimes are often conducted by crime syndicates. The offences indicate sophisticated organisations of criminals which are run by the work ethics of a busy successful corporation. The crime syndicate can be located in one country and that particular country can be denoted as the headquarters of the syndicate. There can also be a group of countries that act in tandem in order to conduct criminal activities especially using cyberspace[62].

In order to curb these multinational levels of organised crimes United Nations General Assembly resolution in the year 2000, created an organisation dedicated towards transnational organised crimes. This organisation was created by the United Nations Convention on transnational organised crimes (hereinafter referred as UNTOC). It is the only organisation specially dedicated to controlling organised crimes which are planned and executed involving more than one country. It is to be noted that there isn't any provision under UNTOC which defines the space of Cybercrimes or even mentions the word cyber jurisprudence in the international statute. Where the aforementioned organisation becomes critical in order to control the cybercrime-related abuses is that it provides a labyrinth of liberal interpretation of its statutes which defines the environment in which a crime is committed and can be related to the cyberspace[63].

Modern-day cybercrimes involve an intricate setup that can be compared with a set up of a multinational company. It is to be noted that today cybercrime is a one man's job but when it is targeted surgically to a population of millions it has to be executed with the precision of a surgical operation. Today fraud and identity theft is conducted at the

[62] Katitza Rodriquez, The cybercrime convention's new protocol needs to uphold human rights, Electronic Frontier Foundation, 18 September 2017, https://www.eff.org/deeplinks/2017/09/cybercrime-conventions-new-protocol-needs-uphold-human-rights

[63] Tim Maurer, When states pretend to be terrorists or hacktivists in cyberspace, 18 April 2017, https://carnegieendowment.org/2017/04/18/whenstates-pretend-to-be-terrorists-or-hacktivists-in-cyberspace-pub-68703

mass scale and major terrorist organisations such as Al-Qaeda or ISIS have also exhibited terrorist activities using cyberspace.

Section 3[64] of the United Nations Convention on transnational organised crimes elucidates the meaning and nature of the word transnational. It states the following:-

1. A crime that is committed in more than one state is referred to as transnational
2. A crime that is planned in one state but the preparation and execution of the same is conducted in a different state
3. A crime that is planned and executed in one state but the execution involves the involvement of certain elements which may include human resources or technological assets which are hired or engage from a different state
4. A crime is committed in one particular state but the repetition of the crime is found in multiple States when direct execution was not conducted.

It is to be noted that the jurisprudence of cybercrime is extremely difficult to pinpoint as the crime is dynamic in nature involving multiple parties, and is conducted through a virtual interface. Therefore, while the essence of cybercrime is the breach of a persons' personal computer system in order to access information which in simple terms can be termed as theft, and can be traditionally defined under criminal law but the problem lies with the interface where the crime is conducted. Since the interface of the crime is a virtual space that cannot be seen, it makes it extremely challenging for criminal justice administration systems (which are itself lacking in information and technology-related infrastructure) to cope up with the rise in the number of cases pertaining to Cyberspace.

The nature of cybercrime is such that a person can commit a crime from a different country and the victim can be from a different country, thereby making the detection, arrest and subsequent fair trial and prosecution extremely difficult and time-consuming. Since it is fair to say that cybercrime in the 21st century involves a structured pattern resembling an operational activity, which involves parties from different states exhibiting organised criminal activities, the United Nations Commission on transnational organised crimes used one of the most traditional

[64] Source: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

principles of criminal law in order to define the jurisprudence of the cyberspace. Under Section 15 of the United Nations convention of transnational organised crimes, it is clearly mentioned regarding the applicable jurisdiction over offences that are covered under the same statute by the states that have signed and ratified this convention.[65]

The said Section 15 of the United Nations convention of transnational organised crimes states that the active jurisdiction is that where the offence has been committed. It basically reiterates the **territorial principle of jurisdiction**, which is a common concept of criminal law across the world. The principle basically states that in a crime that includes cyberspace also which is conducted in multiple countries, all the local jurisdictions of the countries in which the damage has been incurred shall be applicable in the trial and proceedings of the same. There are instances when cybercrime is committed in spaces where territorial or natural sovereignty does not apply[66]. Territorial or natural sovereignty means the crime has been committed in a place that is beyond the geographical limits of the country, for example, cybercrime has been committed on an aircraft or a ship cruiser. In such instances where the crime has been committed in a place that is beyond the geographical sovereign limits of the country, the standard principle states that the jurisdiction will lie with the country of registration of the aircraft carrier or the ship cruiser. Therefore it means that wherever the aircraft carrier, ship has been registered, the country which owns the same has the jurisdiction to hear and trial the crimes committed on the same.

The aforementioned provisions of territorial jurisdiction apply to only those parties who have signed and ratified the international convention. Here the international convention does not discriminate between the parties. The word parties include both the victim country where the cybercrime has been executed and the country which is accused to have been conducting the cybercrime as well. This theory of including both parties is in consonance with the **active personality principle in international law**. It is to be noted that if the incidence where the crime has been committed is different the principle still applies to the victim's basic nationality. For example, if a person who is a resident

[65] Source: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

[66] UNODC, Global Programme on Cybercrime, http://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

of India has gone for a business trip to Hong Kong, where a surgical cyber attack has been committed against him and based on the *prima facie* evidence available it can be said that the said cyber attack was organised from the country of North Korea. The jurisdiction, in this case, shall apply to the country of India and not Hong Kong where the offence was committed. The victims' nationality supersedes the place where the crime has been committed. The United Nations convention of transnational organised crimes also extends its relief to people who are refugees, or stateless individuals seeking asylum. In this case what happens is that if cybercrime is committed against a person who is stateless, thereby he has no proof of nationality but he resides in a state who is the signatory of this convention, the jurisdiction which would apply in the trial proceedings of the cybercrime shall be of the state in which the person is living at the moment as a refugee or as an asylum seeker[67]. For example, the American national Edward Snowden who is wanted for a criminal trial in the USA has fled from the same country and currently is staying in Russia as an asylum seeker. Therefore if an offence is committed against Edward Snowden the jurisdiction which would apply shall be of the country of Russia. This principle is borrowed from the **passive personality theory in international law**.

The international convention also provides safety measures in which offences are committed involving cyberspace during the performance or execution of contractual liability. This is extremely crucial as it safeguards the international commerce being conducted between countries. Therefore under this if a company is registered in India and is supplying certain proprietary software to Singapore but before the Indian company could fulfil its contractual liability and there was a breach in the security systems and thereby the software was ultimately pirated and could not be used by another party in Singapore. Based on the preliminary investigation it was ascertained the crime was conducted by hackers based in Russia. The jurisdiction which would apply in order for the investigation trial and proceedings of the same shall belong to the country of Singapore. The international convention elucidates between article 15 and article 16: defines the different setup in which claims can be ascertained as per the

[67] Source: https://globalinitiative.net/initiatives/untoc/

jurisdiction where the crime was committed. It is to be noted that the geographical location where the crime has been committed shall lie within the territorial limits of the Sovereignty of the state which has signed and ratified the aforementioned international convention – in order for its domestic jurisdiction to apply[68].

It is to be noted that the international convention provides provision for extradition of the culprit residing in the signatories' country. An attempt has been made to avoid multiplicity of suits in lieu of multiplicity of jurisdictions. A case-by-case approach is adopted in order to avoid the same. Another International Convention provision makes it mandatory that the person who is accused of the offence has to be extradited at the request of the country where the victim resides. This request has to be obliged by the other country who is signatory to the international convention[69].

Council of Europe and Jurisdiction of Cyber Crimes

The Council of Europe signed a multilateral Treaty in the year 2001 which came to effect in 2004, which exclusively focused on the offences committed over cyberspace. This multilateral Treaty was signed by 29 countries including the United States of America. The cybercrime convention was conducted in the city of Budapest which is in the country Hungary[70].

This particular multinational cybercrime convention is extremely important and contemporary in nature because this was the first attempt by a group of developed countries to figure out a common criminal set-up which includes policies and statutes by virtue of finding coherence between domestic national laws with the ultimate motive of creating a secured and safe cyberspace. This particular international convention is the first-ever convention that deals with frauds committed by hackers, child trafficking and

[68] Source: https://globalinitiative.net/analysis/untoc-review-civil-society/

[69]Source: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en

[70] Council of Europe, Towards a protocol to the Budapest Convention, 19 March 2018, https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713; for a list of observers, see Parties/observers to the Budapest Convention and observer organisations to the T-CY, https://www.coe.int/en/web/cybercrime/parties-observers

the introduction of child pornography, cyber thefts including infringement of intellectual property rights[71].

The hackers who commit cybercrimes often feel invisible as it is extremely difficult to detect them and in cases whereby preliminary investigation detection is possible, it becomes arduous to prosecute them as the difference of loss between the two countries makes it extremely difficult for the judicial system to work efficiently. Parties that have signed and ratified the international convention have made necessary changes to develop domestic national laws for crimes related to cyberspace. In general terms, the most popular cybercrimes have been divided into four categories which include IPR infringement, frauds and other hacking activities conducted online, human and child trafficking and security infringements in important government or corporate offices[72].

This International Convention has also created a positive responsibility on the signatory members to legislate laws for trial, investigation, and international cooperation between member countries for quick and efficient execution of Justice regarding crimes committed in cyberspace.

International cooperation between States is an essential aspect in criminal justice administration related to cybercrimes. As mentioned above cybercrimes are offences that are committed against nationalities involving one or more States, therefore for international cooperation in the investigation, which encompasses the collection of evidence, interrogation of culprits/accused, trial and extradition of criminals: lay as paramount importance to the signatory countries of this international treaty[73]. This sentiment has been reciprocated in the international convention as well as articles 27 to 35 of the aforementioned convention lay down the process of mutual cooperation between States for the criminal justice administration of offences related to cybercrime. Article 35 of the International Commission states that the countries which are involved in the process of investigation shall remain in touch throughout the process of investigation, that is 24 into 7 connection for the joint collection of technical

[71]Source: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[72] Source: https://www.coe.int/en/web/conventions/full-list

[73] Source: http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf

data, which may include evidence derived either virtually through the internet or are collected through traditional methods of investigation involving interrogation, search and seizure as standard practices.[74]

Article 22 of the convention related to cybercrime elucidate a search regarding the jurisdiction which governs the signatory parties to the international convention to conduct investigation and trial. Article 22 states that the jurisdiction for where the offence is committed, whereby the territory in which the offence is committed *de facto* becomes the jurisdiction for the trial in the situation of the same. Article 22 of the international convention reiterates the principle of territorialism, in which it states that the jurisdiction which applies is where the crime has been committed. Occasionally where the crime has been committed does not belong to any territory or sovereignty, such as the open high seas, on the space; In those cases the vessel or aircraft in which the offence has been committed is seized and it is figured out that where the aircraft or the vessel carrier has been registered. That particular country shall apply its jurisdiction to investigate the crime.

There are certain cases in which the signatory member countries conduct the preliminary investigation and an accused is pinpointed by the states and parties involved but there isn't an extradition treaty between the States. In this case when the accused resides in one particular country and the other country where the injury or damage has been caused (and there isn't a extradition treaty between the concerned States), in that case, it is said that the country where the accused is residing shall proceed with the investigation and trial of the accused as if the accused had committed the offence in the very sovereign he is residing[75]. The commission in various provisions repeatedly reiterates the **importance of interdependence** and mutual cooperation in the investigation of crimes related to cyberspace. It is extremely important to mention Article 24 of the international treaty which states that when one of the states/parties involved in the cybercrime isn't a signatory member of the international treaty then in that case each matter shall be discussed with the state who is the non-signatory member

[74] Source: http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf

[75] Joyce Hakman, Building a stronger international legal framework on cybercrime, Chatham House, 6 June 2017, https://www.chathamhouse.org/ expert/comment/building-stronger-international-legal-framework-cybercrime.

separately as the international Treaty recognises and acknowledges the principles of extradition of state parties and the limitation of the state to conduct extradition of the accused on reasonable grounds. This topic is extremely important as the crime involving cyberspace is often a multi-jurisdictional setup with more than one country involved, therefore a lucid and developed criminal justice administration is necessary for the expeditious execution of the trials in proceedings arising from the offences committed using cyberspace[76].

In consonance with the international treaty, the group of most powerful 8 countries of the world which are known as the G8 countries have come up with a possible permanent measure to control internet hacking and breach of cyberspace. The group of the eight countries comprises the following, France, Germany, Italy, Japan, the United Kingdom, United States of America, Canada and Russia. Two G8 countries have come up with an internet surveillance system that protects and monitors the activity of hackers around the clock. The online protection system works as a shield that is set up by the finest and most intelligent information and technology experts from the aforementioned countries[77]. The Shield notifies the government regarding any breach of cyberspace either through emails or any FTP codes being circulated in the municipal domestic cyberspace of a particular server using the shield as a security measure to protect their cyberspace. The Shield not only informs them about a breach conducted but it also informs the government regarding the attempt of a breach. Therefore, it has the potential to stop a crime before being committed using cyberspace. The Council of Europe had requested the G8 countries to come up with a permanent solution to cybercrimes. The rise in number of cybercrimes and subsequent difficulty in tracing the hackers (as they disguised their internet protocol addresses) were among the many objectives of the invisible cyber shield. The G8 counties installed a scrutiny system for the active invigilation of police and other investigative agencies for the offences committed over the internet. It is extremely important to mention that the G8 countries

[76] Council of Europe, Discussion guide for consultations with civil society, data protection authorities and industry, https://rm.coe.int/t-cy-2018-16- pdp-consultations-paper/16808add27.

[77] Markoff and A. Kramer, U.S. and Russia Differ on a Treaty for Cyberspace, N.Y. Times (June 27, 2009), available at http:// www.nytimes.com/2009/06/28/world/28cyber.html?_r=1&scp=3&sq=Vladislav%20Sherstyuk&st=cse

worked in tandem in order to successfully code this universal invisible cyber shield. This cyber protection mechanism is not provided to the common public but can be linked out to two important corporate companies for the protection of that data and security by the government[78].

Domestic Laws of United States of America on the Jurisdiction of Cyber Crimes

Like any other country, the United States of America must have legitimate jurisdiction in order to prosecute an individual for an offence of crime which may include the involvement of cyberspace (as the medium through which the crime was committed). In judicial proceedings which involves the assumption of jurisdiction in order to hear and try the matter shall prove to be *ultra vires* if the jurisdiction claimed by the court is not accurate, this principle applies to the courts all around the world including the United States of America. Therefore as per this principle, the court pronouncing the judgement and entertaining the matter to be heard in the United States can proceed to execute justice for the clients which have been committed in the territory where the court is empowered to hear the matter. This principle of extraterritorial application of the law where the court cannot entertain a matter where its jurisdiction does not exist was enshrined in the case **United States v Cotton[79]**. The principle of extraterritorial application of the law has been propounded by jurists in order to avoid the ambiguous amalgamation of jurisprudence, where the subject matter involves multinational complexities. In a case that requires multiple parties from different jurisdictions, it is quite likely that a part of the subject matter is influenced by the international or domestic law of a different State, therefore to avoid inconsistency and hindrance in the justice mechanism it is an established principle that courts abound by their territorial jurisdiction in order to dispense justice and in this way there isn't any fiction or ambiguity/inconsistancy with the set of laws enshrined by a different sovereign or even international law.

[78] William New, "Privacy agenda in 2002 has international flavor," *National Journal Technology Daily*, Jan. 23, 2002; "Under Antiterror Law, Government Can Use U.S. Standards to Nab Foreign Hackers," Associated Press, Nov. 21, 2001.
[79] 471 F.2d 744

However, in the past decade, it is seen that there is a Proactive effort on behalf of Congress to legislate laws that endorse the idea of a flexible criminal jurisdiction which may in certain circumstances exceed the geographical limits of the sovereignty. This type of Jurisdiction which exceeds its territorial limit was legislated in the first place in order to tackle the dynamic nature of Cybercrimes. As mentioned above cybercrime seldom originates from the same country in which the damage is caused, therefore, in a developed country such as the United States of America, it is imperative for the speedy delivery of justice that they are have an efficient criminal justice administration of cyberspace. For example, Section 1029 of The United States of America Patriot Act of 2001 was tastefully modified by Congress with the intention of providing it with flexible jurisdiction for not only the particular statute but the whole act in itself.

The aforementioned Section 1029 of the United States of America Patriot Act elucidates that, any individual, group of individuals or even juristic persons who had committed an offence outside the geographical territory of the United States of America shall be subject to prosecution which may end up in them paying fines, forfeiture of property, in even imprisonment, in cases where the said offence was committed outside the geographical territory of United States of America. It is also defined that in order to pursue the offence the culprit had used a device that is owned, manufactured, controlled by an official financial institution or any other entity residing and registered from the United States of America. Furthermore, the culprit has transported, delivered, or conveyed proprietary information such as, information and technology details which are confidential, passwords and secrets or even if he has not delivered this information but he had stored them without authority irrespective of whether he is residing in the United States of America outside, he shall be liable for prosecution from such offences as if he had derived the position while residing in the sovereignty mentioned above[80].

In furtherance of the Congress legislating laws which exceeds the geographical jurisdiction of the courts in order to prosecute matters where the damage has been inflicted by someone residing in a different country - the state legislators have taken a

[80] Uniform State Laws: A Discussion Focused On Revision Of The Uniform Commercial Code, 22 OKLA. CITY U. L. REV. 257, 259 (Albert J. Rosenthal, Moderator 1997) (symposium discussion); Steven L. Schwarcz, A Fundamental Inquiry Into The Statutory Rulemaking Process Of Private Legislatures, 29 GA. L. REV. 909, 940 (1995).

lead from the same and celebrated the true essence of federalism by legislating laws which provide extraterritorial jurisdiction even to the statutes which state bound. In other words, a particular state who is a part of the federal structure of the United States of America, while hearing a matter involving the use of cyberspace for the commission of an offence, whereby the accused involved resides in a different state where the jurisdiction of the local court does not ideally apply but now after the amendments and the new laws been legislated even the states can exhibit extraterritorial jurisdiction for the trial of particular of offences, especially involving cyberspace. For example, the state of North Carolina has an extremely liberal law when it comes to cyberstalking. The law states that the offense of cyberstalking which involves sending an email or even an electronic message which can be communicated by using social media for instance in order to communicate a message by a stranger shall deem to be the ideal components of cyberstalking. Therefore any individual who has sent a message in order to stalk an individual shall mount at cyberstalking and the state of North Carolina can prosecute the said individual even if he is residing in a different state in the United States of America.[81] Similar encroachments of the local jurisdiction involving cyberspace can be seen by other states in the United States of America as well. For example the state of Arkansas which provides jurisdiction and power to the courts to conduct trials regarding computer-related offences. The statute states that any offence which is committed against a resident of the state of Arkansas which involves the medium of the internet in order to complete the offence in that case the federal court of Arkansas has the power to hear and trial the matter against an individual who had inflicted the damage and who may reside in some other state.

Olez Zezev v. Bloomberg Inc.[82]

Right at the turn of the millennium, this particular case shook global headlines as a targeted and surgical attack invasion of cyberspace was conducted against one of the industry's leading cyberspace experts. In the month of March, the year 2000 Olez Zezev who was a hacker and cyber abuser, conducted a surgical operation against Bloomberg organisations computer security system. Bloomberg was founded in 1981

[81] Source: https://commons.erau.edu/cgi/viewcontent.cgi?article=1373&context=adfsl
[82]Source: https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/zezevSent.htm

by Michael Bloomberg and the company extensively contributes to today's finance, software and cybersecurity infrastructure. Olez Zezev was successful in gaining access to Bloomberg private computer security system, this access was ofcourse unauthorised in nature. The hacker not only assessed the breach of the computer system but also garnered sensitive and confidential information regarding the company. He even managed to hack into the computer of Michael Bloomberg who was then the founder and CEO of the company[83].

This particular case is extremely relevant to study the extrajudicial application of the domestic laws of the United States of America and the expeditious commitment of judicial mechanism of the country in order to deliver justice for crimes committed by using cyberspace. Olez Zezev hacked into the computers and accessed information which was confidential and limited to the employees of Bloomberg and the surprising fact about the whole operation was the hacker did all this from his home country, which is Kazakhstan under a pseudonym taken by him (Alex) in order to hide his identity. From Kazakhstan sent an electronic message to the CEO of Bloomberg under the fake name and threatened him that he will expose Bloomberg's confidential information to the public if he is not paid a ransom of $200000.

The case was ultimately taken up by the Federal Bureau of Investigation and a booby trap was set up in order to catch Olez Zezev. The hacker was informed that if he comes to the United Kingdom and explains to a group of employees from Bloomberg regarding the methods incorporated by him in order to breach the security system of Bloomberg, that subsequently he would be paid the ransom amount. Tempted by the fact he could make $200000 this way, Olez Zezev went to the United Kingdom and where he was supposed to meet the alleged Bloomberg employees, he even demonstrated the method used by him in order to hack the security systems of Bloomberg.[84] Right after the demonstration he was arrested by the Federal Bureau of Investigation in the United Kingdom and was extradited to the United States of America where he was subsequently prosecuted for the offence of Cyber hacking and

---

83 https://www.researchgate.net/publication/321392125_The_Jordanian_General_Prosecutor_Decision_No_1231_of_2008_over_the_Case_of_the_Dutch_Cartoons_vs_Prophet_Muhammad_PBUH_Case

84 *Ibid.*

was jailed for more than 70 years. This is one of the examples where the jurisdiction of the court exceeded beyond the territorial boundaries of the United States of America.

The United States of America v. Vasiliy Gorshkov[85]

In this particular case, a group of hackers belonging from the country Russia conducted a series of hacking activities in the pursuit of defrauding common people in the year 2000. The bulk of the hacking activity was instigated in the United States of America. The FBI took the cognizance of the breaches made by the hackers in the personal computers of the common folk and decided to set up a plan in order to catch the culprits. The FBI set up a fake company dealing in information and technology and they named it Invita. After setting up the company they broadcasted an advertisement seeking cyber experts who can help them run the company in its day to day functioning. The hackers who are responsible for the series of hacking conducted in 2000 were namely Vasiliy Gorshkov and Alexey Ivanov. The above-mentioned hackers were contacted by the fake company set up by the Federal Bureau of Investigation and invited for an interview in the United States of America for a lucrative position in the company. The hackers were proficient with information and technology; they were tempted by the proposal and went to the United States of America to pursue the interview. They had no idea that the interview and the company was fake and this was all set up by the Federal Bureau of Investigation in order to catch them red-handed.[86]

When Vasiliy Gorshkov and Ivanov came to America they were requested to exhibit their hacking skills before the board of interviewers in order to prove that they qualify for the job which requires high technical skills and computer proficiency. The hackers demonstrated their hacking skills on the computers which were provided by the Federal Bureau of Investigation little did they know that this was a method incorporated by the Federal Bureau of Investigation to procure the username and password of the hackers. Upon procuring the username and password of the hackers they were arrested by the Federal Bureau of Investigation and subsequently put up for trial. The username and

[85] 2001 WL 1024026, U.S. Dist. LEXIS 26306 (W.D. Wash. 2001).

[86] Attfield, Philip (2005). "United States v Gorshkov Detailed Forensics and Case Study; Expert Witness Perspective". *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*. Institute of Electrical and Electronics Engineers. pp. 3–26. doi:10.1109/SADFE.2005.28

password were used by the information and technology experts at the FBI to get proprietary information from the system which was used by the hackers to conduct the hacking operations in the United States of America. These personal computers were situated in Russian and the proprietary information was gathered by the Federal Bureau of Investigation, by the medium of the internet, from America itself. At the trial, the hackers contemplated that the evidence used by the Federal Bureau of Investigation was illegally obtained as the same did not have a search and seizure warrant to garner proprietary information which was accessed from the computer which was in Russia. The hackers say that the information provided by FBI was obtained from the domestic computers and proceeding with the trial the evidence would amount to self-incrimination which is against the Fourth Amendment of The United States of America constitution. The Fourth Amendment states that any criminal accused under trial has the right to remain silent during interrogation and has the right to protect himself from self-incrimination. Finally, the hackers' arguments concluded by stating that the search conducted by the FBI was illegal in nature as they did not have a search warrant to conduct the same in the first place[87].

The question which lay before the court was the fact that two Russian citizens were involved in the crime of hacking conducted from Russian to the citizens of the United States of America. It was such that the method incorporated by the FBI is not in the traditional sense as there was no physical entrance open office to get first-hand information in the premise used by the hackers to conduct the illegal activity. On the one hand, the United States of America did not consult with the Russian authorities for joint and mutual investigation of the offence committed by the hackers. The flip side of the argument mooted by the Federal Bureau of Investigation was that downloading information from a computer does not amount to search and seizure as traditionally the data downloaded remains in the hackers' computer and since there isn't a need for the physical influence of an officer inside the premise used by the hackers, therefore, the Federal Bureau of Investigation did not need the warrant to conduct the activity of

[87] Lemley, Mark; Menell, Peter; Merges, Robert; Samuelson, Pamela; Carver, Brian (2011). *Software and Internet Law* (4th ed.). ISBN 978-0-7355-8915-5.

downloading information remotely from the United States of America from the personal computers of the hacker situated in Russia.

The court dismissed the matter in favour of the Federal Bureau of Investigation and pronounce that the accessing of information from the computer of the hackers situated in a remote location outside the territory of The United States of America does not amount to self-incrimination therefore the immunity desired under the Fourth Amendment of the American constitution cannot be granted to the hackers. It is clarified by the Hon'ble Court that the proprietary information which was downloaded from the Russian computer was not downloaded to get the possession of the same as the altered data was present with the Russian computers, whereas the data was only used to get evidence against the hackers. The Federal Bureau of Investigation clarified that the operation was conducted while keeping the best interest of justice in mind therefore the Russian counterpart was not contacted as it would have resulted in the delay of proceedings and trials of the same which would give the hackers the opportunity to alter the data present on their personal computer[88].

Laws of the United Kingdom on the Jurisdiction of Cyber Crime

The main act or statute which is the foundation of the laws related to cyberspace in the United Kingdom is the Computer Misuse Act of 1990. This act was the first act that attempted to define the abstract jurisprudence of cyberspace. Sections 1, 2 and 3 of the act define the various offences committed in cyberspace which includes the breaching of the computer. In order to seek information that was not meant to be accessed by the hacker in the first place, the sections also include alteration and modification of the information present in the computer[89]. A similar practice of exceeding its jurisprudence in crimes involving cyberspace as seen with the United States of America is explained in the above section. Here as well in the United Kingdom it is the common practice that when an offence is committed involving cyberspace and the cyber abuser resides outside the territorial boundaries of United Kingdom, the code of law in the United

[88] Newcomb, Penny. "Russian Man Sentenced for Hacking into Computers in the United States". U.S. Department of Justice. Retrieved February 6, 2012.

[89] Digital Britain Report http://www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf

Kingdom has the power to prosecute the cyber abuser who resides outside the United Kingdom. Under the Computer Misuse Act 1990, there is only one condition that has to be satisfied in order to invoke the flexibility of the jurisdiction of the court floor and the condition is that the offence committed by the cyber abuser has to cause an injury or damage which is pertinent to the United Kingdom. In other words, the action of cyber abuse has to be significantly and directly linked to the damage or injury caused to any citizen, juristic person, a group of people, institutions including the government of the United Kingdom.

Earlier when the United Kingdom was part of the European Union, the Computer Misuse Act of 1990 was read and applied with the Council of Europe's international convention in cases of prosecution and trial. The computer misuse act 1990 attempts to define the abstract jurisprudence of cyberspace but it has certain lacunas such as initiating trial against foreign nationals where the Treaty of extradition has not been signed with the country the United Kingdom and the other country where the cyber abuser resides. This limitation was fulfilled by the international cybercrime convention which was passed by the Council of Europe in the year 2000 as it supplemented the shortcomings which were part of the Computer Misuse Act 1990. To explain this further Article 22 of the international convention against Cybercrimes provides the rules and regulations which the contracting parties of the Treaty have to oblige in order to demarcate the jurisdiction of the criminal action or act committed by the cyber offender[90].

The aforementioned article of the international convention jurisdiction of the criminal action is defined as the country where the crime has been committed shall act as the primary jurisdiction empowered to pursue the prosecution and conduct the trial of the offence committed within the territorial limits of the country which gives power to its court of law to hear and prosecute matters which involve infringement of rights. The subsequent subsection of the article elucidated regarding the principle of territoriality and its application in the field of cyberspace. The paragraphs explain the various

[90] Source: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

scenarios when the offence is committed which involves the usage of cyberspace but the place of execution of the offence has no sovereign identity. This type of offence is extremely common as it is executed on the deck of a ship, cruiseliner, carrier vessel, or even an aeroplane. In this case where the offence is committed through cyberspace where there is no sovereign control over the territory then the principle of territoriality exceeds its boundaries and it is flexible in such a way that helps to initiate the trial and investigation of the said offence committed. Therefore in this case the jurisdiction which has the power to hear and prosecute the offence is the country where the ship, aeroplane, cruiseliner, any other vessel on which the offence was committed was initially registered. Therefore that country where the registration belongs of the vessel or aeroplane on which the offence has been committed shall have the power to prosecute and continue the trial and investigation. It is mandatory for the trial and investigation of an offence which may or even may not involve cyberspace to be related with nationality as the court system gets authority to prosecute from the nationality and without having a justified nationality it is impossible to register a complaint of an offence. Places where the offence is committed which does not directly have the geographic identity of a nationality feature as a cruise liner, but instances where a complaint is required to be registered, these vessels/aeroplane act as the representatives or extension of the nationality where they are currently registered. Therefore, in other words it means that it is a crime committed on board the ship registered ascertains nationality, the act of an offence shall be deemed to have been committed in the geographical territory of that nationality itself. Thereby the court of the law getting its power from the particular sovereignty in question has the right and power to prosecute the particular offence committed remotely[91].

The aforementioned paragraph and statute also mentions in the international convention the cases where a person who is a foreign national residing in a different country, whereby he commits an offence which cannot be prosecuted in the domestic laws of that country but his action amounts to an offence in his own country. In such a case the international convention states that the person can be prosecuted in his own country and

[91] House of Lords Science & Technology Committee Report into Personal Internet Security http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

can be extradited from the foreign country to his own country in order to complete the process of investigation and trial.[92] This principle is successful in those cases where there is a treaty of extradition already signed between the countries. The aforementioned principle can be explained with the following example, that a man who had the nationality of Pakistan commits an offence in the kingdom of Bhutan but his action does not amount to an offence under the laws of the Kingdom of Bhutan, although his actions amount as an offence in his motherland, that is Pakistan. In this case, the court of law in Pakistan has the power to initiate a proceeding against this person in Pakistan and once the proceeding is initiated by the government then Pakistan can extradite this person from the Kingdom of Bhutan. Therefore the international convention on cybersecurity which was passed by the Council of Europe provides a fair deal of flexibility of jurisdiction with respect to matters involving cyberspace[93].

Gary McKinnon Case[94]

This particular case of Gary Mckinnon is the landmark case in the jurisprudence of Cybercrimes in the United Kingdom as the offence of hacking and controlling computers from a remote location was conducted by Gary Mckinnon right around the same time when a new treaty for extradition was signed between the United Kingdom and the United States of America. In 2002 Gary McKinnon who was doing a job in administration sector in the United Kingdom conducted a series of hacking activities and was eventually successful to Breach 97 military bases of United States of America and also a few computer systems of The National Aeronautics And Space Administration Agency which is the world's premier organisation for space exploration situated in Washington DC, USA[95].

Following this paragraph is the list of computers and databases that Gary Mckinnon was able to successfully breach and access unauthorized confidential information:-

---

[92] ps.gov.uk/legal-guidance/cybercrime-prosecution-guidance#:~:text=Computer%20Misuse%20Act%201990%20('CMA,hacking%20or%20denial%20of%20service.&text=There%20also%20must%20have%20been,of%

[93] Gregory T. Nojeim, Cybersecurity and Freedom on the Internet, 4 Journal Of National Security Law & Policy, 119, (2010).

[94] [2007] EWHC 762 (Admin)

[95] Sherwell, Philip (26 July 2009). "Hacker Gary McKinnon will receive no pity, insists US". *The Telegraph*. London. Retrieved 30 January 2010.

- He was successfully able to hack 2000 computers belonging to the United States Army military district to Washington network. Due to this hacking activity, the aforementioned 2000 computers were forced to shut down for a whole day.
- Around 2500 US Army computers became inaccessible as they were shutting down and restarting the booting process.
- The confidential information regarding the location, number of personnel serving on the vessel, the type and condition of the vessel, was obtained by the hacker as he was able to bridge the computer of US Naval weapons station Earl, which was already a battle-ready Naval ship of the US Navy.
- The hacker was not only able to bridge the computers and was able to remotely control the activities of the same but in addition to that, he copied confidential information which he was not authorised to access onto his own personal computer.
- Since the computers of the US Defence Services were remotely controlled by Gary Mckinnon, the country was exposed to a compromised security system for a number of hours as the premium defence organisation was struggling due to the security breach. Therefore the citizens of America were in danger of any intruder during the period of hacking as the control of the US Army which largely depends on information and technology was breached and hacked by Gary Mckinnon.
- It was estimated that 22 confidential documents from the US Army computers, 35 confidential files from the US Navy computer database And subsequently six search files which were of confidential nature were intruded from the database of the National Aeronautics and Space Administration agency.

Gary McKinnon, who was a British National, conducted the activity of hacking into the US military database from the United Kingdom remotely. He was successful in hacking the computers and when it was figured out that he was involved in the offence of hacking he was arrested by the police in the United Kingdom and was arrested on the grounds of the Computer Misuse Act of 1990. The United States of America government wanted the culprit to be extradited to America where the

punishment/gravity of the offence committed by Gary McKinnon was more severe than what was available in the United Kingdom[96].

Since there was an extradition treaty already in place between the United Kingdom and the United States of America it was only a matter of formality which was initiated by the United States of America to initiate the process of extradition of Gary McKinnon so that he can be prosecuted under the US Federal laws. In 2004, 2 years after the commission of the offence of hacking by Gary McKinnon, he was extradited to the United States of America and subsequently in autumn of 2004 charges were filed against Gary McKinnon in the court of Virginia and New Jersey and thereafter when the charges were filed against him, the Courts issued an arrest warrant against Gary McKinnon. [97]

Gary McKinnon and his lawyers challenge the arrest claiming it that it is an extrajudicial exercise of power and that such in rest and subsequent prosecution is against rule of law. The claim of Mr McKinnon is that the offence was committed in the country of the United Kingdom and thereafter the jurisdiction which shall conduct his prosecution should be the jurisdiction where the offence was committed. To whom the offence was committed does not determine the jurisdiction in the court of law empowered to conduct the prosecution. It is to be noted that while Mr MacKinnon and his lawyers vehemently try to impose the jurisdiction of the United Kingdom because of the very fact that the United Kingdom and the Computer Misuse Act 1990 is extremely lenient regarding the sentence of punishment in crimes involving cyberspace and particularly the nature of the crime which was committed by Gary Mckinnon[98].

The offence committed by Gary McKinnon which involved hacking into the US military computers and computers of the National Aeronautical and Space Administration agency amounted to a maximum sentence of 5 years under the Computer Misuse Act of 1990 in the United Kingdom. Whereas to a stark contrast from this, the jurisprudence in America governing this type of crime allows a maximum

[96] Sherwell, Philip (26 July 2009). "Hacker Gary McKinnon will receive no pity, insists US". *The Telegraph*. London. Retrieved 30 January 2010.
[97] Boyd, Clark (30 July 2008). "Profile: Gary McKinnon". *BBC News*. Retrieved 15 November 2008.
[98] Batty, David (26 November 2009). "Timeline: Gary McKinnon's fight against extradition to the US". *The Guardian*. London.

sentence of 70 years if an individual is found guilty of the nature of the offence committed by Gary Mckinnon. In the year to come that is in 2006 the honourable justice at Street Magistrates Court pronounced that the extradition of Gary Mckinnon was lawful in nature and therefore there is no extrajudicial influence was involved in the prosecution of the same. The Crown Prosecution service also give the public notice in 2009 which stated is that its jurisdiction on the case isn't of primary nature and although the offence committed by Gary Mckinnon as a citizen of the United Kingdom and was residing at the of the commission of the offence in the United Kingdom is all true but the offence was targeted against The US military making the injury and the damage caused by the accused multinational in nature.

In addition to that, the Crown Prosecution Service was unable to find the *mens rea* behind the actions of Gary McKinnon activities of hacking into the US defence computer system. It should be noted that in order to be prosecuted under the Computer Misuse Act of 1990 the Crown Prosecution Service has to establish the reason for the commission of a crime in order for the court to deliver its judgement. Section 3 of the computer misuse act state that an individual is liable to be trialed under this act if he or she has deliberately or rashly venturesome and included an individual, group of individuals or even institutions including government organisations, computer or information technologies databases, with the clear intention of causing hindrance which results in the absence difficulty to perform the requisite service required from the same in the first place. Therefore under the section, if we juxtapose the facts of the Gary McKinnon case it seems that the reason for causing the hindrance was unclear by the Crown Prosecution Service, therefore his prosecution could not be conducted under the court of law of the United Kingdom. In addition to that, the Computer Misuse Act is empowered to conduct prosecution against individuals who have committed an offence involving cyberspace where the culprit resides in the country of the United Kingdom and the damage inflicted by the same is closely and intricately related to the country of the United Kingdom. In this case, the damage was caused in the United States of

America remotely this *de facto* makes the Computer Misuse Act of 1990 inconsistent and inapplicable.[99]

Principles of Conflict over the Jurisdiction of Cyber Crimes

Crimes involving cyberspace are executed in multiple countries at the same time, therefore, to give you an example if the offence is committed against an American citizen who is residing in America by a British citizen who is residing in the United Kingdom, in such a case if the offence committed by the British citizen is punishable in America and there is an established set of laws catering to the jurisprudence in which the crime has been committed then in that case the court of law in the United States of America has the jurisdiction to prosecute (the accused individual who is a British citizen residing in the United Kingdom). The principle of nationality is enshrined that the States provides the necessary flexibility of its jurisdiction in order to conduct trials where damage has been caused to its citizen from a remote location.

In the aforementioned Gary Mckinnon case is an extremely complicated case as it involves two nationalities and the damage which was incurred hacking activity Gary Mckinnon was against the nationality of the United States of America. This made the USA a party to the suit hacking activity based on its defence system making the most powerful country in the world vulnerable to Cyber attacks and other security breaches for a long period of time. It is to be noted that is Gary Mckinnon who had been an American citizen residing in the United Kingdom at the time when the offence was committed, he then too would have been eligible to be extradited to the United States of America as he committed an offence which was punished in the court of law established under the federal laws of the United States. The offence committed by Gary McKinnon while residing in the United Kingdom is directly associated with the United States of America and was not remotely associated with the United Kingdom, which was the place of his residence. Therefore the nationality where his actions are directly involved would qualify as the requisite jurisdiction to conduct the prosecution. The Computer Misuse Act of 1990 explicitly provides that the action of the culprit conducting the

[99] Law Lords Department (30 July 2008). "House of Lords - Mckinnon V Government of The United States of America and Another [2008] UKHL 59". Publications.parliament.uk. Retrieved 30 January 2010.

cybercrime has to be directly linked to the United Kingdom in order to be prosecuted. The equation becomes slightly complicated had Gary McKinnon, a citizen of America, conducted a crime while he was residing in Russia and this particular crime would have been targeted at the US military. In this hypothetical example, the courts of the United States of America would still have the authority to prosecute Gary McKinnon and the country of Russia who is not directly involved in the execution of this offence whereas the damage has been categorically targeted at the United States of America.

Jurisdiction of Cyber Crimes in India

The concept of cybercrime is slightly new in the Indian jurisprudence but before we understand the jurisprudence governing cyberspace in India it is important to understand the meaning and nature of the jurisdiction of cyberspace in India. It is challenging to understand the jurisdiction of cyberspace when the word jurisdiction has not been defined under any statutes on legislation that is applicable in India. Jurisdiction however has not been defined anywhere it means the authority of the court given by the constitution of India making it eligible to conduct proceedings against various parties who put forward a dispute to be resolved. Ideally, the dispute which has to be resolved originates from the territory where the Court of law is situated. Therefore it is the territorial boundary that gives the abstracts shape to the jurisdiction of the court.

It was in the case of **Hriday Nath v. Ram Chandra[100],** which elucidated the power of the court to decide cases that involve the infringement of right by one party and the other party is affected by the same. In this case, the Honourable Judiciary took the cognizance of the Maxim *ubi jus ibi remedium* as it's one of the core principles in dispensing Justice. The maxim states that whenever there is an infringement of right the Court established by law shall offer remedy against the infringement of the same. Therefore the yardstick to calculate or test whether the jurisdiction of the court is legitimate to conduct the proceedings is by simply checking where the offence has been committed. The court of law which pronounces and delivers justice in the area where

[100] AIR 1929 Cal 445

the offence has been committed shall have the requisite jurisdiction to initiate proceedings.

Code of Civil Procedure under Section 9 provides that every Court established in India has the power and the right to conduct trials and only when it is expressly implied or prohibited by a statute or legislature then the court of law would not prosecute the subject matter. This particular section was elucidated and explained in the landmark case of **Ganga Bai v. Vijay Kumar[101].** In this case the Honorable Court said that it is an inherent right of an individual to file a matter of a civil nature in a civil court and the court has the duty to listen to the grievance of the parties involved but this would not imply in cases where the court is restricted to perform its duty by a statute in place which makes it expressly implied the particular court where the matter had been initiated is the debarred to perform it's normal duty pertaining to the subject matter of the case.

In the case of **Robust Hotels Private Limited v. EIH Limited[102],** the Honorable Court elucidated that regarding the jurisdiction of Civil Court the power to initiate and file the subject matter is of the absolute nature unless the same is expressly implied law to apply by a statute or otherwise the particular court in question has the power to prosecute the matter.

The burden of proof in order to prove the maintainability of the jurisdiction lies on the party who has initiated the proceedings in the first place. In the case, **Saheb Gouda v. Ogeppa[103]** the Honorable Court pronounced that it is the duty of the person who has brought to the notice of the court that it has superseded its power to advocate the particular subject matter, in this case, the party who has brought the notice has to put before the court its limitation to proceed with the matter.

The maintainability of a suit is a question of law. At the time of the admission of the suit all cases involving a civil nature can be tried in a civil court unless they are barred by a law that expressly debars the cognizance of the case. It is to be noted that the subject matter of the court does not determine the jurisdiction wherein it shall be

[101] 1974 AIR 1126, 1974 SCR (3) 882

[102] CIVIL APPEAL Nos. 11886-11887 OF 2016

[103] Appeal (civil) 1352-53 of 1993

adjudicated, this observation was made by the Honorable Court in the case of **Jyoti Limited v. Bharat Jay Patel.**

In the case of **Shankar Narayan Poti v. Sridevi[104],** the Honorable Supreme Court of India in Section 9 of the Code of Civil Procedure pronounced that the Civil Court is capable and empowered to hear a matter arising from a civil subject matter and in cases where it is expressly debarred to conduct the trial of the matter is when the civil court shall have renounced its power to take cognizance of the same.

Definition of Suit of Civil Nature

The word civil nature has not been defined in the Code of Civil Procedure 1908 but a preliminary understanding can be established by differentiating a civil suit from a criminal case. The basic ingredient which is required for a case to be a criminal suit in nature is the *mens rea* which is behind the commission of the offence. Enough said that offence which is committed against an individual to cause harm or injury and this particular option is defined under the Indian Penal Code then the state shall take cognizance of the case and prosecute as a criminal case. Whereas if a wrong has been committed against an individual which infringes civil rights then the individual, in particular, can file a Suit against the other party. In cases arising from civil suit, it (court of law; unlike the criminal courts/jurisprudence) does not take *de facto* cognizance and the subject matter has to be initiated by the parties involved in the subject matter. As mentioned above, it is the inherent right of the court to take cognizance of the case where the Civil right of an individual has been harmed in one or more ways possible. In the landmark case of **Kehar Singh Nihal Singh v. Custodian General[105]**, The Honorable apex court of India that is the supreme court of India let down the guiding principles which help us establish whether a suit can be initiate or not. The guiding principle is that during the course of injury or damage to the right(s) of the individual; whether this right is a private right to access civil liberties or a personal right is for the purview of the court to decide.

[104] AIR 1990 Ker 151
[105] AIR 1958 HP 58

In the United States of America case, namely **Frothinghham v. Mellon**[106], the term private rights was defined as right which is given to a particular individual who has received immediate danger of injury and in a way, such injury which was targeted at an individual may lead to the general public in a contagious manner. Civil rights include the right to assemble, the right to follow and propagate religion, the sexual orientation of an individual, his right to assemble and share ideas to the public, his rights related to gender, life and liberty under civil rights.

Exclusion of Jurisdiction

The cardinal principle involving the exclusion of jurisdiction pertaining to the civil court is an expressive or implied applicable law which ousts the jurisdiction of the civil court, whereby the matter cannot be preceded in that court. It was decided in **Balawwa v. Hasanabi**[107], civil court jurisdiction which is defined by the statute giving power to the civil court to proceed such proceeding that can be debarred if there is a statute which expressly or implied ousts the jurisdiction of the civil court. It should be noted that there have been cases where the subject-matter involves many matters within it, therefore there can be cases where only a part of the subject-matter of the suit has been debarred to be proceeded in the civil court but other Sub subject matter of the main suit can proceed in the same civil court. Therefore an implied or expressive exclusion of jurisdiction does not disqualify the competence of the civil court in order to proceed with the proceedings part of the whole suit and not the whole suit in itself. Keeping this thing in mind we can understand that the civil procedure code is ambiguous regarding the continuation of dual proceedings of the same subject matter. It is not mentioned in the Civil Procedure Code that while a part of the proceeding can be conducted in the civil court, the special tribunal or the special court has no jurisdiction to proceed in case if part of the subject matter is heard by the special court/tribunal and whether it has the power to give a decree which can be made applicable in the civil court.

Plea of Absence of Jurisdiction

[106] 262 U.S. 447
[107] JT 2000 (3) SC 600, (2000) 9 SCC 272

In the case of **Kiran Singh vs. Chaman Pavan**[108]**,** the Honorable apex court of India provided with the definition of the jurisdiction of the Civil Court and made it more flexible and accommodating for the people who are parties to the suit. The Honourable apex court pronounced that any Court which is competent to deliver justice in matters arising from civil jurisprudence can hear and continue with the trial of the case but if there is an objection raised against the jurisdiction of the court then the burden of proof would lie on the party which promulgates the objection. The court further elucidated that the absence of jurisdiction can be brought in at any stage of the proceedings of the trial and even at the stage of pronouncement of the judgement, (at the time when collateral proceedings commences). It is the duty of the court to entertain the plea of absence of jurisdiction and thereby the court is competent to pronounce its own validity of Jurisdiction pertaining to the subject matter of the case.

In the landmark case of **Chief Engineer Hydel project v. Rabindranath**[109], the Honourable apex court pronounced that the plea of absence of jurisdiction raised by the other party cannot be mechanically dismissed. It was observed that it is not *sine qua non* in the proceedings of a trial that the application of plea against jurisdiction is rejected on the grounds that the same was not initiated by the party during the framing of the charge. The civil court is competent to decide its own validity pertaining to the jurisdiction and such validity can be decided at any point of the suit and the only condition which lies is the burden of proof which is on the party which puts forward the plea of absence of jurisdiction. It is to be noted that while the first plea of absence of jurisdiction can be initiated during any time of the proceeding, it has to be kept in mind that such a plea would only be entertained during the first instance and not during the appeal against the order of the Civil Court. In other words, it basically means that when the Civil Court pronounces judgement then an appeal against the judgement lies with the party which has not won. In the appeal, the losing party cannot bring the plea of absence of jurisdiction on account of the lower court when the same was not brought during its proceedings in the lower court. This way the losing party gets the undue

[108] 1954 AIR 340, 1955 SCR 117

[109] Appeal (civil) 658 of 2008

advantage and it is discouraged in the common practice of law. This would give the losing party a chance to hinder with the process of justice and also cause delays in the justice administration system. Such a practice is against the principles of natural justice and rule of law. It is a standard principle in India regarding the plea against the jurisdiction of a court of law hearing a civil matter that it cannot be entertained in the stage of appeal; a plea against the jurisdiction of the court can be initiated by a party during any time of the proceeding but the standard condition relies upon as the proceeding must be at the initial stage in the court of law and shall be deemed to be the original jurisdiction of the suit.

Types of Jurisdiction in India

Pecuniary Jurisdiction

According to the Oxford English dictionary, pecuniary means something related to/containing money. Pecuniary jurisdiction is the limit of the valuation of the suit which ultimately decides the competent jurisdiction of the court empowered to hear and try the case. Every case which is initiated in a civil court brings forward a subject matter where a private right of an individual or a group of individuals including a juristic person has been breached by the other party. Such a breach of private right is accompanied by a cost that tells us about the magnitude of the loss and the cost of the subject matter. Therefore this valuation of the subject matter determines the pecuniary value of the case and thereafter the particular case has to be filed in the court which is competent to hear matters belonging to a certain range of valuation.

To further explain the pecuniary aspect of jurisdiction of the courts, Section 15 of the Code of Civil Procedure elucidates that the court case has to be initiated by a court that is of the lowest grade competent to hear the matter. The fact that Indian Judiciary has a hierarchical system where there are different courts competent to hear different matters. These matters are differentiated in terms of their jurisdiction.

Jurisdiction can be related to the geographical position/situation/occurrence of the subject matter of the suit or it can be related to the pecuniary valuation of the suit.

Therefore Section 15 of the Code of Civil Procedure[110] tells that the court which is of the lowest grade in the hierarchical system of the Indian Judiciary, which is competent by law to hear the matter which comprises a certain specific valuation, shall be initiated in that Court only.

There are multiple reasons to differentiate a suit on grounds of pecuniary jurisdiction. Pecuniary jurisdiction gives us one more method to categorise the competent court where it is understood/certain regarding the occurrence/origination of subject matter. In other words in cases where it is known that the original jurisdiction lies where the subject matter had occurred then, in that case, there is a series of courts competent to hear the matter, in order to reduce the burden on the courts and finalize which particular Court within the territorial jurisdiction is competent to hear the matter, the concept of pecuniary jurisdiction was given. Under this where the primary jurisdiction is established followed by the valuation of the court enables the parties to initiate the proceedings in the right court. The principle of pecuniary jurisdiction can be understood by the following illustration: Ravi, who is a transporter by work, was getting Satin material delivered to Rahul in New Delhi. Due to some delay the material was not able to be delivered to Rahul within the stipulated time frame. For the breach of this contract between Rahul and Ravi, the former is obliged to initiate the proceeding where the contract was signed over (where Rahul resides). It is understood that Rahul resides in New Delhi and the contract was signed in New Delhi therefore the original jurisdiction. That is the territorial jurisdiction lies in New Delhi now in Delhi there are multiple courts in Delhi, for example the High Court of New Delhi, the Supreme Court of India, Tees Hazari Court etc, therefore the question arises in which court the subject matter has to be initiated. To solve this question the evaluation of the subject matter is determined which in the above analogy can be assumed to be Rupees 5000. In this case, where the valuation of the suit is Rupees 5000 and the original jurisdiction where the subject matter has been associated is New Delhi, it is certain that this case would be filed at the Court of Small Causes in New Delhi.

[110] Source: https://www.indiacode.nic.in/show-data?actid=AC_CEN_3_20_00051_190805_1523340333624&sectionId=33348&sectionno=15&orderno=15

Territorial Jurisdiction

In a civil case, there is a subject matter and it is logical to assume that there would be a territorial association related to the subject matter. In other words, it basically means the subject matter of a case has originated or associated with the local premise, therefore that local premise is called the territorial jurisdiction of the case. Any action or subject matter cannot be beyond the said territorial limit. However, there have been occasions when there has been more than one jurisdiction pertaining to the subject matter. Such subject matters are complicated in nature and the court of law where the matter is processed has to go on record and explain in writing for its reasons to continue with the case[111].

In addition to that Section 16 of the Code of Civil Procedure explains that the matter has to be initiated in the court of law where it was created. Section 16 of the code includes the following point where the case has to be filed where the subject matter exists/orients:

1. Rights related to immovable property (with or without rest)
2. partition of immovable property
3. Sale, foreclosure or redemption of mortgage
4. Analysis of rights pertaining to movable property
5. Allotment for compensation to the movable property
6. Recovery of movable property

It has to be noted that in the case of **Harshad Chiman Lal Modi v. D.L.F. Universal Ltd[112]** the Hon'ble court observed that while interpreting Section 16 of the Code of Civil Procedure it is certain that the competent court is ascertained by ascertaining where the *rex* is situated. The court has no authority to continue with the proceeding where it is not certain where the subject matter arose. In addition to that, the court has the power to grant relief to the Defender if upon initiation of proceedings he/she through a plea requests the court to consider its jurisdictional competency.

[111] Kush Kalra, Emergence of Cyber Crimes: A Challenge for the New Millennium, Bharati Law Review, April 2017, http://docs.manupatra.in/newsline/articles/Upload/4730150C-4A12-4EBA-8CAF-F1146FDD5657.pdf

[112] Appeal (civil) 2726 of 2000

As mentioned in the above paragraph the there can be instances where the subject matter is complicated, thereby the same has more than one territorial jurisdiction. In such a case where there is more than one geographical location where under Section 16 of the Code of Civil Procedure the immovable property/the movable property is associated within then, in that case, the parties have the choice to proceed in either of the locations where the subject matter is associated. This location is decided based on factors such as where the subject matter is prominently related and which place is more convenient for the party who is initiating the suit to access the court of law. In a case where the suit could have been initiated in a different court of law or in other words, there is a multiplicity of territorial jurisdiction, in that case, the court which has taken cognizance of the matter needs to mention its reasons for the same in writing while continuing with the proceedings of the case.

Furthermore in order to comprehend section 16 of the Code of Civil Procedure[113], it can be interpreted as where the damage to the movable property occurred in that place the suit for the recovery of this damage done to the immovable property can be initiated. The same principle applies in case when the movable property or the movable property has been mortgaged. The place of location can be calculated based on the interpretation of facts, as well as where the plaintiff in performance of its contract conducts his business, or other sides in his place of residence, or the place where the contract was breached, deciding factors to calculate the territorial jurisdiction of the subject matter. Interpretation of Section 16 becomes complicated when the subject matter itself is complicated. There are instances when damages have been inflicted upon a movable property or an immovable property through a series of actions. And the series of actions originate from different places of occurrence. The plaintiff has the right to initiate the proceedings in any individual place where singular damage had been inflicted upon. This principle where multiple territorial jurisdictions applies can be explained via the following illustration:-

Rahul is a businessman dealing with the business of furniture. He lives in Bangalore and has employed his helper Ravi to fetch him some raw material from Chennai. Ravi

[113] Source: https://www.indiacode.nic.in/show-data?actid=AC_CEN_3_20_00051_190805_1523340333624&orderno=16

goes to Chennai as per his master's instructions and gets the raw material. While in Chennai, Ravi conspired with the raw material supplier and supplied inferior quality material to Rahul while charging him the money for superior quality material. When Rahul found out about this he had the right to initiate proceedings for recovery of damage from Ravi and the raw material supplier in Chennai and he had the option to file the suit in either Bangalore or Chennai.

The idea behind this section/provision is that it safeguards the interest of the parties involved in the suit and gives them the opportunity for fair representation. There have been instances wherein cases have multiple territorial jurisdictions, then the party which is well-off and the party that can afford good lawyers can harass the other party by initiating cases in multiple jurisdictions, thereby it creates mental pressure and other stresses on the other party. To mitigate this it was decided that one such location related to the subject matter shall be finalized which is convenient for the parties; particularly to the plaintiff therefore multiple cases are not filed related to the same subject matter.

Subject Matter Jurisdiction

Each case is unique in its own way. Once the territory of the subject matter is finalized and the valuation of the suit is analysed it is important to understand what the orientation of the subject matter is. The cardinal principle used to determine the orientation of a subject matter relies on the relief that the party which has been injured or harmed seeks to get from the court[114]. In other words, the type of relief determines the subject matter orientation. For example, the relief sought from the court can be in the form of compensation or restoration of some personal private right of the plaintiff etc. In other words, the plaint which is submitted to the court has the desired relief mentioned in its prayer, thereby the relief soughted enables the court to understand the orientation of the subject matter. Depending upon the orientation of the subject matter the case can be initiated in a specialised court dealing with that particular subject matter. For example, if Ravi bought a pizza from a popular pizza restaurant in the city of Lucknow then upon receiving the pizza Ravi contracted food poisoning then Ravi

[114] Krishchendra Joshi, CPC's Application in Cyberspace, May 2019, https://blog.ipleaders.in/civil-procedure-codes-application-cyberspace/

has the right to initiate a proceeding for compensation from the Pizza Restaurant for delivering contaminated product. So the relief sought from the court is in form of compensation and the same arises from the deficiency of service on account of the pizza delivery restaurant. Therefore the orientation of this particular case is a consumer dispute which has to be preceded in a consumer forum of Lucknow. As the subject matter of the suit is the contaminated Pizza was made in Lucknow and the parties involved in the suit reside in Lucknow and it can be presumed that the pizza was amounting to 1000 Rupees, therefore the district consumer forum is a competent court to hear and conduct the trial of the case.

The above example is a very linear form of a commercial transaction/dispute where all the parties involved in the suit live in the same premise/locality. There are cases where it is difficult to determine the territorial and pecuniary jurisdictions of the subject matter. In the case of: **Harshad Chimanlal Modi v. DLF Universal Limited and Another**[115], the honourable Court pronounced that whenever there is a doubt between the actual pecuniary or territorial jurisdiction then the defendant has the right to initiate a plea before the court to rectify or clarify its competence or territory to continue with the proceedings. However, it has to be noted that such a plea cannot be brought by the defendant in an advanced stage of the trial. Therefore a plea before the court to contemplate its competence to proceed with the case can be initiated by the defendant but the same has to be done in the initial stage of the trial. The Honourable Court while delivering this judgement reflected upon Section 21 of the Code of Civil Procedure which states that any objection regarding the jurisdiction of the court can be initiated in the initial proceedings but the same cannot be initiated in appellate proceedings or revision proceedings. Same rule applies for discrepancies arising from the pecuniary jurisdiction or territorial jurisdiction[116].

Original Jurisdiction

In the language of the court original jurisdiction means the jurisdiction of the court which conducted the proceedings primarily. In the court of law in India, a matter is initiated before a competent court and thereby the competent court after considering the

[115] Appeal (civil) 2726 of 2000

[116] Source: https://www.law.cornell.edu/wex/subject_matter_jurisdiction

various evidences decides the matter in favour of one of the parties. This particular court which has the power to hear the matter for the first time is called the original jurisdiction. In addition to this, the aggrieved party has the right to reach out to the higher court in the hierarchy in order to file an appeal against the order of the lower court. The court which would hear the matter as an appeal would be *de facto* referred to as the appellate court. In this court, the matter is tried for the second time and any appeal regarding the competence of the original jurisdiction, that is the court that primarily took cognizance of the case and issued its order cannot be challenged at the appellate level.

Appellate Jurisdiction

Appellate jurisdiction is the exact opposite of original jurisdiction. This is a court of law that initiates the trial of the subject matter which has already been decided by a lower competent court where the matter is initiated ideally by the defendant who feels that he has been aggrieved. It has to be noted that any new fact cannot be initiated in this jurisdiction pertaining to the subject matter and the discussions that are based on the interpretation of the law. Appellate jurisdiction should not be confused with revision jurisdiction which is only reserved to the court itself whereby the court *suo moto* takes cognizance case where it feels that there have been some deficiencies or shortcomings in the final order of its lower court or even by its own volition.[117]

Analysis of Civil Jurisdiction and its Relation with Cyberspace

The jurisprudence of cyber law in India is at its nascent stage. The main statute that deals with the crimes related to cyberspace has been legislated in the year 2000. Considering the loopholes in the current jurisdiction and with the increase in the number of cybercrimes especially in the forms of civil wrongs or cyber torts, there has been an over-reliance on the Code of Civil Procedure in the trials related to cyberspace in India[118].

[117] Krishchendra Joshi, CPC's Application in Cyberspace, May 2019, https://blog.ipleaders.in/civil-procedure-codes-application-cyberspace/

[118] Yuganter Singh Chauhan, The problem of Jurisdiction in Cybercrime, https://www.vidhikarya.com/legal-blog/the-problem-of-jurisdiction-in-cyber-crimes

Cyber Law as a crime is a borderless crime. It can be initiated remotely from a computer and can target a series of computers including highly secured systems run by governments or multinational companies. While the Information & Technology Act of 2000 explains and covers various cybercrimes and its ramification pertaining to the pecuniary jurisdiction of the subject matter, the same statute fails to deliver a concrete picture regarding the original jurisdiction or the territorial jurisdiction where the offence was executed.

As territorial jurisdiction pertaining to cybercrime is dynamic in nature and the same does not support the idea of a conventional jurisdiction, the courts, in order to process and file the case, depend upon the Code of Civil Procedure in order to decipher the correct jurisdiction arising from the cybercrime. The general principle followed in India when it comes to deciphering the jurisdiction of the crime is that the area where the crime was committed *de facto* becomes the jurisdiction of the crime. This principally is based on the latin maxim *lex loci deliciti* which means that the laws apply where the deceit has been conducted[119]. This principle however does not apply in the case of cybercrime for the obvious reason that the location of the crime varies therefore it has a dynamic jurisdiction. In cases where the dispute is regarding a non-movable property then the principle of law in order to determine the jurisdiction is that the law is where the physical location of the subject matter is situated. This principle is derived from the Latin Maxim *lex situs*.[120]

It is crucial to implement and provide recognition to the foreign judgement and decrees passed during the adjudication of cybercrime as the offence is beyond a fixed boundary of the territory. It is extremely important to safeguard international online transactions therefore recognising foreign judgements by competent courts regarding the subject matter is crucial for the criminal justice administration in India (arising from the same subject matter). This can be understood via the following example, where a citizen in India uses the internet as a medium and buys a product in Canada. The website is registered under the Canadian domain and the product, as well as the seller, resides in

[119] Prevy Parikh and Taruna Rao, Cyberspace and Jurisdiction, https://jcil.lsyndicate.com/wp-content/uploads/2016/07/CYBERSPACE-AND-JURISDICTION-FINAL-PAPER-Prevy-Tarunya.pdf

[120] Soumyo D Moitra, Cybercrime: Towards an assessment of its nature and impact, International Journal of Comparative and Applied Criminal Justice, 28, 2, 2004, p 106.

Canada. The transaction is made and the payment is completed by the Indian citizen but the product was not delivered to the same. The Indian citizen has the right to solicit legal help in Canada and can get the desired relief from a competent Canadian Court. Now the judgement by the Canadian Court requires a part performance of the execution of some provision on behalf of its Indian counterpart then this judgement must be enforceable in India. Under section 13 of the Code of Civil Procedure, it is provided that foreign judgement shall be applicable in India but in cases where the judgement has been pronounced by the court, whereby it vitiates the principles of natural justice, or the court in its capacity was not competent to hear the matter, or where the subject matter involves some aspects or laws which are applicable in India, or where the judgement has been obtained by fraud, then the international foreign judgement/decree shall not be enforceable in India.[121]

The concept of international litigation can be reciprocated in India as well, whereby a citizen of India residing in India commits cybercrime via the online transaction to citizens residing in Canada, then the Canadian citizen can conduct judicial proceedings against the Indian citizen in India. It is mentioned under Section 19 of the Code of Civil Procedure, where it states that any party can initiate a legal proceeding against an individual involved in a fraud involving movable property. Section 19 of the Code of Civil Procedure can be read with Section 45 of the Code of Civil Procedure which empowers the international court to implement our domestic judgements in their country where the subject matter was partly associated.[122]

Chapter 4: Insight into cybercrime in India

Cybercrime in the 21st century has a direct relationship with the digital economy and online transactions which are carried all around the world using the internet. According to a report which was published in 2018, it was found that cybercrime produces 1.5 trillion US dollars in one year. This amount is the estimation of the worldwide transaction whereby it was illustrated by the report that around 500 billion US dollars come from infringement of intellectual property rights and cyber theft of identity and

[121] Yashraj Vakil, "Jurisdictional Challenges – Cyber Crime Prosecutions", The Lawyers Collective, February, 2005, p. 29

[122] Yuganter Singh Chauhan, The problem of Jurisdiction in Cybercrime, https://www.vidhikarya.com/legal-blog/the-problem-of-jurisdiction-in-cyber-crimes

data. More than half of 1.5 billion US dollars that's close to 860 million US dollars are generated from illegal online commerce. [123]

It has to be noted that there is ample proof obtained by independent international media houses in the previous decade that Chinese and Russian intelligence agencies have gathered a comprehensive database of pertinent information, particularly from the US computer systems. This data was obtained by hacking and can be considered as strategic cyber espionage in disguise. To give an example of how technology is used to access critical information is for instance, the face-app which was extremely popular in 2018 and 2019. This application was developed by a Russian company and the service that the app provided was that it converted the photograph of an individual into various permutations of gender and age difference. This app was widely downloaded all across the world as it provided amusement to the general public. The dark side of this application was that it enabled the app to access the images in the gallery of the individual. Thereby it breached the privacy of the individual as the access not only provided the infringement but also enabled the app to keep a copy of the image uploaded on its system[124]. There were similar applications developed by China and other modes of infringement of privacy while using the internet and the world of hacking were incorporated by the same to gather cyber- databases.

Based on the international cybercrime and the various modes and patterns incorporated by the cybercriminals to conduct these crimes it can be comfortably stated that cybercrime can be distinguished into two groups. One group comprises small networks of cybercriminals, the main characteristic that these groups have is that they are dynamic in their membership and they rely on technical assistance pertaining to Information and Technology in order to execute the crime. The other group of cybercriminals confirm as large groups which have corporation like a setup. Here like corporations or corporate companies, there is a hierarchical system in which every organisation has its key purpose and role to execute in the commission of cybercrime.

[123] Garrett M Graff, China's hacking spree will have a decades-long fallout, Wired, 11 February 2020, https://www.wired.com/story/china-equifaxanthem-marriott-opm-hacks-data/

[124] Alice Hutchings, Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission, Crime, Law and Social Change, 62, 1, 2014, p 4

In simple terms, the complicated gang-like setup of a large network of cybercriminals functions on three levels. The first level comprises the uppermost management. They have the financial expertise and the necessary administrative acumen to run an organisation. The uppermost management circle acts as the source of leadership which guides the lower ranks in the execution of cybercrimes. Under the careful observation of the uppermost management circle lays the middle rung of the organisation. These people are the technical mind behind the commission of cybercrime. This category of individuals has the necessary knowledge of Information and Technology which is required for the execution of the crime but they do not indulge in any administration of the crime as they seek instructions for the same from the upmost management circle.

The lowest category in this corporate-like structure of crime comprises people who may not have the technical knowledge regarding the execution of the crime but are considered as the foot soldiers without which the execution of the crime cannot be completed. These people come from a highly vulnerable section of society and accept to do this job due to financial constraints. People who are used as bait often do not even know the scale of the crime nor do they understand the various aspects related to the law which day knowingly or unknowingly breaks in order to earn easy money[125].

The concrete thing which has come out from this type of corporate setup of organised crime is that it has merged diminishing lines between sophisticated and skilled cybercriminals and the criminals who conduct activities on the street. Therefore the gang like set up merges the fine line between cyber dependent and cyber-enabled crimes. The previous decade has seen a rise in the concept of bot-nets which are used to hack computers. This is alarming as a type of crime that required a high degree of skill set and training to execute now has been incorporated with the lowest rung of the society which is extremely vulnerable therefore making this crime highly volatile in its nature.

The bot-nets are basically computer Malware which is software developed by the hacker which upon inserting into the system slows down the computer system and

[125] E Rutger Leukfeldt, Edward R Kleemans and Wouter P Stol, Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis, Crime, Law and Social Change, 67, 1, 2017, p 42

provides breaching of privacy as the hacker can access private and confidential information stored in the computer. Bot-nets can be discharged or dispersed in a number of computers using the internet; therefore it does not require human intervention for its execution. It saves time as well as it is cheaper to execute. According to a report, in order to execute an activity of hacking while using a bot-net, the cost comes down to room 0.10 US Dollars per system. Hiring an individual to conduct a telephone call and making the victim fall into a trap of phishing costs around 1 to 5 US dollars and it also makes the operation vulnerable as tracking of the individual who is trying to phish becomes susceptible to the criminal justice administrator. According to a report which was published in 2019, stated the number of bot-net intrusions which were conducted in India and when tracing the internet protocol address it turned out that it was launched from the Central European region (countries such as Czech Republic, Poland).[126] On deeper analysis it was found that although the bot-nets were executed from Central Europe they manage from countries in South Asia. It can be presumed that the volatile relationship between India and Pakistan with the history that the countries have pertaining partition and disputed land of Kashmir, it is highly plausible that the South Asian countries involved in conducting strategic surgical operations in India may include Pakistan. The surgical operations involving the breaching or hacking of systems becomes extremely difficult to trace as the bot-net does not leave a trail and it becomes extremely difficult to trace from where the bot-net was launched thus making the whole operation of the crime discreet.

The amalgamation of different types of criminals and the diversity of the cyber offences was reflected in an well-articulated British Law Journal[127] as following:-

" If I wanted to get involved in fishing a bank or something that everybody knows but I don't know how to write the actual page someone will write it for me and reasonably cheaply I can ask them to do it. and if I am not to show how to host it they will host it for me on one of the boats for part payment. and if I don't want to get involved in cashing out and receiving the money because that's a little bit too risky there are guys

[126] E Rutger Leukfeldt, Edward R Kleemans and Wouter P Stol, A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists, Crime, Law and Social Change, 67, 1, 2017, p 29.
[127] David Décary-Hétu and Benoit Dupont, Reputation in a dark network of online criminals, Global Crime, 14, 2–3, 2013, p 177

*doing cash-out services all over the world who you can talk to and meet online. There is a whole **community** out there of thousands of people that can solve any one of the problems online or make any link of the chain if you don't want to get involved."*
(**Emphasis supplied**)

The word community mentioned in the aforementioned paragraph elucidates the professional experts involved in information and technology who take care of the tactical execution of the offence[128]. In other words, it basically points out to the middle rung of the organised cybercrime setup that is mentioned as a community. These professional individuals have the technological know-how which is sent back by the infrastructural paraphernalia provided by the topmost management circle and based on the guidance and brief regarding the execution of the cybercrime from the utmost management circle these hackers execute the offence. It's always widely published in popular media the hackers of Eastern Europe are more sophisticated when it comes to execution of the crime and the type of crimes that they execute is cyber dependent in nature. This is due to the fact that the Eastern European region had the influence of the Soviet Union this gave them a strong foundation of technical literacy and post the fall of the Soviet Union and the rise in capitalism the Eastern European countries they (local government) failed to provide sustainable good governance[129] therefore these technically sound young men decided to use and knowledge for the purpose of cybercrime.[130] There have been articles on the Eastern European hackers which state that they are said to be linked with intelligence agencies run by the government(s) which help them get information which they cannot pursue themselves as pursuing the same would attract international scrutiny.

[128] Alice Hutchings, Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission, Crime, Law and Social Change, 62, 1, 2014, p 11
[129] Shweta Punj, Welcome to jobless growth: Why India is facing an unemployment crisis, India Today, 20 April 2016, https://www.indiatoday. in/magazine/cover-story/story/20160502- employment-scenario-job-crunch-joblessgrowth-economy-828782-2016-04-20
[130] Srinath Srinivasan, Cyber Security: Are IoT deployments in India safe from hackers?, Financial Express, 19 August 2019, https://www. financialexpress.com/industry/technology/cybersecurity-are-iot-deployments-in-india-safe-fromhackers/1679046

Table 3: Hierarchical structure of a large cybercriminal network

UPPER MANAGEMENT: CORE LEADERSHIP

• Responsible for administration and the movement of large funds.

• Experienced in financial crime and money laundering.

MIDDLE RUNG: 'ENABLERS'

• Responsible for providing technical and informational support.

• The only rung that requires advanced computer skills to steal data remotely or handle other technical aspects of a cybercrime

LOWER RUNG: 'FOOT SOLDIERS'

• Responsible for handling the operation's external interface.

• Members could be 'money mules' or call-centre employees, but have to do whatever they have been told to do.

In an article published in the year 2000 it is mentioned that;-[131]

"Crime gangs are starting to actively recruit skilled young people into cybercrime. They are adopting KGB style tactics to recruit high-flying Information and Technology students and graduates thereby targeting computer society members, students of specialist computer skills schools, and graduates of Information and Technology courses"

One has to keep in mind that despite there seems to be a link between the organised and unorganised sectors of crime especially involving the domain of the internet it cannot be presumed that such a conjoint intervention exists universally. In the year 2000, a

[131] Rob McCusker, Transnational organised cyber crime: distinguishing threat from reality, Crime, Law and Social Change, 46, 4–5, 2006, p 265

mafia group from Italy attempted to scam a bank with the intention of prodding the funds from European Union accounts into 400 US million dollars. This crime operation was not successful as an informant who was part of the mafia group provide information regarding the operation and the personal details of 20 inside hackers involved in the offence. In the year 2019, another case was reported in the Eastern European region where a criminal conglomeration breached a security system called GozNym (The name is an acronym derived from the combination of Nymaim software and Gozi ISFB banking trojan virus). This conglomeration was proficient in information and technology and conducted the coding activities as well as the planning of the offences by using the Russian language as the mode of communication. The investigation is still going on regarding the uppermost management circle of GozNym as they are the think tanks as well as the financial recruiters of cybercriminals who are a part of GozNym[132].

Case Study of Shailesh Kumar 'Sam' Jain and IMI

Shailesh Kumar 'Sam' Jain was an Indian immigrant who was residing in the United States of America. During his youth, Sam Jain was involved in petty offences. He was arrested when he was 21 as he was attempting to open a fraudulent bank account by using fake documentation. When he was interrogated by the police who said that he lived his life by the moto, '*either I can screw the society or he can be screwed by the world*'. Shailesh Kumar 'Sam' Jain became a Federal Bureau of Investigation most wanted criminal after he was involved in the 9/11 terrorist activities in which a passenger aeroplane was hijacked and later crashed in the World Trade Centre Building, New York[133].

As the internet became more user-friendly and people bought personal computers in America, Shailesh Kumar 'Sam' Jain along with Information and Technology expert Daniel Sundin started a technology company together which dealt in making antivirus protection software for personal computers. The software was mainly targeted to countries where their exponential growth potential of internet-users. Therefore the

[132] Jonathan Lusthaus, Trust in the world of cybercrime, Global Crime, 13, 2, 2012, p 84
[133] Benjamin Wallace, How Two Scammers Built an Empire Hawking Sketchy Software, Wired, 27 September 2011, https://www.wired. com/2011/09/mf_scareware

software company targeted countries like the United States of America, Argentina and India as prime targets. The headquarters of the software company was situated in Ukraine from which the daily operations were conducted by Shailesh Kumar 'Sam' Jain. The country of choice is selected as Ukraine because it had the desired loopholes in the criminal justice administration system which was exploited by Shailesh Kumar 'Sam' Jain and his business partners. Alongside it had a good base of educated technicians who were proficient with information and technology; therefore, they were able to work for the company for less amount of money compare to the same technician who would have been hired at the company was operating from America. The company which was set up by Shailesh Kumar 'Sam' Jain and called it **Innovative Marketing Inc** and slowly it became one of the best-performing companies in Ukraine. The technical support was provided from the country of Ukraine with citizens who were having good knowledge of Information and Technology mathematics and Science while the day-to-day operations of the same were conducted from India through Call Centres where labour was even cheaper to hire.[134]

The basic operation of the company was based on fraud. The company used to provide software that can be installed by the consumer in lieu of it being an antivirus. In application the antivirus provided by IMI was the malware which was eventually used to slow down the personal computer that limited the personal computer performance and the PC could not operate. When the consumer used to call the tech support call centres in India, the customer service executive is used to advise them to uninstall all the legitimate but outdated antivirus programs currently installed on the personal computers.[135] When the consumer used to oblige the advice of the customer service executive the same (consumer) cease to get notification regarding any malware operation/any Trojan attack which has been already inflicted on their computer systems. After the conversation with the customer service executive and the consumer of the antivirus program successfully and installing the partially working good

[134] Jim Finkle, Inside a global cybercrime ring, Reuters, 24 March 2010, https://www.reuters.com/ article/us-technology-scareware/inside-a-globalcybercrime-ring-idUSTRE62N29T20100324

[135] Andy Greenberg, Global Takedown Shows the Anatomy of a Modern Cybercriminal Supply Chain, Wired, 16 May 2019, https://www.wired.com/ story/goznym-takedown-cybercrime-supply-chain.

antivirus, he did not use it to get any notification regarding any cyber-attack on the personal computer. The customer used to feel that after the advice the computer was working fine as it was not showing any notification of an attack, therefore the consumer used to become callous and continued using the fraudulent malware application provided by Shailesh Kumar 'Sam' Jain company.

Shailesh Kumar 'Sam' Jain sold millions of software in a short span of two to three years. The majority of the sales in computers are all about marketing, and Shailesh Kumar 'Sam' Jain knew how to market the software. Atlas peak his revenues were 180 million US dollars while he paid 0.10 dollars to the hackers for acquiring the computer system. Legitimate business sources used to pay somewhere between 2US dollars to 5 US dollars to acquire its customers. Although it seems that Shailesh Kumar 'Sam' Jain did not get much profit as he was only paying 0.10 US dollars but it is seldom about how much money a person makes on these crimes involving personal computer system as these faults/crimes are meant to penetrate deep into the society and affect a number of individuals living.[136]

Shailesh Kumar 'Sam' Jain and Sundin abandon the company that they established in the year 2009 and start living as fugitives while the hundreds of employees who worked for them in Ukraine lost their jobs. An interview was conducted on a number of employees who were working for Shailesh Kumar 'Sam' Jain and it turns out that many did not even have the slightest idea regarding the frauds being conducted in broad daylight.

Origin of Cybercrime in India

Cybercrime in India began with the IT revolution which came into the country around the turn of the century. In order to understand the development of cybercrime in India, it is important to understand how cybercrime unfurled in Russia and the Eastern European countries in the decade of 1990s as they are the minds behind the foundation of Cybercrimes in India.

[136] Benjamin Wallace, How Two Scammers Built an Empire Hawking Sketchy Software, Wired, 27 September 2011, https://www.wired. com/2011/09/mf_scareware

In 1990 after the United Soviet Union was dissolved, a new era of capitalisation and privatisation started in Russia. Russia as a country had educated people working in the sector of Information and Technology and they were back in the day pioneers when it came to computer technology. Suddenly it became extremely difficult for educated youth to get employment in Russia as capitalisation brought in an open market which made it difficult for the youth to get employment in western countries because of the ongoing competition. Urbanisation and the rising costs of day-to-day life propelled the educated youth in information and technology to take the road of cybercrimes in order to make a legitimate earning. Back in 1998, it was calculated that a person working in the cyber industry was probably indulging in cyber crimes and could earn 10 times more than traditional careers which were popular in Russia. It has to be noted that while the ten times exponential income is extremely lucrative it cannot be compared with the remuneration obtained by Silicon Valley engineers working in computer science in America.

As the Western European society improved in its socio-economic parameters the youth in Russia also wanted something better from themselves rather than providing the basic minimum which they were entitled to by the government under the Soviet Union. Internet usage in countries where there are highly skilled individuals who had knowledge in information and technology including mathematics and computer science coaxed them to take the path of cybercrimes as it was one of the quickest ways of making money and providing a better future. The reason for indulging in cybercrime was that it was extremely difficult to be traced by the law enforcement agencies back then as the phenomena of the internet was extremely novel. Consumerism and capitalism were the major factors that propelled the thinking of the youth to indulge in criminal activities and to use their knowledge for some bad activities pertaining to society. The crimes committed by such empowered youth were cyber-enabled in nature and later on went on to be the masterminds behind cybercrimes in developing countries[137].

[137] Diego Gambetta and Steffen Hertog, Engineers of Jihad: The Curious Connection between Violent Extremism and Education. Princeton: Princeton University Press, 2016, pp 44–50.

In 1991 India opened its gates for foreign direct investment in India and it was regarded as one of the most crucial economic reforms made in independent India. We suddenly saw a fleet of international companies coming to India as the labour market booked cheap and highly skilled technical individuals to work for the multinational companies. Post the 1991 reforms India has experienced exponential growth and the same can be seen in the infrastructure and development in the country. During the early 2000s, India was often compared with China and the growth was projected to be similar to the Chinese exponential growth and talks had made that India should also be made a permanent member of the Security Council just like China as India is an equally powerful Asian supergiant. However, things were different in reality as the Indian growth model was growing but was not successful or sustainable. After the global recession of 2008 and 2009, the Indian GDP suffered and was reduced to a single digit. Earlier it was projected to match the numbers of Chinese GDP by the year 2012. One of the biggest failures of the 1991 economic reform is that India was not able to create a strong and sustainable base of manufacturing. India is the home for the most number of youth in the world but our youth is not technically skilled and lacks the general know-how of conducting vocational training. According to the census done in 2011 less than 3% of Indians are trained in any kind of Technical training compared to the Global average which is somewhere between 60 to 70%. Indian economy in 2019 is still has an agrarian base which is alarming as we were once projected to be the world's tech giants. The Indian growth was an illusion as it was largely based on the foreign direct investment made by people strategically investing in Indian corporations[138]. It is to be understood that when a foreign direct investment happens in a country it does not invest in the areas where the country mainly needs help, for example, health infrastructure, transportation etc. In a foreign in a country like India they (FDI investors) invest keeping their interest in mind. For example if a company like Vedanta set up of a mineral plant in Orissa they develop the area not to uplift the tribals living in that area but for the smooth functioning of the day-to-day operations of the company. Therefore when the foreign direct investmentor decides to abandon the business the local areas

[138] Nir Kshetri, The Global Cybercrime Industry. Cham: Springer, 2010, pp 178–179.

who were getting the benefit of infrastructure suddenly go back decades in development as there is no investment of money in order to maintain the infrastructure created by the foreign direct invest mentor. Such investments cannot act as a substitute to the municipality of the government elected by the citizens of India[139].

India is home to 111 million people living under the poverty line. This figure is extremely big and can be understood from the context of the United States of America, as the number of citizens living in America is equal to the number of people living below the poverty line in India. It's just not the 111 million people living under the poverty line in India who are poor and vulnerable; the vast majority of people who are just above the poverty line but are educated yet they are deprived of social benefit schemes under the Government of India also form a niche of highly vulnerable individuals. These individuals are educated and part of modern India who has access to the internet on a regular basis. They want a certain sense of entitlement which they have seen while using the internet and they feel that somewhere their education and the background is one of the impediments which is stopping them from finding possibilities in life. The 111 million people living under the poverty line in India comprise 28% of the global population of the world's poor. These people live in conditions of chronic poverty and are suffering from generations regarding abuse from society. The section of society that is just above the people who are below the poverty line use the fear of falling into chronic poverty as one of the motivators in order to work hard to achieve a better life. In the quest of achieving a better life these people often take part in ventures that they should not have taken a part off as such decisions lead to cybercrimes or crimes in general. It is to be noted that these individuals are educated youth of this country who are proficient in information and technology and can conduct activities such as hacking. They are basically used by the Russian or Eastern European hackers as foot soldiers which create large scale cybercrime activities in India. The people who live below the poverty line do not get proper access to criminal justice administration

[139] Thomas J Holt, Olga Smirnova, Yi Ting Chua and Heith Copes, Examining the risk reduction strategies of actors in online criminal markets, Global Crime, 16, 2, 2015, p 83.

agencies therefore they are highly vulnerable as they are convenient targets for the cybercriminals to create micro-level scams on individuals.[140]

The section which was empowered enough to receive education could not provide better circumstances for themselves as a social benefit schemes were not available to them; there was always the fear of falling into the deep roots of poverty. In India, there is poverty in general but what lies uniquely as an intricate aspect of poverty in India is its generation property.[141] A person is under chronic property for a number of generations; therefore falling in the trap of poverty is extremely dangerous as it is extremely difficult to come out of it. In order to quench the desire for entitlement and the worldview that they had seen through the internet the Indian educated youth decided to be a part of revolution starting in the decade of 2000 for the main purpose of getting themselves unemployed which would ensure that they do not fall into the trap of poverty[142].

There were a lot of jobs that were created by the IT industry when it came to India. The idea behind creating all these jobs is that the Indian market was cheap to hire and they have educated youth who were proficient in the language of English and they could represent the company properly to the Western clients. The people who seek jobs in the IT industries (initially in early 2000s) are those individuals who did not have high amount of Information and Technology knowledge but they had a basic level of literacy and the new language of English which helped them get these multinational companies jobs (particularly in the call centres).[143] Between 1998 to 2005, there was a growth of these IT jobs in India which increased from 1.2 to 10% contributing to the Gross Domestic Product growth of India. It was significant to see the rise in call centres and IT companies in India due to the fact that during the year 2000 and 2001 the American

[140] Nir Kshetri, Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers, Crime, Law and Social Change, 60, 1, 2013, pp 47–48.
[141] Amitendu Palit, Dragon in the Elephant's Backyard: Chinese Imports in India's Mobile Revolution, Pacific Affairs, 85, 3, 2012, p 545.
[142] Sourav Majumdar, Data and the new India, Fortune India, 6 November 2018, https://www.fortuneindia. com/opinion/data-and-the-new-india/102658.
[143] Ian Jack, India has 600 million young people – and they're set to change our world, The Guardian, 13 January 2018, https://www.theguardian.com/ commentisfree/2018/jan/13/india-600-millionyoung-people-world-cities-internet.

companies suffered a recession which was followed by a lay-off in which hundreds of thousands of people were without a job as they could not pay according to the basic minimum pay package of the western standard. Therefore companies who were operating in multiple nationalities had to look for cheap labour options in order to continue their day to day transactions. It should be noted that the collapse of the American IT industry led to the creation of new jobs and prospects in information and technology in India. India went on to take this opportunity where educated youth lived; basically in cities off Bangalore Mumbai, Pune and Chennai - the cyber industry was established while the north and the northeast of India remained fairly aloof from this cyber boom. The major reasons for the non-involvement of the north and Northeast of India in this type of boom was the fact that the people were not too efficient in the language of English which was one of the modes of communication and the north of India lacks in the literacy rate when compared to the southern cities. The sole exception was the megacity Calcutta which is on the banks of the holy river Ganga in the state of West Bengal.

Therefore to summarise how the cyber boom happened in India was due to the economic reforms in 1991 which invited foreign companies to invest in India. During this, the subsequent dissolution of the United Soviet Union and the emergence of capitalism and consumerism in Europe particularly to the east and Europe dealt with the rise of cyber activities in the world. It should be noted that the citizens living in Eastern Europe and Russia were poor people but they were technically qualified in computer science and information and technology. It has to be noted that the youth of Eastern Europe indulged in activities including the cyber crimes in order to get easy money. As they were technically sound to use than knowledge for the wrong activity. The Eastern Europeans were more inclined to use this technology for the bad of society as it was the easy way out to earn more money. They wanted a better sense of entitlement of life. The sense of entitlement was evolved by the usage of the internet when they came to know about the western standard of living and they felt extremely bad regarding their own living conditions and social benefit schemes provided by their governments.

As companies started to invest in India it was observed that in the year 2001 the market recession in America led to the transfer of the labour industry to India where they were

educated Indians willing to participate and help out the foreigners. The section of society which served in the information technology industries early on was established in India with basically a chunk of the society who was educated but was extremely vulnerable as they did not get any relief from the government and they were prone to chronic poverty. It should be noted that here the educated youth in India was not technically educated in computer science-mathematics or information and technology but they had basic primary education which made them a cheap labour market for the western companies to hire in order to conduct their day to day activities. These employments were of a contractual nature and at their peak used to provide a million jobs to the citizens of India.[144]

Indians who were administered in these jobs received a sense of security and entitlement from the recruiter. They were somehow living the oriental version of the American dream by working for an American multinational, during the working hours which were functioning during the transactions in America. The traditional jobs which were available from the basic education (conducted by the target groups who were employed under IT job) when compared with the multinational companies' jobs felt that the IT jobs were far more satisfying than the traditional jobs. As the traditional jobs did not provide an element of excitement, thrill and independence (like working in a big city and for a big company).[145]

For the ambitious Indian youth who got a job at a call centre while working for a multinational company which was situated in the United States of America seemed like he/she had won a golden ticket in order to get a visa for the United States of America. The Indian youth thought that while working for the company they will get the requisite amount of experience which then they can later use in order to procure a good job in the United States of America. One has to understand how the thinking has changed within one and half decades, while before 1991 there were no such activities conducted in India and the very thought of going abroad was considered extremely far-off and can be

[144] Ian Jack, India has 600 million young people – and they're set to change our world, The Guardian, 13 January 2018, https://www.theguardian.com/ commentisfree/2018/jan/13/india-600-millionyoung-people-world-cities-internet.

[145] Puja Mehra (2 April 2016). "8% GDP growth helped reduce poverty: UN report". *The Hindu*. Retrieved 16 August 2017.

only executed by the super-rich. The transition happened within fifteen years wherein the basic common denominator, the common man of India could imagine their future in the United States of America and this was due to the boom of Information and Technology companies in India. The idea of a Boston education or western employment was considered delusional by society[146].

The democracy of India was divided into the egalitarian society which was educated and the society which was not educated and was in a deeper rut of poverty. The egalitarian divide was utilised by the foreign direct investment as it targeted the educated Indian who was proficient in the language of English to be part of their employment/companies. As per the situation this was too new for India to understand regarding the scale of magnitude of this IT innovation. The society was divided into two parts where the traditional families could not fathom the range and the scope of the IT application of these companies while another section of the society which was far more enterprising in nature decided to take a chance and take a job with unconventional nature in order for greener prospects in near future which was likely immigration to the United States of America. In the next 15 to 20 years in which information technology companies have been working in India, we have seen a change in the reception of Indians towards the same companies when it comes to employment.

Table 4: Chronology of Development in the Jurisprudence of Cyber Crime in India

Year	Chronology
Early 2000	**A time of unrestricted capitalism. India is presented as 'the next China'. There is a misguided expectation that call-centre dealings with Western clients will be harmonious.**
2001	**Low-wage jobs relocate to India, with its large, English-literate labour force. BPO units set up call centres in Bangalore, Hyderabad, Pune, Mumbai, Gurugram and Noida.**
2005	**Reports surface of abusive clashes between Indian call-centre**

[146] https://sinhaprats.medium.com/story-of-indias-it-review-of-book-the-outsourcer-567bd44718df

	employees, and US and UK customers. The first cases of cybercrime from India targeting US and UK nationals begin to appear. **The national crime rate sees a marked increase over the next decade. The economy is slowing down, and after brief prosperity, many IT/ITes workers experience a sudden loss of status. This sets the scene for entrepreneurial criminality**
2008	**Many call-centre workers hoped to use their limited exposure to the West as a springboard for emigration. These dreams are shattered following the 2008 global economic crisis. BPO contracts begin to dry up.**
2010	**Growth projections for Indian IT/ITes firms drop considerably, and firms have to lower recruitment standards. Many US companies relocate their operations to countries like Malaysia and the Philippines. Cybercrime in and from India appears to increase and become more organized.**
2011	**Turnover rates among demoralized call-centre personnel are now as high as 60%. A lack of fresh Western contracts reduces the incentive to enforce regulatory standards. A new start-up industry appears, built from the debris of the off-shoring boom and focused on scamming**
2012-2016	**One of India's biggest and most successful scams unfolds in the city of Thane, on the outskirts of Mumbai. This would become known as the Mira Road scam.**
2016	**A landmark development occurs on 8 November, when the Indian government withdraws 86% of all currency circulating in the economy overnight. Many households turn to digital payments. This, in turn, leads to a spike in cybercrime.**

2019	**The level of cybercrime has increased by 700% since 2015. A new QR code scam emerges in south Indian cities.**

Hotspots of cybercrime in India

During the turn of the century when information technology companies had been established in India the target cities were those with demography citizens were educated and proportion to the English language users. This criterion was set as the companies did not require employees to be educated in Computer Science or information and technology, as their job did not require any technical aspects of Computer Engineering such as coding etc. The employee's are customer services executive who are required to speak in fluent English to the western customer. The conditions of employment was that the employees had to work during the night-time in India as that was a working time in the United States of America (who was perhaps the main recruiting country).[147] Therefore cities like Bangalore, Chennai, Pune, Hyderabad became the instant hotspots where the companies set up their subsidiaries. It is to be noted that slowly the penetration of these companies increased in the northward direction as well. But this was gradual in progression as the North of India is slightly less literate when it comes to the southern megacities. Calcutta is the exception in northeast India as it was a hub of information and technology companies recruiting customer service executives. Later on these agencies served as data points where cybercrime was conducted initially. The belt of Uttar Pradesh, Bihar, Jharkhand, and Uttrakhand in India was devoid of such foreign direct investment as the demography lacked the prerequisites required for employment[148].

The earliest pattern that can be seen in cyber crimes in India can be associated with the city of Delhi and Gurgaon. One of the factors that were involved is common in these two cities, in particular, was that the citizens who were taking part in these companies had access to confidential data which was shared by customers (these customers include

[147] Suchi Kedia, Sriram Gutta, Terri Chapman and Vidisha Mishra, Here's what young Indians really want from life, World Economic Forum, 5 October 2019, https://www.weforum.org/agenda/2018/10/here-s-what-young-indians-really-want-from-life/.

[148] Ben Crair, Maniac Killers of the Bangalore IT Department, Bloomberg, 15 February 2017, https://www.bloomberg.com/news/features/2017-02-15/ maniac-killers-of-the-bangalore-it-department.

both Indian nationals as well as people living overseas) and the X-factor behind the crime was the language Hindi which bound three fourth of India together. The combination of a common language that can be used to influence the common citizen of India alongside certain information makes their pitch highly credible while conducting the cybercrime involving the method of phishing. Therefore the confidential information shared by an alleged concerned employer made the victim believe in him therefore he went on to share private information such as banking and personal security numbers which was not meant to be shared in the first place to the cyber abuser. Hindi language is the main language which is spoken in India, whereas there are 22 other recognised languages as well, but these languages are spoken by a relatively smaller size demography hence the choice of language to conduct the offence was fairly convenient with the Hindi language[149].

As mentioned above, the Indian Information Technology industry boomed in the year 2000 and the Indians could see a version of an American dream where the working class could imagine immigrating to America and working in America. To understand that the psychology behind such migration was generations worth of discrimination and struggles which made them believe that the American society is better as public benefit schemes provided by the American government is far superior to what is provided in their country that is India[150].

Such hopes of the American dreams were shattered by the global crisis which happened in the year 2008. In the year 2008, there was a global crisis as the markets fell into recession, India primarily perceived this recession on the grounds of the 2001 recession as it saw an onset of new opportunities, whereby a whole IT industry was created in India, but the 2008 recession had different repercussions. Instead of more work flowing in the country which provided cheap and educated labour to foreign direct investment and multinational companies, the jobs which were prevalent in this country started to dry-up.

[149] Source: https://www.hindivarta.com/cyber-crime-in-hindi/

[150] Mihir Sharma, India's burgeoning youth are the world's future, LiveMint, 8 September 2017, https://www.livemint.com/ Opinion/2WSy5ZGR9ZO3KLDMGiJq2J/Indiasburgeoning-youth-are-the-worlds-future.html.

It was such that companies which were prevalent in India between 2001 to 2006 and companies that provided an annual growth rate of 40% could barely manage to provide a double-digit growth rate post-2008 to 2010. The decline in the growth rate of these companies eventually persuaded their Masters who were situated overseas to try to conduct a different recruitment market for employment rather than employing Indians for customer service executive. There was a time in Hyderabad which is documented by a well-known journalist in India where people who worked in the information technology industry as computer engineers could not repay loans from the banks as the banks were not convinced by the profile of the individual's company and it was thought that they would be likely to lose their job. Loans were provided to information and technology workers at a high percentage while other sector employees were provided with the same at a lower rate percent.

Keeping aside the economic crisis with the information technology workforce, IT personnel were also subjected to racial and ethnic abuse by the customer's calling from the United States of America. The racial and ethnic abuse was also an underlying cause which propelled Indians to take part in two minor Hawala scams in order to make even against the racial abuses. The underlying cause of racial abuse was due to the stress in the society caused in the United States of America as a number of jobs were lost as cheap labour markets were explored by the recruiters especially in Southeast Asia. Asian abuse or racial abuse is not a new concept in the world but however, in the rise of internet usage, it was pretty common to come across such abuse on a daily basis.[151]

Before we understand the range and reasons for Asian abuse we have to understand that the Indian who was employed by the multinational company comes from which background. The Indian background is often very humble but comes from rich history which includes the history of culture as well as the history and values of family. For Indians who once graced the civilization with extreme wealth and prosperity, were slowly looted by the colonization which resulted in the pathetic condition of India economically. The first reports of clashes between the customer service executive and

[151] Suchi Kedia, Sriram Gutta, Terri Chapman and Vidisha Mishra, Here's what young Indians really want from life, World Economic Forum, 5 October 2019, https://www.weforum.org/agenda/2018/10/here-s-what-young-indians-really-want-from-life/.

the overseas customers mainly from America and Britain came in the year 2005. The language barrier was removed when English was chosen as the mode of communication but there was an issue of dialect which used to always hinder the understanding of the conversation. The overseas customers made fun of the Indian dialect and accuse Indians of stealing the jobs which were once provided to the American citizens. Things escalated as there were websites which provided abuses and slangs in the Hindi language which were made accessible to the American and British customers and then they used to abuse during the call which was extremely demoralizing for the customer service executive[152].

During the early days of such abuse, the customer service executive were advised not to react at the explicit remarks made by the customers and to treat the abuse as normal daily activity in the job. But as the abuse went out of hand the Indians started to retaliate by either engaging in a passive-aggressive conversation or simply hanging up the phone which was earlier considered as a forbidden activity. The world most famous incident that happened in 2005 regarding racial abuse when a radio station in Philadelphia made a call to a Indian call centre and much to the amusement of the radio presenters the caller addressed the woman with demeaning abusive words and American slang. During this time the bilateral relationship between India and America was under-pressure as the bilateral nuclear treaty was being negotiated between the two countries, however even after the treaty was signed, a certain human to human contact and abusive treatment of Indian citizens by the Americans was never discussed by the top authorities of either government. An independent study was conducted by a print media company and it pointed out that around 60% of employees working in the information and Technology Sector including the call centres faced racial or ethnic abuse in some way or form in the year 2011[153]. The study went on to show that the relationship of Indians with the call centre company was perceived by the employees as the relationship their ancestors had with the colonizers. Such as the boss used to trivialise the bottom layer working for the company and the white man and the

[152] Source: https://scroll.in/latest/859397/indian-call-centre-workers-face-racial-abuse-frequently-finds-study

[153] Source: https://economictimes.indiatimes.com/jobs/abuse-and-stress-what-indian-bpo-workers-have-to-undergo-on-a-daily-basis/articleshow/61806162.cms?from=mdr

company was run by brown *Sahebs* who were Indians but in the capacity of the job they will not be empathetic towards the Indians. The inadequate pay and the lack of job security made the Indian who was working in the Information and Technology sector feel demoralized and vulnerable.[154]

The American recruiters also analyse the market and they felt the Indian recalcitrance towards the IT sector but instead of solving the problems arising from racial abuse the American recruiters decided to shift their labour market from India to Malaysia and Philippines, where the population was more globalised than India.

Cyber Crimes in Bangalore

Bengaluru was one of the main cities which was used as the information technology hub by the recruiters and prevalence in educated English speaking youth seeking employment at call centres and companies dealing with information and technology. According to a media report, it stated that the growth of Information Technology was around 10% per year between 2000-2003. With the increase in the number of job prospects around information technology online fraud started to be conducted as well. In the year 2005, there were 3500 companies in Bangalore which included 750 multinational companies. In 2005 Bangalore reported around 30 Cybercrimes per day and roughly around 4,000 cybercrimes per month. To tackle this rise in the number of cybercrime particularly located in the city of Bangalore the law enforcement agencies had only 20[155] working personnel and one office vehicle as infrastructure[156]. The hackers knew about the difficulty of the law agencies to trace them due to the lack of strict laws in India dealing with cyberspace and the lack of human resources as well as physical infrastructure to deal with the rise in the number of cases pertaining to cyberspace. However, the number of cybercrimes conducted in one month in Bangalore should not discourage as Bangalore was regarded as one of the safest city when it

[154] Source: https://ubiquity.acm.org/article.cfm?id=1119623

[155] Aishwarya Rakesh, Just 20 constables to tackle 4 000 cybercrime cases, Deccan Herald, 28 June 2018, https://www.deccanherald.com/ city/top-bengaluru-stories/just-20-constablestackle-4000-677553.html.

[156] There was one case, in June 2006, where payment information of British customers of HSBC bank was sold by an employee of HSBC's Bangalore call centre. However, subsequent references to the city in media reporting on call centre scams have been noticeably rare. Miles Brignall, HSBC call-centre man held over data theft, The Guardian, 28 June 2006, https://www.theguardian.com/ business/2006/jun/28/accounts.money.

comes to cyber jurisprudence or cybercrime; it was when the epicentre of the IT industry shifted from Bangalore to Gurgaon and National Capital Region, that's when the proportion of cybercrimes went berserk. The unemployed educated youth found the medium of cyberspace as an ideal medium to conduct a crime, including activities of fraud and stalking because chances of them being chased by the police were minimal.

Citibank Fraud from Pune

Explain from the above paragraph there was a prominent atmosphere of abuse which made the Indian service provider extremely demoralized and it somehow fuelled his desire to conduct the crimes associated with cyberspace and this particular Citibank Fraud developed from the same repeated abuse of Indian Call Centre employees by the overseas customers. In 2005 the employees of Call Centre working on behalf of Citibank were able to transfer 500000 US dollars into their accounts by using the confidential information provided by the customers. In addition to that, there were instances when information such as credit card numbers was manipulated by the employees to use for *mala fide* intention. After the Pune City Bank fraud was conducted, an independent investigation was conducted by a British agency and it was held that the accounts which were breached by the hackers provided an amount of 5.5 Dollars per individual account which was breached.[157] The hacking activities seem to be a multinational activity where the middle tire hacker was in India and the human contact was between the hacker and the customer who was situated overseas but the mastermind behind the whole activity remained untraceable. Due to the activities, the Indian corporations formed the **National Association of Software and Services** which is the controller body when it comes to the standard guidelines of internet usage software management and services in India. The National Association of Software and Service established a subsidiary called the **Data Security Council of India** which is the regulator organisation when it comes to data protection. This organisation shows that industry-standard parameters have been adhered to when it comes to data protection by both the national recruiter as well as the overseas international customer.

[157] Source: https://www.business-standard.com/article/current-affairs/12-booked-for-involvement-in-selling-dormant-account-data-worth-rs-216-cr-121031700112_1.html

There is a stark difference between cybercrimes committed in India and that which originated in the Eastern European region. The Eastern European cybercriminals are better technically sound youth who had prior knowledge of Information and Technology. It differs from the situation in India where cybercrime is conducted not as a form of subaltern resistance within the section of society but as a form of resistance arising due to the abuse received online. Due to the lay-offs in the field of cyberspace as the jobs were made redundant after the 2008 recession the technically qualified individuals went back to their home cities from the cyber hub that they were working from. When back in the home town there was a lack of employment[158] and individuals who were once employed by the call centres indulged in low-level Cybercrimes. Journalist Snigdha Poonam[159] conducted a series of interviews of unemployed youth who were once part of the call centre Boom and she observed that the youth lived in a dystopian world and they did not have any future prospects and set section of society is the biggest target as cyber victims as well as the most vulnerable victims of a big scam.

The article was written by her to elucidate that while taking employment a certain section of the educated youth of a country (India) is so desperate that he does not even care whether a certain part of the transaction or certain part of the course of their employment is unethical or unlawful in nature. Therefore the employee does not ask questions to the recruiter and has no fiduciary relationship with the customers in the business as well. Therefore these grounds make it extremely ideal to conduct low key level cybercrimes which are less sophisticated in nature when compared to the Eastern European cyber abusers. The victims of crime in India are extremely vulnerable as they take part in the operation of the cybercrime in itself and due to the lack of knowledge they give private and confidential information to the hacker thereby being a part of the crime as well. The level of sophistication in Indian cyber crimes without being targeted

[158] 94% of engineering graduates are not fit for hiring, says this IT stalwart, Times of India, 4 June 2018, https://economictimes.indiatimes.com/jobs/only6-of-those-passing-out-of-indias-engineeringcolleges-are-fit-for-a-job/articleshow/64446292. cms?from=mdr.

[159] Snigdha Poonam, The scammers gaming India's overcrowded job market, The Guardian, 2 January 2018, https://www.theguardian.com/news/2018/ jan/02/the-scammers-gaming-indias-overcrowdedjob-market.

to the Indians by the Indians is relatively less and it is unidirectional and focused on one nationality. Whereas the traditional cybercrime which is seen overseas is targeted at multiple demography's living in different nationalities.

The major problem that India faces is the lack of infrastructure of the Indian police to tackle cybercrime. The rate of cybercrime is extremely high in India and the location of the perpetrator cannot be traced. The police are only left with the location of the victim. It becomes extremely difficult to project accurate statistics for curating cyber jurisprudence. This particular ability to conduct crimes while remaining under stealth was exploited by the Jharkhand Jamtara scammers as they targeted the victims of the crime residing in different states. Therefore the crime rate remained less in Jharkhand pertaining to Cyber abuse; therefore it is extremely difficult for the local police to trace the hackers in Jharkhand. There is an anecdotal incident during a court proceeding where upon investigation and trial the court ordered the police to recover CD-ROMs from the alleged hacker/ cyber-criminal. The police who are not trained in information and technology and how to handle sensitive information which has been derived from computers produced the evidence. Much to the amusement of the court, the police produced the CD ROMs which were punched in the middle by a needle and thread was put across the CDs in order to tie the bundle. This sort of mistake not only gives the accused person undue advantage but is also causes delay in the criminal justice administration. Cyberspace sensitivity and due diligence training is required to be given to the local police in order to handle cases arising from cyber jurisprudence as traditional intelligence and methods in policing cannot be sufficient in order to tackle the highly sophisticated and rising number of cyber crimes alone. [160]

Mira Road Scam Mumbai 2016

The Mira Road scam which was done by Indians from the city of Mumbai is recorded as one of the most sophisticated and well-planned cybercrimes. Mira Road cybercrime was mainly a call centre business that decided to make quick money by scamming the overseas clients by taking their vital information by making a call to them and telling them about false information which basically resulted in them paying the money to the

[160] Abhishek Waghmare, In 2015, Crime In India At 11- Year High, India Spend, 1 September 2016, https:// archive.indiaspend.com/cover-story/in-2015- crime-in-india-at-11-year-high-78461.

scammers. In order to conduct the scam the mastermind behind the whole operation hired number of employees as call centre service executives. These employees were paid a higher amount compared to the average salary of a call centre employee back in the day. The scamming operation was active between 2012 to 2016. [161]

The whole scam was on the basis that certain calls were made from India regarding tax arrears on account of certain non-payment of taxes committed by the citizen residing in America. The employees working for the scammers did not ask the employer regarding the credibility of their authority to conduct these calls. This is because of the fact that they were paid better compared to the market rate and at the end of the day the subject of the calls were foreigners, therefore, they were recalcitrant to pursue the credibility of the call centre to conduct such calls as the thought that even if it is something which is illegal they would not be in trouble as the subject matter is not directly under the jurisdiction of Indian Judiciary. This type of scam was carefully calibrated and executed as it had the essence of the east meets west tactics when it comes to cybercrimes. Therefore, from India scams were conducted following this particular method which involved smooth-talking credible executive which was matched by a Hi-Tech escrow account which used to collect the money which was paid by the victim. The latter part of the scam had the technical aspect which was inspired by the Eastern European Ukrainian scammers. The success rate of the scam conducted from the streets of Mira Road was likely to be less as it was conducted in a developed country against people who were aware of the cyberspace and the necessary precautions required to be maintained by them in order to safeguard their interests. Despite the high literacy in cyber jurisprudence, Indian Mira Road scammers were successful in scamming the vulnerable and poor victims from the United States of America[162].

In the month of October in 2016, a team of the special police force of 200 personnel raided the office of the call centre which used to conduct this scam in broad daylight. At the time of the raid there were 700 employees who were working for this call centre.

[161] Anamika Gharat, Exclusive: Mira Road call centre scam accused Shaggy reveals his side of the story, Mid-Day, 25 June 2018, https://www.mid-day. com/articles/exclusive-mira-road-call-centrescam-accused-shaggy-reveals-his-side-of-thestory/19546176.

[162] https://www.mid-day.com/mumbai/mumbai-news/article/Call-centres-employees-Mira-Road-detained-duping-US-citizens-raid-crime-news-17663186

All of them were detained by the special task Police Force and were questioned in groups as well as individually. After the primary investigation Special Task police allowed the majority of the employees to go back to their respective residence except for the top 70 senior employees who were running the administrative unit of the call centre. Special Task Police Force received proprietary information from the special intelligence unit based in the United States of America which provided with the lead regarding this investigation as well as vital sensitive information which was required by the Indian police in order to conduct this surgical raid. If a layman saw the functioning of this call centre he would think that everything is normal and the daily business is conducted by the employees. Upon close inspection it was found that the call centre used to indulge in fraud people from the United States of America in lieu of non-payment of taxes[163].

The genesis of the Mira Road scam took place when the mastermind behind the scam stole around 1 lakh personnel records pertaining to tax loan payment from people residing in America from the U.S. Internal Revenue System. It is to be noted that this database of tax arrears was bought by the scammers for an amount of US 1400 dollars. The steps which were incorporated after the data was achieved by the scammers were highly technical and extremely well-calibrated like a corporate company.

The first step in order to commit the crime of frauding citizens from America was to send them automated short messages on their registered mobile phones regarding the intimation of tax arrears conducted on their behalf whereby they would receive a call from the government agency which would for the elucidate them regarding the nature and extent of the arrear made by them. The bulk messages were sent by the hackers using magic jack software application which made the job easy as the application was a one-stop solution to send a message which cannot be traced back. Therefore the message received by the victim did not bear any telephone numbers but rather had an alphanumeric code written on the standard name which stated that this message was sent through an official source[164].

[163] Source: https://telanganatoday.com/gang-of-mira-road-nabbed-for-sim-swap-fraud-in-cyberabad
[164] Source: https://timesofindia.indiatimes.com/city/mumbai/cbi-may-open-cyber-crime-unit-in-mumbai/articleshow/51209244.cms

The success rate of the hackers varied as 90% to 85% of the US population was aware of such cybercrimes and they completely ignored the message. However, it is to be noted that the people who ignored the calls were not essentially the target groups that were pointed by the scammers to take advantage of. It was the vulnerable group who were mostly immigrants in the United States of America who were the prime targets of the scammer. Around 10-15 per cent of people contacted the scammers and most likely paid them. This crime conversion and success rate of the crime can be explained by the reason that the target/victim was in a developed countries and was literate in computer and cyberspace[165].

The Mira Road Scam was conducted in tandem when two people called the victim. The first individual calling the victim was referred to as the 'opener' of the conversation. Despite this type of scam being highly sophisticated in nature it relied on human intervention as well. Commission of information and technology scams are usually devoid of gender-oriented crime but in the case of the Mira road scammers it was usually seen that the role of the 'opener' was played by a woman. The choice behind this decision was that it was easy for a stranger to trust a woman and that this lady was proficient in an American accent. This decision was made by the uppermost management circle in order to vitiate the chances of racial abuse as was seen in the previous decades.

The person who was the victim at the end of the call is a valuable individual as he thinks that he faces a deputation or any federal offence maybe charged against him. Usually such people (Mira Road Scam victims) come from a poor background so they cannot afford a lawyer for fighting their case in the federal court, therefore when they call the scammers they are in relative fear of apprehension of jail or quitting their American dream as the Government of America would deport them for their alleged arrears. Majority of skilled chore labourers move to the United States of America in anticipation of a better future and while doing so they have invested all their savings. Such people may include information and technology engineers who work in America

[165] Source: https://economictimes.indiatimes.com/news/politics-and-nation/three-fake-call-centres-in-mumbai-made-rs-500-crore-by-duping-us-citizens/articleshow/54710487.cms?from=mdr

by using the H1B visa[166]. This H1B visa is very essential for them to work in America as the recruiter who employs the individual sponsors for his stay while he works in the United States of America. This step not only takes the burden off the finance of the immigrant but also provides them with a basic level of security as the recruiter covers the essential cost for living on behalf of the immigrant. The H1B visa is also the stepping stone in order to procure the much sought after American Green Card which provides the immigrant with citizenship in the United States of America. Therefore any opportunity or threat which hinders the process of getting the green card causes extreme anxiety and stress to the victims (who have received the message regarding the tax arrears). The opening of the con call is usually in a strict yet calm tone and the scammer explains the nature of the problem to the victim and thereby demands from the victim for the payment of the tax. Now in America when a person is permanently employed he has to pay the tax by a federal card. The same card is not provided to immigrants living in America under a work visa or the student visa. This particular information is not available to the victim or they are unable to process this information in a moment of panic and they in retaliation request the call centre employee (scammer) to help them figure out a method for the payment of the tax. At this point, the compassionate women scammer would show empathy towards the victim and request her senior to join the call in order to help the victim to pay his tax. The person who joins the call as a team member is another scammer and this person is usually referred to as the 'closer'. His job is basically to convince the other person to pay immediately and close the call, therefore, commencing in a successful case of fraud. The 'closer' suggests the victim to buy certain gift cards which are sold online on various E-commerce websites such as amazon.com and when the code of the gift card is shared with the call centre employee they can convert the amount from the gift card into normal currency, thereby compensating and completing the process of payment of the tax.[167]

The victim does not know that the gift card money is collected by the scammer for his own personal use and it does not strike to the victim that how come a federal agency

[166] Source: https://indianexpress.com/article/explained/call-centre-racket-irxs-scam-maharashtra-3076002/

[167] Source: https://economictimes.indiatimes.com/news/politics-and-nation/three-fake-call-centres-in-mumbai-made-rs-500-crore-by-duping-us-citizens/articleshow/54710487.cms

would accept the gift card as a mode of payment for arrear in tax. At this point, the victim is completely flabbergasted and confused thereby he goes to the nearest brick and mortar retail store or even online and buys a gift card and as soon as he procures the card, he shares the details with the scammers and in this way the *Hawala* scam is complete. It is to be noted that after 2016 when the Mira Road scam was busted by the special task Police Force led by Mumbai Police in collaboration with intelligence agencies helping the Indian police from the United States of America, it was found that there was a drop in around 95% of calls in America regarding the arrears of payment. Similar scams based on the model of Mira Road were subsequently raided in Ahmadabad Gujarat, Surat in Gujarat, and Thane in Mumbai. Call centres operate day to day activities as a sham to the public and even have fake paperwork in order to misguide the police and investigation agencies.

Cybercrime in Jamtara Jharkhand

In order to understand the crimes committed by the citizens living in Jamtara Jharkhand it is important to know about the background of the place. Jamtara in Jharkhand is the area where agriculture is the main occupation and the total size of Jamtara is roughly around 2000 square kilometres. Jamtara has a high level of unemployment as it is one of the poorest states of India. Total population of 1 million and the whole district is a conglomeration of roughly 100 villages. There are a dozen mobile towers in the district and at least more than half of the towers were used in order for the commission of the crime. It should be noted that there was a time when the scammers from Jamtara used to call an average of 3000 calls a day which was quite bizarre as the population density in that particular district is around 800[168].

It's been noted that the cyber crime in Jamtara cannot be compared with the crimes committed in cities which are savvy in information and technology. For example, the crimes committed in Pune, Mumbai and Bangalore are different from the crimes committed in Jharkhand, as the former was highly dependent on cyber knowledge whereas the later is dependent upon the old school method of crime which was street-

[168] Fraudsters from Jamtara gang arrested for duping elderly man, The Statesman, 3 February 2020, https://www.thestatesman.com/bengal/ fraudsters-jamtara-gang-arrested-duping-elderlyman-1502852574.html.

smart deceit. The only difference was that the scamming activity was conducted via a telephone call and was completed by a transfer of amount money through digital transaction. But the method behind the conversation and the transfer of money was based on the age-old method of frauding people that is misappropriation of information on wrong guidance of information[169].

According to a news report in which the news agency interviewed the youth from Jamtara who were involved in the offence of misappropriation of money and frauding individuals using telephone, the news journalist found out that there was no iota of remorse or regret in the individuals who were involved in the offence. Even the family members of the criminals did not show any sort of regret based on the actions committed by their family members. The reason behind being that the state did not provide any sort of social benefit scheme for any economic benefit to the marginalised communities, therefore if they were able to create better opportunities for themselves they thought that they had done so out of their own hard work; therefore there was no regret. They receive the sense of entitlement to the activities conducted by the youth even if the methods to procure the better service in life or better goods in life were obtained by *mala fide* intention/means did not make any difference to the people living in Jamtara. It is to be noted that one particular difference that was seen in the criminals from Jharkhand and the rest of India was that the criminals from Jamtara were younger when compared to rest of India (especially the citifies which were involved with Cybercrimes). The average age of criminal in Jharkhand who was a part of the cybercrime was around 15 to 25 years old, whereas in the other cities the mean age limit used to begin from 25 to 45 years old. The only reason behind slightly less age was technically/formally unskilled criminals in Jharkhand.[170] The cyber crime criminals who were operating from the big cities in India landed up in doing the wrong actions after completing their formal education in information technology or computer science. The main target victim group of the big city criminals were foreigners whereas the

[169] Christine Hauser, U.S. breaks up vast I.R.S. phone scam, The New York Times, 23 July 2018, https://www.nytimes.com/2018/07/23/business/irsphone-scams-jeff-sessions.html.

[170] hehindu.com/news/national/ed-attaches-assets-of-jamtara-based-cyber-criminals/article34042508.ece#:~:text=Cyber%20crime%20hubs%20of%20Jharkhand's%20Jamtara%20district&text=It%20is%20alleged%20that%20over,premises%20of%20the%20gang%20members.

cyber criminals from Jamtara targeted criminals from impoverished backgrounds who were living in India.

According to a book written by Dr Amar Hussain it was the lack of social security and school dropout rates that were major factors for the kids to be part of this type of scam. Quality of the criminals who were part of the scams which were conducted from Jharkhand - highly unsophisticated in nature and the crimes committed by them require a little to less amount of cyberspace acumen. The scammers from Jharkhand were extremely careful about choosing their targets as they tried to contact only those people who were living outside Jharkhand. The sole reason behind this strategy was to mitigate police investigation. The scammers know that it is difficult to trace cyber based crimes in India but they can remain a prime target if all the victims of the crime come from one particular area or state.[171] Therefore the activities done by the scammers from Jharkhand targeted pan India and particularly aimed at migrant labour class gentry who were extremely easy to be manipulated as they'll have the technical know-how of banking and cyber jurisprudence. The society also protected these criminals as the journalist in the aforementioned paragraph states that the atmosphere of socialism and the social protection offered by the elders to the youth who were involved in such activities. The elders were happy to see the youth engage in some activity which was not physically dangerous and at the end of the day they were able to bring that money for them. This is extremely rare to see in India but the state of poverty in Jharkhand had forced the citizens to acquire unlawful means to make ends meet. There was an egalitarian distribution of the money and bounties made during the calls by the scammers which was distributed among the family members as well.

The mode of operation of this scam was extremely basic in nature and this type of scamming is seen on a day-to-day basis on the streets of India. The scammers from Jharkhand relied on the age-old technique of both talking and the lack of knowledge regarding the basic functioning of banks and cyberspace. It has to be noted that the scammers of Jharkhand were not technically skilled in doing the scams but

[171] Source: https://www.thehindu.com/news/national/other-states/the-cyber-con-artists-of-jamtara/article19476173.ece

they conducted the activity of scamming in a highly methodological manner.[172] For this they even had a training institute or informal training set up where children used to get training in how to scam victims using the mobile phone. However, it has been noted that such training was only provided to the people who were residents of the village and no outsiders were allowed to be part of the training. The training comprises of a basic script which is given to the villages in order to prepare themselves for a professional telephone call and the victim should be made aware that he is speaking to a customer service executive of a reputed banking institution. This training is somewhat similar to the language and communication training which is provided to the call centre employees when they join the call centre.

After the training is complete the youth of Jamtara divide themselves in small groups and then they disperse into the forest area in order to begin the offence. The forest area is chosen because it is easy for the criminals to hide in the forest in case of a police raid or investigation. The criminal call individuals on their mobile phones and they state that they are calling on behalf of online banking assistance provided by the State Bank of India. The sole reason behind choosing State Bank of India is as the bank is the largest stakeholder in India so there is a high chance that the victim on the other end may be a *bona fide* customer of State Bank of India.[173] These numbers are obtained randomly from the internet and for the same the scammers do not even pay. It is to be noted that such crime is conducted during broad daylight, when the scammer calls the victim he assured that the call is from the bank and he is calling on behalf of the online banking service provided by the bank and wants to convey the information they have been certain illicit payments made by the debit card of the victim and if the payments are not made by the victims in person then it is highly advisable for him to block the card. At this point the victim is confused as he has not made any payment but the call seems extremely convincing therefore the victim asks for help from the fake customer service executive. The scammer on the other side advise the victim to share the card details so that he can block the card from his system, thereby he can go to the bank

[172]Source: https://www.newindianexpress.com/states/telangana/2021/mar/15/9-of-10-cybercrimes-in-telangana-traced-to-jharkhands-jamtara-2276704.html

[173] Source: https://www.jagran.com/jharkhand/ranchi-border-of-up-rajasthan-and-haryana-becomes-second-jamtara-cyber-crime-real-story-jharkhand-news-21673309.html

physically and check the payments which were made without his knowledge. Once the card details are shared by the victim the fake customer service executive tells that in order to complete the call a one-time password would come on his mobile phone which is required by the sales executive as the number would conclude the conversation. As soon as the password is shared the scammer has already transferred money from the victims account to another account which cannot be traced. It is to be noted that due to the surplus availability of SIM cards and number portability technology it is extremely difficult to trace and track the Jamtara scammers.[174]

Chapter 5: Legal Provisions and Case-Law related to Cybercrime

The following are legal provisions from the Information Technology Act of 2000[175] which covers various aspects and crimes related to cyberspace in India.

Section 65: This section is regarding tampering of computers with the intention to destroy the seal or change the identity of the computer source code or a computer software program or a local area network with the sole purpose of hindering in the performance of the computer so that it can cause and impact to the user or to the organiser of the computer system. Under this offence a person can be sentenced up to three years of imprisonment with the fine of rupees 2 lakhs. There are certain times when a virus is inflicted upon a computer by which the computer seizes to perform on its regular capacity therefore the individual using the computer cannot use the computer as it was intended to be used. In such a case he or she can file a case under section 65 of the information technology act.

Section 66: This provision of the legislature deals with the crime of hacking of computers which is done for the purpose of data alteration with the intention to cause any harm, injury, destroy or delete information that resides in that system. Usually this information is confidential in nature and the person who has hacked into the computer does not have the authority to access the information. The action of hacking is done to cause damage to the owner of the personal computer as when the data is altered or

[174] Source: https://indianexpress.com/article/india/in-jamtara-community-libraries-offer-hope-way-out-of-cyber-crime-7377561/

[175] Source: https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=

stolen from his computer he has to be answerable to the authorities above him regarding the breach of the side station. Under section 66 a person can be convicted for a sentence amounting to three years of improvement to find that can extend upto 2 lakh Rupees.

Section 66A: This is a very important section considering the social fabric of India; it safeguards the dignity of women. Under this stature if a person sends offensive messages through the use of social media or any other mode of electronic communication through any text or SMS or email which bears a language which is toxic or threatening in nature or it has certain characters which causes anger inconvenience then this section shall be invoked. Criminal interpretation is extremely common in India and people somehow don't understand that the language they use causes the amount of anguish to the other person who is reading it. One moment's anger causes the other person a lot of pain and often it persuades other parties to take severe action against each other which may not be lawful in nature. Under this section an individual if found guilty can be sentenced to three years of improvement along with a fine as regarded suitable by the Honourable competent court.

Section 66B: Under section an individual can be penalised and can also be sent to Jail if it is obtained that by his computer or any other storage device under his possession has proprietary confidential information which was obtained by him which in the first place was obtained by using dishonest or fraudulent methods. There are cases in India where information in form of data is stored by people who are not authorised to store that data. In this case they can be prosecuted under section 66b of the information and technology act of 2008 found guilty by the competent court date can be sentenced to imprisonment for a term of three years along with a fine of 1 lakh rupees.

Section 66C: This section can be imposed against an individual who has used a fake identity in order to take unlawful advantage. Therefore, if an individual has used a digital signature or any other official insignia or downloaded from the internet which makes the other person (victim) believe that the communication made by such person is legitimate and from the official source then this individual is considered to have used the identity in order to take a dishonest advantage on the other party. Under this section

if a person is found guilty he can be imprisoned for a term of three years along with fine which can extend upto 1 lakh rupees.

Section 66D: Under section a person can be prosecuted if he has assumed the online identity of any other person. Therefore the action of impersonation of somebody else in lieu of taking advantage of people and this advantage is of an unlawful nature then the person shall be guilty under section 66D. 21st century is time of social media everybody is on social media when you access Twitter, we come across several accounts which are made by different people trying to impersonate celebrities in the society and in such a manner they try to deceive the public. In modern day such tactics are used to spread fake news which is highly dangerous in a hybrid heterogeneous society like in the case of India. If a person is found to be impersonating somebody else's account on the internet and uses communication in such a way that he tends to take advantage of the victim then he shall be imprisoned upto a period of three years and along with that a fine of rupees 100000 Shal be paid by him.

Section 66E: This particular section is extremely important considering the Indian context as a lot of young and vulnerable women fall in the trap of boys and later are taken advantage of by their emotions. Under this section any person who publishes, transmits or captures videos of the private areas moments or private parts of any individual without his or her consent shall be liable for a sentence of three years of imprisonment and fine exceeding a lot more than 2 lakh Rupees. It should be noted that there are many instances in India when upon certain encouragement young couples try to record their private moments and later these photographs of videos are used to blackmail the other party. In order to solve this problem this section was introduced as an amendment in the information technology act of 2000.

Section 66F: This section deals with the concept of Cyber terrorism. This problem is extremely difficult to tackle as multiple countries face this problem and it is extremely important to have a good cyber infrastructure in the criminal justice administration system to tackle crimes committed in the space of Cyber terrorism. According to the section anyone who intentionally threatens the integrity, unity, sovereignty or security of India by conduct or action by methods incorporated such as the common man is unable to access its computer resources, or of cyberspace in which virus attacks are

made to the computer systems, there is an unauthorised access of computer program in order to gain access to certain vital information which the person who is getting the access is not authorised to get in the first place then in that case the person can be prosecuted under section 66F of the information technology act and if found guilty he can be sentenced to a maximum imprisonment of life imprisonment.

Section 67: Crime against women and children who are considered to be vulnerable sections of the society. The sections of society are often not aware of the various kinds of exploitation done against them and section 67 along with Section 67A and section 67B of the Information Technology Act safeguards the women and children of our society.

Under Section 57 whosoever transmits or publishes any of scene materials in form of a video or a photograph in electronic form shall be liable for punishment for 5 years of imprisonment alongside a fine of rupees 100,000 but if this person is found to be a seasoned convict then the term may be extended up to 10 years and the fine can be extended upto 2 lakh Rupees.

Section 67A elucidates that any publication of material which is sexually explicit shall be punishable up to five years of imprisonment and in case the person is a seasoned convict or it is a second time imprisonment under the same offence then the term of punishment can extend up to seven years and the fine can be extended upto 20 lakh rupees. Section 67B particularly safeguards the interests of children. Child trafficking is a huge problem in India and usually children who are born and living on the streets are engulfed by child trafficking. Child trafficking not only spoils the future of the children but it also mentally scars them throughout their life. Any person who is found to transmit or publish electronic material which depicts children performing sexually explicit acts then the person shall be punished up to five years of imprisonment and fine would amount 10 lakh rupees. However, if the court finds out that the offence committed by the person is his second offence and he has been involved in similar offence previously then the court can extend the punishment up to seven years alongside a fine of rupees 10 lakh rupees.

Section 67C: Under this section it is defined that if a person is found to have stored an information or data which was obtained as an intermediary and has had a copy of the

same for his own personal reference, then the person shall be liable under the section. It is to be noted that section 67C employs on a person who uses the information or data. It is to be noted that section 67C implies on a person who uses or stores the information or data without any legitimate authorisation and in such case the court can provide a sentence of three years to the individual.

Table 5: Relevant Provisions Related to Cybercrime at a Glance

Sl. No.	Offences	Sec. under IT Act, 2000
1.	Damage to Computer, Computer System etc.	**Section 43**
2.	Power to issue direction for blocking from public access of any information through any computer's resources.	**Section 69A**
3.	Power to authorize to collect traffic information or data and to monitor through any computer's resources for cyber security	**Section 69B**
4.	Un-authorized access to protected system.	**Section 70**
5.	Penalty for misrepresentation.	**Section 71**
6.	Breach of confidentiality and privacy.	**Section 72**
7.	Publishing False digital signature certificates.	**Section 73**
8.	Publication for fraudulent purpose.	**Section 74**
9.	Act to apply for contravention or offence that is committed outside India.	**Section 75**
10.	Compensation, confiscation or penalties for not to interfere with other punishment.	**Section 77**
11.	Compounding of Offences.	**Section 77A**
12.	Offences by Companies.	**Section 85**
13.	Sending threatening messages by e-mail Sending defamatory messages by e-mail.	**Section 503 IPC**
14.	Sending defamatory messages by e-mail.	**Section 499 IPC**

15.	Bogus websites, Cyber Frauds.	**Section 420 IPC**
16.	E-mail Spoofing.	**Section 463 IPC**
17.	Web Jacking	**Section 383 IPC**
18.	E-mail Abuse	**Section 500 IPC**
19.	Criminal intimidation by anonymous communications.	**Section 507 IPC**
20.	Online sale of Drugs.	**NDPS Act**
21.	Online sale of Arms	**Arms Act**

Important Cases Regarding Cyber Crimes

United States v. Jake Baker[176]

This is one of the most important cases in the recent history of cybercrime as one side of the story explains the factors responsible behind crime against women in society while the other side deals with an individual's right of freedom of expression. In this case Jake Baker who was a student then made a website for blogging purposes and in that website he used to share stories which are highly graphic in nature. The graphic story is where he shared his sadomasochist ideas such as concept of bondage, rape and torture of women. He expressed in the blog that he wants to commit kidnapping and abduction of a person and even make-out with an injured person. In the year 1995 he submitted a story of fantasy sex to alt.sex.stories.net in which he described a conjugal relationship based on non consensual intercourse with his classmates who was named in the case as Jane Doe. It is noted that this name is a made-up name as his classmates did not want her name to be mentioned publicly. This case is a complicated case to understand because Jake was charged as he violated Section 18 of the US Section 875 Subsection C which elucidates that a person shall be convicted if he communicates threats to kidnap for enjoyment and infliction of injury. On the other hand Jake Baker pleaded immunity from the court under the first amendment of The United States of America constitution. The first amendment of the US Constitution says that an

[176] "United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997)". *Scholar.google.com*. Retrieved 2017-05-28.The full title of this case is United States of America v. Abraham Jacob Alkhabaz, also known as Jake Baker

individual has the freedom to express by speech and Jake Baker said that in this capacity he exercised his right of expression of speech. Jake Baker's explanation for his fantasy stories was that he considered them as therapy. He was going through mental health issues and thereby considered sharing his dark fantasy on the inter-web as one of the methods of letting out frustration and anger in a harmless way.

The Lonely Shepherd Double Court observed that the State did not have requisite amount of evidence against requisite amount of evidence against Jake Baker in order to prosecute him under the charge. Therefore in the opinion of the court Jake Baker exercised his right of expression of speech. It is a controversial case as his blog exposes other individuals to such brazen expressions of sadomasochistic sexual actions which may deemed to be heinous crimes against women.

Manish Katariya v. Ritu Kohli[177]

This is one of the first cases in India in which involved cyberstalking. After this case the legislature amended the Information Technology Act of 2008 and introduced section 66A in 2008 in order to provide a better understanding when it comes to cyberstalking. In this case Manish Kathuria met Ritu Kohli online on a website which was made to mingle adults later they to decide not to talk to Manish but Manish kept on chatting with her on the website. When Manish found out Ritu was not interested in chatting with her he then used foul language and interpretation of a criminal nature to coax Ritu to talk to her. When Ritu did not reply to Manish Kataria's constant abuse he decided to leak Ritu's private information regarding her address and contact information on a website called www.mirc.com. This website was made by Microsoft in order to chat with strangers, therefore as a result Ritu received many lewd telephone calls during the night, demanding sexual favours. Ritu was extremely aggrieved by this as it caused a lot of mental trauma on her, thereafter she made a complaint to the Delhi police and the same was able to trace the internet protocol address of Manish Katariya and eventually Manish Katariya was prosecuted under section 509 of the Indian penal code 1860[178].

[177] C. W. P. No. 14104 of 2013

[178] Dr Sapna Deo, Cyberstalking and online harassment, Bharati Law Reviw, July 2013, http://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf

At that time the Information Technology Act was not amended and after this case there were similar cases of cyberstalking in Goa, where a group of students from Delhi University were stalking women online. However, it is to be noted that the Honourable Supreme Court in its judgement observed that Section 66A of Information and Technology Act is unconstitutional as it violates Article 19 (1)(A) of the Indian Constitution. This judgement was made by the apex court in the year 2015.

Karan Girotra v. State[179]

In this case there was one Shivani Saksena who used to live in Delhi and she married in 2009 in the month of November. However the couple file divorce as according to Shivani her husband could not consummate the marriage. In 2010 Shivani got a divorce based on a mutual petition. In the month of April 2010, Sivani met Karan online and they started chatting but it is to be noted that they were in contact 6 years before her marriage as well and at that time Karan wanted to marry Shivani but Shivani did not want to marry Karan.

In May 2010 Karan and Shivani met when Karan invited Shivani to his house so that she could meet his family members. When she arrived she found that there was only one family member available who was bedridden at that time and she was the grandmother of Karan. Karan invited Shivani in a room and they had physical relationship. When Shivani woke up and found that she was sleeping on current bed and she was completely naked on the latter examination she found that she was sexually exploited by Karan as well. According to Shivani she was intoxicated by Karan and the next day she found out that her naked pictures are shared online. After the action was committed by Karan he tried to console Shivani and promised that he will marry her. When she called Karan he replied by consoling her that he will marry her and that she should not bother about the images being circulated online. Thereafter Karan exploited Shivani and asked for sexual favours. After this conversation he started to blackmail Shivani and she was repeatedly raped by him.

In the month of September of the same year there was an engagement ceremony conducted between him and Shivani and during that ceremony the mother of Shivani

[179] BAIL APPN. 977/2011

gifted Karan valuable gifts such as gold jewellery, clothes and other items of electronics. A few days after this engagement ceremony Sivani broke down and explained what ever happened to her with her mother and thereby they went to the Delhi Police to lodge a complaint against Karan.

Delhi Police registered a complaint under section 328 and 376 of the Indian Penal Code alongside section 66A of the Information Technology Act of 2000 and prosecution was conducted against Karan. The learned Court pronounced that Karan was not guilty of section 376 of the Indian Penal Code and there was a delay in lodging the FIR by Shivani. The repeated physical intercourse between Karan and Shivani were of consensual nature and thereby the charges were dismissed. This is one of the rare cases in which a heinous charge has been dropped by the virtue of delay in lodging the FIR.

Vinu Priya Case[180]

In this case charges were filed against a 21 year old person called P Suresh who used to live in Chennai. The charge which was levied upon P Suresh was of the abatement of suicide of Vinupriya. The cognizance of the case was made when the district magistrate of Salem went to the local police regarding the incident. Morphed photographs of Vinupriya were uploaded by P Suresh on Facebook. These photographs were sexually graphic images which were downloaded from the internet and after that Vishnu Priya's face was juxtaposed on the photograph. Vinu Priya was extremely shocked and went into a state of depression after seeing the photographs and ultimately committed suicide. The Honourable Court power P Suresh guilty of abetment of suicide.

Yahoo! Inc v. LICRA[181]

This case involves laws of two countries, the United States of America and France. Yahoo IMC, the United States Corporation, was operating in France under Delaware Company Yahoo France. When an international corporation works in a foreign country the company has to obey the domestic Municipal laws of the country and the operation

[180] Habeas Corpus Petition No.1956 Of ... vs State Of Tamil Nadu on 16 March, 2017

[181] Christine Duh, Yahoo! Inc v. LICRA, Berkeley Technology Law Journal
Vol. 17, No. 1, Annual Review of Law and Technology (2002), pp. 359-378 (20 pages)
Published By: University of California, Berkeley, School of Law

of the company in day-to-day business activity has to be consistent with the municipal laws of the country in which the International cooperation is operating. Yahoo used to conduct an online auction in which people could sell items to users worldwide. The US Company Yahoo used to offer terms and conditions before taking part in the auction. LICRA and UEJA are French nongovernmental organisations who used to perform antisymmetric awareness and organisations filed complaint against Yahoo as one of the items which were sold on the French forum of the US Corporation was a watch which was having Nazi Insignia on it. According to the French Law under Article R645-1 it is prohibited to sell any item which belongs to Nazi Germany supports communal disturbance in the society.

Avinash Bajaj v. State of Delhi[182]

In this case one Mr Avinash Bajaj who was managing director of an online E-commerce website called Bazee.com approached the Honourable Delhi High Court invoking its inherent powers vested under Section 482 of The Criminal Procedure Code in order to quash an order of summon. It is important to understand the background of the case in order to understand why Mr Avinash Bajaj approached the Delhi High Court. On November 27 2004, a multimedia format video was uploaded on this website and the video was given a title as following, 'DPS School Girls Having Fun'. Upon investigation by the Delhi Police it was found that a student from IIT Kharagpur whose name was Ravi Raj had uploaded the video which had obscene content. The Managing Director of the website Mr Avinash Bajaj was held responsible as the content on the website was uploaded and there was no due diligence done by the website in order to scrutinize the videos or content before uploading it on their platform. This MMS video was sold for Rupees 125 and was uploaded under the section of e-books. Three days later the cognizance of this pornographic material was taken by Delhi Police Crime Branch and FIR was registered against Ravi Raj who was a student of IIT Kharagpur and Avinash Bajaj who was the Managing Director of Bazee.com

[182] W.P.(CRL) 771/2014 & Crl.M.A.5999/2014

The Criminal Court of the metropolitan magistrate took cognizance of the case and filed charges against the aforementioned accused individuals under section 292 and 294 the Indian penal code and section 67 of the Information Technology Act. Ever since the Honourable Court to cognizance of the case the student Raviraj was absconding while Avinash Bajaj applied for bail which was rejected by the court of the metropolitan magistrate. Section 67 of the Information and Technology Act states that whoever intentionally uploads or causes to upload, any online content which has lascivious material and can cause injury to the public health and morality, such a person if found guilty of the offence can be sentenced up to 5 years imprisonment and a fine of rupees one lakh.

The Honourable Court observed that the role of the company was of a moderator whereas the content which was uploaded on the company website was an integral part in completion of the offence, therefore there has been a laxity on the part of the company whereby the questionable content has been uploaded online. The company has strict liability upon its performance in order to upload a material which should be consistent with the Indian laws. The court found that the company has liability under section 292 of the Indian Penal Code however this criminal liability does not transfer to the Managing Director of the company as automatic criminal liability transfer is not recognised under the Indian Penal Code however Avinash Bajaj was held guilty under section 67 and section 85 of the information technology act 2000 because of the fact that the performance or the lack of performance on behalf of bazee.com was an essential part of the commission of the offence.

Delhi Balbharti Case[183]

In this case there was a school which was managed and run by the Indian Air Force. It is to be noted that this is a one-of-a-kind case in which it highlights what is the toxic influence of the internet on the minds of the teenagers who get early and unlimited access to the same. This case revolves around an adolescent love story between a boy and a girl. When the boy does not reciprocate his affection towards this girl he uploads illicit and morphed images of this girl on http://www.amazing-gents .8m.net website.

[183] W.P. (C) 7902/2018 AND CM No. 30296/2018

On this website there were other pictures of different women, even photographs of teachers working at Bal Bharti School. Girls and teachers were classified on the basis of their physical attributes and the website soon became an adult boys joke amongst corrupted students. The girl in question soon found out about the website and this made her shattered psychologically. She informed her family members and his father who was a serving officer in the Indian Air Force made a formal complaint to the Delhi Police. The Delhi Police registered a case under section 67 of the information technology act and the concerned student was charged under section 67 of the Information Technology Act and was kept at Timarpur Juvenile home. He was at that time 16 years old and was provided a bail after 10 days.[184]

Sony Sambandh.com Case[185]

This is one of a kind case in India where Sony India Private Limited filed a complaint against the website which was registered as www.sonysambandh.com. This case was basically a fraud transaction in which there was a person named Arif Azmi who ordered a television which was imported at that time and he used to live in Noida. This website used to provide Sony brand products from abroad to the people who were living in India. A woman ordered a product from this website and the delivery was made to Arif Azmi. The delivery was accepted and after 90 days when the credit card company contacted the woman for the payment she denied making any transaction. The woman outright rejected any transaction made specially using this website. The police traced Arif and it was found that he gained access to the credit card of the American lady and after that he misused the same to buy a television. The Central Bureau of Investigation had received evidence from the American police and Arif was arrested under section 418 section 419 and section 420 of the Indian Penal Code. At the time of conviction his age was 24 years old and he was the first time convict therefore after one year of sentence the court granted him relief through probation.

Bank NSP Case[186]

[184] Source: https://www.casemine.com/judgement/in/5c5ec7e79eff430ba24c8773
[185] Source: https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf
[186] Source: https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf

This is a very unique case where the personal performance of an individual led to a point where his place of employment had to bear the consequences of his personal action. There was a management trainee in a bank who was supposed to get married and during his course of employment he used to exchange emails using the company's official computers and thereafter he also used his official email ID while writing to his fiancé. The marriage could not happen and they broke up. The young lady decided to send insulting and fake emails using the email ID of his former fiancé. These emails were directed to the clients of a former fiancé. To the clients it seemed that the employee of the bank was sending emails which were filled with abuses and other toxic language. The bank lost a huge number of clients and was held liable for the email sent using its official system.

Parliament Attack Case[187]

Bureau of Police Research and Development in Hyderabad took cognizance of a case when a computer was recovered by the terrorists. The laptop seized by Bureau of Police Research and Development had confidential information of the ministry of Home Affairs, Government of India. On top of the laptop there was the emblem of India consisting of three lions however after a closer inspection it was found that the laptop was forged in the state of Jammu and Kashmir and the two terrorists who had the possession of the laptop were arrested by the Bureau of Police Research and Development, Hyderabad.

Andhra Pradesh Tax Case[188]

Plastic manufacturing company in Andhra Pradesh was arrested for the laundering of Rupees 22 crore. This amount was seized by the central Vigilance committee from the home of the owner of the plastic manufacturing company. In order to avoid jail the owner of the plastic manufacturing company submitted 6000 vouchers to prove that his business was legitimate. When the police department did the careful study of the vouchers and the paperwork and other data obtained from his personal computers, it was found that the paperwork including the vouchers was made within five days of the

[187] Vishnu, J T (17 December 2001). "ISI supervised Parliament attack Main coordinator of Jaish, two others arrested". *The Tribune*. Retrieved 23 October 2014.
[188] Source: http://www.cyberlawclinic.org/casestudy.htm

police raid. It was conducted that the plastic manufacturing company was a shell company and underneath it there are many other companies who were administered by the same person. The person used fake and computerized vouchers to show a low sales record and save tax.

Chapter 6: Conclusion and Policy Recommendation

It is extremely important to know what types of cyber crimes are prevalent in India. There are two types of cybercrime, one which has a hierarchical structure, which functions as a corporate company, and there is a clear defined leadership and goals which the company or the unit of criminals follow in order to fulfil the purpose of its creation. On the other hand there are a group of cyber criminals who do not rely on a well structured set up to conduct their cyber crimes whereas they rely on a small circle of criminals and the level of involvement of technology is less compared to the former method.

If you take the example of India, it appears that largely it is a country where bottom-up phenomena draws a pool of this disempowered youth who have technical education and take part in hacking or other methods of cybercrime in order to make quick money. The youth of this country knows that the criminal justice administration system is under a lot of pressure and it is extremely difficult to trace and track down criminals. Therefore, they weigh and consider positives and the negatives of their action, and it turns out that committing a cyber crime is far more lucrative. The youth of this country who engage in cyber crime involve hacking and phishing as one of the most common methods of conducting this crime and criminals have little to less technical knowledge regarding information and technology. They will lie on the age-old method of cold reading and active reading whereby they utilise the confidential information accessed by manipulating them (victim) under their spell[189].

Cyber crimes in India are prevalent using the aforementioned model but it has been noted that it was not introduced in this country based on the aforementioned model but by disgruntled employees chasing their American dream. Multinational companies

[189] John Kelly, Even telephone scammers agree: Don't trust them!, The Washington Post, 9 December 2019, https://www.washingtonpost.com/local/ even-telephone-scammers-agree-dont-trustthem/2019/12/08/f353c616-17a1-11ea-a659- 7d69641c6ff7_story.html.

when they decided to enter the Indian market to set up information and technology companies did not reach out to India to empower their youth but it was more on the lines that India provided a cheap labour source and the business model was based on a cost-saving idea and not on a quality agenda. Following the 2008 economic recession the jobs in IT sector reduced and the stringent immigration policies were introduced by the United States of America - the disgruntled employees of the Indian call centre decided to take legal jobs or jobs which did not clear the purpose of their employment as a source of revenue because they had no other option.

The main reason for the rise in the number of cyber enabled crimes in India is the difficulty to investigate the same by our police. Cases are too costly to investigate for the small sum of money or the scale of damage conducted/committed by the hacker. The hackers in India are very smart as they do not conduct the activities in their neighbourhood or even in the district. In addition to that the hackers conduct micro-level scams which are difficult to trace but when addressed to a large number of people culminate into a big sum of money. These micro-level scams are often not reported by the victim and even if it is reported by the victim the police cannot judiciously search the hacker.

It is an area of crime which gives an undue advantage to unskilled criminals who have limited knowledge of the Information and Technology sector. It is extremely important to understand whether cybercrime falls under the concept of traditional crime or not. It is to be noted that cyber crime can be initiated by an individual against an individual or multiple people even a single person can take on sovereignty, however, there have been occasions and conspiracy theories where State sponsored cyber activity has also been reported where the State used discreet measures to acquire confidential information about private persons[190].

One particular reason why cyber crimes have increased in India is the rate of internet accessibility to its citizens. Today Indians can access the internet via their mobile phones which are ready to use gadgets that are a perfect receptive for cyber

[190] Sanjay Pandey, Digital India's response readiness against cyber attacks is frail, lack of online security awareness biggest weakness, Firstpost, 25 June 2019, https://www.firstpost.com/india/digitalindias-response-readiness-against-cyber-attacksis-frail-lack-of-cyber-security-awareness-biggestweakness-6876111.html.

crime activities as well. In addition to that the Indian political parties also add fuel to fire when it comes to cyber crimes. Knowing about the limitations of our cyber jurisprudence and the pressure under which the criminal justice administration system works, the Indian political parties in order to win populist opinion provide internet connectivity to remote and local areas without any prior training. The local government of Delhi has announced a scheme to create 11000 free Wi-Fi hotspots therefore in a city with 75% of all Cyber crimes reported in India it is a daunting task for a law enforcement Agencies to curtail the high rate of crime pertaining to Cyber jurisprudence[191].

Another reason why there is high cyber crime in India is the fact that joblessness is the highest among educated Indians. It is easier to find employment in India if one is less qualified. Urban unemployment is higher than rural employment. It is to be noted that in the book written by Nobel Laureate Prof. Abhijit Banerjee, (Good Economics for Tough Times) it is noted that between the age group of 15 to 30 Indians do not get the desired jobs and there is a high amount of unemployment, however the same Indian gets employment between the age of 31 to 35 but it should be noted that the job obtained by such individual was not desired by him in the first place. Therefore the job that Indian does after a certain period of unemployment culminates to be a job which he never desired[192]. Therefore he does it with recalcitrance. This problem is augmented due to the slowdown in the IT sector and now with the advent of a pandemic which has lowered the rate of growth which was promised by the IT sectors. Therefore by failing to provide a conducive environment to work for the IT sectors which includes harsh tax systems and lack of transparency in order to set up a small or medium sector Enterprise in India, the Government of India has invariably shunted the IT sector in unfavourable circumstances.

[191] Ankit Yadav and Chayyanika Nigam, Cyber crime risk in free public WiFi, India Today, 11 August 2019, https://www.indiatoday.in/mailtoday/story/cyber-crime-risk-in-free-publicwifi-1579617-2019-08-11.

[192] Amit Kapoor and Anirudhh Duttaa, Indian economy struggles to expand with rising unemployment rates, stagnant wages, poor female participation in labour force, Firstpost, 24 September 2019, https://www.firstpost.com/india/indian-economystruggles-to-expand-with-rising-unemploymentrates-stagnant-wages-poor-female-participationin-labour-force-7392721.html.

The Government of India can boost encouragement for domestic research and development as it would help us evolve our own software and in this way dependency on western products and computers would alleviate. The indigenous growth in the Information Technology sector would encourage local businesses to investing in cyber security. In addition to that the government must make effective efforts for the educational curriculum base of young workers; therefore it would prevent them from objecting to unemployment in times of recession. They will not opt for illegal means to make their ends meet. Major revamp is required in our criminal justice administration system whereby the police must be trained to handle cyber investigations, and creations of special rules or courts which are required in order to segregate the jurisprudence of cyber crimes with traditional organised crimes. Lastly joint effort by the society as well as the government is required to sensitize the general public regarding the risk of cyber crimes and to educate and aware the common man regarding the ethics of cyber world.

Bibliography

Books:

1. Nandan Kamath, Law relating to computers, Internet and e-commerce: A guide to Cyber laws– Delhi: Universal Law Publishing Co. Pvt. Ltd., 2000
2. NA Vijayshanker, Cyber Laws: For Every Citizen in india – Bangalore: Ujvala Consultants Prvt Ltd., 1999
3. Chris Reed, Computer Law, 3rd Edition, London Blackstone Press Pvt Ltd., 1996
4. Ernest Ackermann, Learning to use World Wide Web – New Delhi: BPB Publications, 1996
5. Rahul Matthan, The Law related to computers and the Internet, New Delhi, Butterworths, 2000

Articles:

1. Jambholkar Laxmi, Cyber Law: Issues and Perspective, Indian Journal of International Law, Vol. 40, No. 03, July-Sept 2000, Pg. 559-562
2. Pranam Kumar, Cyber Law is the Need of the Time, Cuttack Law Times, Vol. 89, No. 10, May 2000
3. Mulwad, VH Chalam, Global e-commerce and Cyber Law, Corporate law cases, No. 06, June 2000 Pg 273-78
4. A.V.R. Mayuri (2012), "Phishing Detection based on Visual-Similarity" Conference Proceedings from "International Conference on Network and Cyber Security - 2012" SRK Institute of Technology, Vijayawada, A.P
5. Amit Sharma (2010), "Cyber Wars and National Security - A paradigm shift from Means to Ends" Proceedings from Conference on Cyber Security, "Emerging Cyber Threats & Challenges, (2010)" CII, Confederation of Indian Industry, Chennai
6. Pallavi D Abhonkar, Ashok Kanthe (2012), "Analysis of Tiled Bitmap Forensic Analysis Algorithm for Database Tampering Detection" Proceedings of International Conference on Advances in Computer and Communication

Technology (ACCT-2012) by The Institution of Electronics and Telecommunication Engineers, (IETE) Mumbai

7. Raksha Chouhan, Vijay Singh Rathore (2011), "Electronic Banking Security: Issues, Challenges and Solutions", Proceedings from Conference on Information and Communication Technologies Enhancing Business Competencies through Innovative Practices (2011), Prestige Institute of Management & Research, Indore
8. Ball, Desmond, and Gary Waters. "Cyber Defence and Warfare." *Security Challenges* 9, no. 2 (2013): 91-98
9. R. Ganesan, (2010), "Emerging Cyber Security Trends for 2010", Proceedings from Conference on Cyber Security, "Emerging Cyber Threats & Challenges, (2010)" CII, Confederation of Indian Industry, Chennai.