



NATIONAL LAW SCHOOL OF INDIA UNIVERSITY  
BANGALORE

Dissertation submitted in partial fulfilment of the LL.M degree programme for  
the academic year 2011-2013

---

CYBER CRIMES AND INVESTIGATION  
- A CRITICAL ANALYSIS -

---

Under the guidance of  
Prof.S.B.N.Prakash

Submitted by  
VIVEKHA PON  
ID.No. 507  
II year LL.M

## DECLARATION

I, the undersigned, hereby declare that the work titled "**Cyber crimes and investigation – a critical analysis**" is the outcome of the research carried out by me under the able guidance and supervision of Professor S.B.N.Prakash at the National Law School of India University, Bangalore.

I further declare that this work is original, except for such assistance, taken from such sources, as have been referred to or mentioned at the respective places and for which necessary acknowledgments have been made.

I also declare that this work has not been submitted either in part or in whole for any degree or diploma at any other university.

*Pon.Vivekha*


Vivekha.Pon

I.D.No.507

II year LL.M

**CERTIFICATE**

This is to certify that the dissertation entitled "**Cyber crimes and investigation – a critical analysis**" submitted by Vivekha.Pon (I.D.No.507) in partial fulfilment of the LL.M degree programme for the academic year 2011-2013 at the National Law School of India University, is the result of bona fide research satisfactorily carried out by her under my guidance and supervision.



Prof. S.B.N. Prakash,  
National Law School of India University,  
Bangalore.

3<sup>rd</sup> May 2013

## ACKNOWLEDGMENT

I would like to thank a few people who have been instrumental in the completion of this dissertation.

I extend my gratitude to my respected teacher and guide, Prof.S.B.N.Prakash, for providing a lot of guidance and support to finish this dissertation. Sir, this dissertation would have been impossible without your guidance and support. Thank you Sir.

I would like to thank the National Law School of India University for providing me a platform for doing this research, I would like to thank the library staff who have always been helpful during the process of my research.

I would like to thank the officers of the cyber crime police station located at the Carlton House, Bangalore, especially Mr.Chinnaswamy, DSP, for their kind contribution to this work.

I would also like to thank the officers of the Karnataka Judicial Services Academy, especially Mr.Chandrashekar, Director I/c, for providing access to their library.

I would like to thank Surbi Mam for her kind help in completing this dissertation.

Last, but not the least, I would like to thank my family, friends and the almighty for blessing me and guiding me throughout this journey.

Vivekha.Pon

I.D.No.507

II year LL.M

## TABLE OF CONTENTS

<b>CHAPTER I – INTRODUCTION</b>	<b>1-6</b>
1. Introduction	1
2. Meaning of cyber crime	2
3. History of cyber crimes	4
4. Definition of cyber crime	5
<b>CHAPTER II – KINDS OF CYBER CRIMINALS AND TYPES OF CYBER CRIMES</b>	<b>7-19</b>
1. Kinds of cyber criminals	7
2. General cyber crimes	8
3. Specific types of cyber crimes	12
<b>CHAPTER III – IMPACTS OF CYBER CRIME</b>	<b>20-25</b>
1. Potential economic impact	20
2. Impact on market value	21
3. Impact on consumer trust	24
4. Area ripe for exploitation: National Security	25
<b>CHAPTER IV – INVESTIGATION OF CYBER CRIMES AND THE LEGISLATIONS RELATED TO THE SAME</b>	<b>26-55</b>
1. Applicability of Cr.P.C in investigation of cyber crimes	26
2. Definition of investigation	26
3. Classification of offences under the Information Technology Act, 2000	27
4. Who can investigate under the IT Act, 2000	27
5. Preventive action	28
6. Practical aspects involved in investigation of cyber crime	28
7. Procedure followed while investigating a cyber crime	29
8. Investigation of cyber crime through electronic evidence	30
9. Problems involved in application of traditional criminal laws in investigation of cyber crimes	31
10. Tools of investigation of cybercrimes	33

11. Leading electronic evidence before the court of law	35
12. Difficulty involved in investigation of cyber crimes	36
13. Legislations dealing with cyber crimes in India	38
14. Important Sections of IT Act, 2000	39
15. Developments in the IT law	44
16. Criticism on the laws relating to cyber crimes in India	48
17. Criminal liability under Indian Criminal law and the information technology Act, 2000	50
18. Cyber crime convention	52
<b>CHAPTER V – CASE STUDIES RELATED TO CYBER CRIMES</b>	<b>56-70</b>
<b>CHAPTER VI - METHODS TO EFFECTIVELY COMBAT CYBER CRIMES</b>	<b>71-79</b>
1. Methods to effectively combat cyber crime	71
2. Importance of data protection	76
3. Origin and development of laws on data protection	77
4. Cybercrime countermeasures	77
<b>CHAPTER VII – CONCLUSION AND SUGGESTIONS</b>	<b>80-81</b>
<b>ANNEXURE – BIBLIOGRAPHY</b>	<b>82-86</b>
1. List of statutes and conventions	82
2. List of cases	82
3. List of journals	83
4. List of books	84
5. List of articles	85

# CYBER CRIMES AND INVESTIGATION – A CRITICAL ANALYSIS

## Chapter I – INTRODUCTION

### **Introduction:**

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment. The hallmark of criminality is that, it is breach of the criminal law. As per Lord Atkin, “the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences”.

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. However, the means that enable the free flow of information across borders also give rise to a worryingly high incidence of irresponsible behaviour. Any technology is capable of beneficial uses as well as misuse. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment.

However, substantial legal questions have arisen in many contexts. The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. Websites are created and updated for many useful purposes, but they can also be used to circulate offensive content such as pornography, hate speech and defamatory materials. In many cases, the intellectual property rights of authors and artists are violated through the unauthorized circulation of their works. There has also been an upsurge in

instances of financial fraud and cheating in relation to commercial transactions conducted online.

The digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behaviour if they think that they will not face any consequences. In recent years, there have been numerous reports of internet users receiving unsolicited e-mails which often contains obscene language and amounts to harassment. Those who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cyber-stalking'. Women and minors who post their contact details become especially vulnerable since lumpen elements such as sex-offenders can use this information to target potential victims<sup>1</sup>.

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet.<sup>2</sup>

#### **Meaning of cyber crime:**

A crime committed or facilitated via the Internet is a cybercrime. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the Internet.

---

<sup>1</sup> Vishal Dhotre, Crimes against individuals in India and IT Act available at [http://www.siu.edu.in/Research/pdf/Vishal\\_Dhotre.pdf](http://www.siu.edu.in/Research/pdf/Vishal_Dhotre.pdf), last visited on 22.4.2013.

<sup>2</sup> Hemraj Saini and Yerra Shankar Rao, Cyber-Crimes and their impacts: A Review, T.C.Panda/ International Journal of Engineering research and Applications (IJERA), Vol.2, Issue 2, Mar-Apr 2012, pp.202-209.



Most cybercrimes cannot be placed into a single crime category, which makes statistical recording of this activity limited at best. The Internet Crime Complaint Center (IC3) compiles and releases annual reports on the statistics and cybercrime facts. Using statistics and facts, analysts prepare reports on cybercrime trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data in public and private sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime and can lead to victimization as effectively as common physical crimes. The types of crimes that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and provided with a virtual market of available victims. The responsibility falls on individuals to protect themselves and their families through safe online practices<sup>3</sup>.

Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. Two of the most common ways this is done is through phishing and pharming. Both of these methods lure users to fake websites (that appear to be legitimate), where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity. For this reason, it is smart to always check the URL or Web address of a site to make sure it is legitimate before entering your personal information.

Since cybercrime covers such a broad scope of criminal activity, the examples above are only a few of the thousands of crimes that are considered cybercrimes. While computers and the Internet have made our lives easier in

---

<sup>3</sup>Cyber crimes, National Crime Prevention Council available at <http://www.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf>, last visited on 22.4.2013

many ways, it is unfortunate that people also use these technologies to take advantage of others<sup>4</sup>.

The term can also be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represent the cyber crime as "Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data."<sup>5</sup>

### **History of cyber crimes:**

History reveals that the Cyber crime originated even from the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime<sup>6</sup>.

### **Definition of cyber crime:**

The term 'cyber crime' has not been defined in any Statute or Act. The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet.

---

<sup>4</sup> Cyber crime, available at <http://www.techterms.com/definition/cybercrime> last visited on 20.4.2013.

<sup>5</sup> Essay on computer cyber crime available at <http://www.directessays.com/viewpaper/3856.html>, last visited on 15.3.2013.

<sup>6</sup> Justice K.N.Basha, Seminar and workshop on detection of cyber crime and investigation, 28.06.2010 to 29.06.2010 available at <http://www.hcmadras.tn.nic.in/jacademy/article/Cyber%20Crime%20by%20KNBJ.pdf>, last visited on 22.04.2013.

The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of special knowledge or expert use of computer technology. Cyber Crime could reasonably include a wide variety of criminal offences and activities<sup>7</sup>.

CBI Manual defines cyber crime as:

(i) Crimes committed by using computers as a means, including conventional crimes.

(ii) Crimes in which computers are targets.

A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both".

Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

These definitions, although not completely definitive, do give us a good starting point—one that has some international recognition and agreement—for determining just what we mean by the term cybercrime.

In Indian law, cyber crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act provides the backbone for e-commerce and India's approach has been to look at e-

---

<sup>7</sup> Cyber crime, Encyclopedia Britannica available at [www.britannica.com/EBchecked/topic/130595/cybercrime](http://www.britannica.com/EBchecked/topic/130595/cybercrime), last visited on 28.3.2013.

governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects<sup>8</sup>.

The Information Technology Act, 2000, does not define the term 'cyber crime'. Cyber crime can generally defined as a criminal activity in which information technology systems are the means used for the commission of the crime.

Based on the United Nations General Assembly resolution of January 30, 1997, the Government of India passed the Information Technology Act 2000 (Act No.21 of 2000) and notified it on October 17, 2000. The Information Technology Act, 2000, is the first step taken by the Government of India towards promoting the growth of the E-commerce and it was enacted with a view to provide legal recognition to e-commerce and e-transactions, to facilitate e-governance and prevent computer-based crimes. It is a first historical step.

---

<sup>8</sup> Talwant Singh, Cyber law and information technology, available at <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>, last visited on 15.4.2013.

## CHAPTER II – KINDS OF CYBER CRIMINALS AND TYPES OF CYBER CRIMES

### **Kinds of cyber criminals:**

The Internet space or cyber space is growing very fast and as the cyber crimes. Some of the kinds of Cyber-criminals are mentioned as below.

**Crackers:** These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

**Hackers:** These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

**Pranksters:** These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.

**Career criminals:** These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture"<sup>9</sup>.

**Cyber terrorists:** There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with

---

<sup>9</sup> Mace Brown, Computer Crimes, 2009, Macomb Area Computer Enforcement unit available at <http://www.guru.net/> last visited on 18.3.2013.

traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent.

**Cyber bulls:** Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel email messages are all ways of cyber bullying.

**Salami attackers:** Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers, which deducts a small amount from the account of every customer<sup>10</sup>.

### **General cyber crimes:**

#### **1.1. Data Crime:**

- a) **Data Interception** - An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream.<sup>11</sup>

---

<sup>10</sup> Cyber crime-glossary available at [http://www.virtualpune.com/citizen-centre/html/cyber\\_crime\\_glossary.shtml](http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml), last visited on 22.3.2013.

<sup>11</sup> Common attack pattern enumeration and classification, APEC available at <http://capec.mitre.org/index.html>, last visited on 25.3.2013.

- b) Data Modification - Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites.<sup>12</sup>
- c) Data Theft - Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.<sup>13</sup>

## 1.2 Network crime:

Network Interferences - Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.<sup>14</sup>

## 1.3 Access crime:

- a) "Unauthorized Access" is an insider's view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality.
- b) Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.

---

<sup>12</sup> Oracle, Security overviews, 2003 available at [http://docs.oracle.com/cd/B13789\\_01/network.101/b10777/overview.htm](http://docs.oracle.com/cd/B13789_01/network.101/b10777/overview.htm), last visited on 2.4.2013.

<sup>13</sup> Computer hope, Data theft, 2012 available at <http://www.computerhope.com/jargon/d/datathef.htm> last visited on 3.4.2013.

<sup>14</sup> DSL Reports, Network Sabotage, 2011 Available at: <http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to->, last visited on 10.4.2013.

#### 1.4 **Related crimes:**

##### a) **Aiding and Abetting Cyber Crimes**

There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact"<sup>15</sup>.

b) **Computer-Related Forgery and Fraud:** Computer forgery and computer-related fraud constitute computer related offenses.

c) **Content-Related Crimes:** Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses. The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries. Some of the facts related to cyber crimes can be significantly marked by the information provided by a US base news agency-

- Research study has found that one in five online consumers in the US

---

<sup>15</sup> Legal Info, Crime Overview Aiding And Abetting Or Accessory, (2009) available at <http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory.html>, last visited on 22.3.2014.



have been victims of cybercrime in the last two years.

- RSA, the security division of EMC have released their Quarterly Security Statistics Review concerning identity theft online, phishing and malware, data breaches and data loss.
  - The review found that 23 percent of people worldwide will fall for spear phishing attacks, while web pages are infected on average every 4.5 seconds.
  - In Australia, cybercrime costs businesses more than \$600 million a year, while in the US, one in five online consumers have been victims of cybercrime in the last two years, equating to \$8 billion.
- The review also found that consumers are increasingly concerned about their safety online. The Identity Theft Resource Centre, 2009 Consumer Awareness Survey in the US found that 85 percent of respondents expressed concern about the safety of sending information over the Internet, while 59 percent expressed a need for improvement in the protection of the data they submit over websites.
- One recent report ranked India in 2008 as the fourteenth country in the world hosting phishing websites. Additionally, the booming of call centers in India has generated a niche for cyber criminal activity in harvesting data, the report maintained.
- The words of Prasun Sonwalkar <sup>16</sup> reflects the threat of cyber crime in India "India is fast emerging as a major hub of cyber crime as recession is driving computer-literate criminals to electronic scams, claimed a study by researchers at the University of Brighton. Titled 'Crime Online: cyber crime and Illegal Innovation', the study states that cyber crime in India, China, Russia and Brazil is a cause of "particular concern" and that there has been a "leap in cyber crime" in India in recent years, partly fuelled by the large number of call centers."

---

<sup>16</sup> PTI Contents, India: A major hub for cybercrime, (2009) Available at: <http://business.rediff.com/ slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm>, last visited on 14.4.2013.

From Crime Desk of UK said that online fraud is worth around £50 billion a year worldwide, with criminal gangs increasingly using the latest technology to commit crimes, provoking the Association of Police Officers to state in the FT that "the police are being left behind by sophisticated gangs". Computer spam refers to unsolicited commercial advertisements distributed online via e-mail, which can sometimes carry viruses and other programs that harm computers. For the year to date, the UAB Spam Data Mine has reviewed millions of spam e-mails and successfully connected the hundreds of thousands of advertised Web sites in the spam to 69,117 unique hosting domains, Warner said. Of the total reviewed domains, 48,552 (70%), had Internet domains "or addresses "that ended in the Chinese country code ".cn" . Additionally, 48,331 (70%) of the sites were hosted on Chinese computers. Many of the African countries are lack of the cyber policies and laws (many articles and news are available at in this support). Due to this a cyber criminal may escape even then that is caught. Countries like Kenya, Nigeria, Tunisia, Tanzania etc. are almost free from the cyber laws and policies. The above text only coated only some of the examples related to US, Europe, Asia and Africa to show the horrible situation of cyber crimes. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber crimes and their impacts over society with the future trends of cyber crimes are explained.

### **Specific types of cyber crimes<sup>17</sup>:**

#### **1. Phishing:**

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details. Phishing often directs users to enter details in a fake website who's URL, look and feel are almost identical to the legitimate one. Even

---

<sup>17</sup> M.Loganathan and Dr.E.Kirubakaran, A study on cyber crimes and protection, IJCSI, Vol.8, Issue 5, No. 1, Sep 2011 available at <http://ijcsi.org/papers/IJCSI-8-5-1-388-393.pdf>, last visited on 22.4.2013.

when using SSL with strong cryptography for server authentication it is practically difficult to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploit the poor usability of current web security systems<sup>18</sup>.

Once the attacker has established a realistic and convincing fake web site that mimics a trusted brand, their main challenge is how to divert users of a legitimate web site to the fake web site instead. Unless the Phisher has the ability to alter the DNS for a target web site (DNS poisoning) or somehow otherwise redirect network traffic. A technique sometimes referred to as Pharming, they must instead rely on some form of content level trickery to lure unfortunate users to the fake web site. The better the quality of the lure, and the wider the net that can be thrown, the greater the chance of an innocent user mistakenly accessing the fake website and in the process potentially providing the Phisher with the victim's credentials or other personal data).

## **2. URL obsifucation:**

Using URL obfuscation techniques, the attacker tricks the customer into connecting to their proxy server instead of the real server. For example, the customer may follow a link to <http://www.mybank.com.ch/> instead of the original link <http://www.mybank.com/>. This will result in the customer being cheated.

## **3. Pharming:**

Pharming is a hacker's attack aiming to redirect a website's traffic to another bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in Domain Name System's (DNS) server software. DNS

---

<sup>18</sup> Symantec Brightmail, Anti Phising, White paper: Messaging security available at [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-symc\\_brightmail\\_anti\\_phishing\\_WP-20717027.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_brightmail_anti_phishing_WP-20717027.en-us.pdf), last visited on 2.04.12013.

servers are computers responsible for resolving the Internet names into their real addresses. Compromised DNS servers are sometimes referred to as "Poisoned". DNS cache poisoning is a maliciously created or unintended situation that provides data to a Domain Name Server that did not originate from authoritative DNS sources. Once a DNS server has received such non-authentic data and caches it for future performance, it is considered poisoned, supplying the non-authentic data to the clients of the server.

In recent years both have been used to steal the end user's identity information. Sophisticated measures known as anti-Pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot guarantee to protect against Pharming.

#### **4. Anatomy of phishing:**

A raw phishing message can be split into two components: the content and the headers. These components are commonly accepted as being the major components of a message.

1) Content: The content is the part of the message that the user sees and is used by phishing message producers to deceive users. It can be subdivided into two parts.

(i) The cover is the content which is made to look like a message from the legitimate organization, and usually informs the user of a problem with their account. Early phishing messages could be identified based only on their cover, due to imperfect grammar or spelling mistakes (which are uncommon in legitimate messages). Over time, the covers used in phishing messages have become more sophisticated, to the point where they even warn the users about protecting their password and avoiding fraud.

(ii) The sting is the part of the content that directs the victim to take

remedial actions. It usually takes the form of a clickable URL that directs the victim to a fake website to log into their account or enter other personal details. We call this the sting, as this is the part of the content that inflicts pain, by means of financial loss or other undesirable action after the victim enters their details on the website. Typically the sting is hidden by using HTML to display a legitimate looking address, instead of the address of the fake website.

2) Headers: The headers are the part of the message which is primarily used by the mail servers and the mail client to determine where the message is going and how to unpack the message. Most users do not see these headers, but in terms of determining if a message is phishing or not, this part of the message can be quite useful. Headers can be subdivided into three parts based on the entities which add them to the message:

(i) Mail clients typically add headers such as "To:", "From:", "Subject:" and some client specific headers. Examples of mail client headers are X-MSMail-Priority, X-Mailer, and X-MimeOLE, Phishing messages may try to fake a particular header and in doing so, give away that the message is fake. For example, if the X-Mailer header indicates that a HTML message has been composed using MS Outlook but the message only contains HTML (without plaintext), this is an indication that the message is fake, as MS Outlook cannot send HTML only messages.

(ii) Mail relays will add headers along the path of the message. These are usually "Received" headers, which can be used to determine the originating IP of the message and the path taken by the message.

(iii) Spam-filters or virus scanners will usually add headers to the message to indicate results of the tests run over the message. These headers can then be used by the receiving client to determine (based on

a user-set threshold) what to do with the message<sup>19</sup>.

#### **5. Man in the middle attack:**

One of the most successful vectors for gaining control of customer information and resources is through man-in-the-middle attacks. In this class of attack, the attacker situates themselves between the customer and the real web-based application, and proxies all communications between the systems. From this vantage point, the attacker can observe and record all transactions. This form of attack is successful for both HTTP and HTTPS communications. The customer connects to the attackers' server as if it was the real site, while the attackers' server makes a simultaneous connection to the real site. In the case of secure HTTPS communications, an SSL connection is established between the customer and the attackers proxy (hence the attackers system can record all traffic in an unencrypted state), while the attackers proxy creates its own SSL connection between itself and the real server. For man-in-the-middle attacks to be successful, the hacker must re-direct the user to his proxy server instead of the real server. This may be carried out through:

- DNS Cache Poisoning
- URL Obfuscation

#### **6. Identity theft:**

Identity theft is undertaken by an individual or numerous individuals in order to facilitate criminal activity. Specifically, it involves stealing another person's "identity"—personal and financial information—for the purpose of committing other crimes constituting fraud. More often than not, these fraudulent acts are perpetrated by someone known to the victim such as a relative, friend, employee, or coworker, etc. Further, the

---

<sup>19</sup> Danish Irani et al, PuCollege of Computing Georgia Institute of Technology Atlanta, "Evolutionary Study of Phishing"; eCrime Researchers Summit, 2008.

success of these criminal acts directly depends upon the victim not knowing about it and the perpetrator of the act having an authentic address (one, however, that is actually bogus for the criminal).

(i) Constructions of Identity

According to Finch (2003) "identity theft spans a wide spectrum of conduct and covers varying degrees of fraudulent behavior." p.86 She states that in considering the nature of identity theft, it is important and necessary to distinguish between individual, social, and legal constructions of identity, terms she developed based on the work of Goffman (1963). Clearly, her intent in making these distinctions is to establish a clear delineation between identity and identifiability. In her taxonomy, "Individual identity is concerned with the question of 'who am I.'" It is "what most of us think of when we think of the deepest and most enduring features of our unique selves that constitute who we believe ourselves to be". "It can be seen as the sense of self that is that is based upon the internalization of all that is known about oneself...Hence individual identity is more than simply self-perception; rather, it is a subjective construction of the self that is modified by reflections on the views of others and the individual's interactions in the social world. As such individual identity is not a static construction but one that is constantly evolving and readjusting in line with the individual's life experience." Social identity, on the other hand, is concerned with the question of 'what is the nature of this person.'

While individual identity "can be influenced by the way an individual is received in society," social identity "is contingent upon the way in which individuals present themselves." "For Goffman, social identity is based upon the categorisation of an individual to determine the acceptability of the membership of certain social groups." The key point to consider here, according to Finch, is that while both individual identity and social identity may be affected by identity theft, neither can be stolen. Legal identity is of concern in discussions of identity theft, because given

its “fixed” and “immutable” nature; it has the greatest potential of being abused. Legal identity is concerned with the question of ‘who is this person.’ and “is more concerned with identifiability rather than identity as it seeks to make the link between a collection of facts and the person to whom they relate. Therefore, it is clear that “the legal construction of identity gives primacy to factual information regarding an individual; information that is largely unalterable.”

#### (ii) Traditional Versus Online Identity Theft

According to the better business bureau, “identity theft is more prevalent offline with paper than on-line.” On-line channels are blamed in only 9% of cases. Traditional means of obtaining information fraudulently include:

- (1) dumpster diving (going through trash bins for checks, credit card numbers, identification numbers, pins, passwords, social security numbers, mail, receipts, or other sensitive information);
- (2) shoulder surfing (involving watching someone enter personal information or eavesdropping on personal conversation/information);
- (3) insider abuse (stealing on the job, bribing employees, etc);
- (4) and lost wallets or purses (providing access to credit cards, checks, etc).

Online Identity theft happens in a number of ways including:

- (1) Social Engineering—where users are manipulated into giving sensitive information (also used in f-t-f);
- (2) Phishing—As explained in detail in the previous section of this paper where a spurious site imitates a well-known site;
- (3) Pharming— As explained in detail in the previous section of this paper where malware redirects traffic destined for a legitimate website to one which looks like the original site;
- (4) and Hacking—where the perpetrator intrudes into the system illegally and steals files (can be a method that is part of phishing or pharming).

#### **7. Social engineering:**

Social engineering is the practice of manipulating users to obtain



confidential or sensitive information. Rather than exploiting the security of the technology, the social engineer exploits the weaknesses of the human user to trust the manipulator. It can apply to either to face-to-face, telephone, or internet manipulation to gain access to the physical computer itself or the information on it. Advance-fee scams (i.e. 419 scams) are an example of social engineering. The scam artist, pretending to be anyone from a government official to a surviving spouse, uses fee solicitation to acquire personal information with the promise of sharing inheritances, lottery winnings, and other sums of money. They play on the goodness and compassion of the victim with poignant stories, polite rhetoric, and the "guarantee" of financial gain for all involved. It usually involves the victim first being persuaded to open an e-mail attachment, followed by a malicious attack on the victim's computer, and the victim's computer or information then being used for criminal purposes, be it sending spam or stealing identities.<sup>20</sup>

---

<sup>20</sup> Rae Carrington, Schipke Department of English Central Connecticut State University, "The Language of Phishing, Pharming, and Other Internet Fraud—Metaphorically Speaking"; Technology and Society, 2006. ISTAS 2006.

## CHAPTER III – IMPACTS OF CYBER CRIME

### **Impacts of cyber crime:**

Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime. As criminals move away from traditional methods, internet-based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime.

Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals. In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries.

#### **a) Potential economic impact:**

The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime in 2010. These criminal acts resulted in \$32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online.

As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated that as many as 80% of the companies' surveyed acknowledged as many as 80% of the companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was \$450 million. Almost 10% reported financial fraud. Each

week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks.□As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy. The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem.□Productivity is also at risk. Attacks from worms, viruses, etc. take productive time away from the user. Machines could perform more slowly; servers might be inaccessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization. In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions and bear going into more detail<sup>21</sup>.

**b) Impact on market value:**

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies' that provide cyber-risk policies. For example, a

---

<sup>21</sup> Kevin G. Coleman, Cyber Intelligence: The Huge Economic Impact of Cyber Crime, 19.09.2011 available at: <http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/>, last visited on 30.3.2013.

ruling in favor of Ingram. Micro stated that "physical damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality". This new and evolving view of damage becomes even more important as many firms rely on information systems in general and the Internet in particular to conduct their business. This precedent may force many insurance companies to compensate businesses for damage caused by hacker attacks and other security breaches. As the characteristics of security breaches change, companies continually reassess their IS environment for threats. In the past, CIOs have relied on FUD—fear, uncertainty, and doubt— to promote IS security investments to upper management. Recently, some insurance companies created actuarial tables that they believe provide ways to measure losses from computer interruptions and hacker attacks. However, these estimates are questionable mostly due to the lack of historical data. Some industry insiders confess that the rates for such plans are mostly set by guesswork. As cited in: "These insurance products are so new, that the \$64,000 question is: Are we charging the right premium for the exposure" Industry experts cite the need for improved return on security investment (ROSI) studies that could be used by insurance companies create "hacking insurance", with adjustable rates based on the level of security employed in the organization and by the organization to justify investments in security prevention strategies.

Depending on the size of the company, a comprehensive assessment of every aspect of the IS environment may be too costly and impractical. IS risk assessment provides a means for identifying threats to security and evaluating their severity. Risk assessment is a process of choosing controls based on the probabilities of loss. In IS, risk assessment addresses the questions of what is the impact of an IS security breach and how much will it cost the organization. However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the following reasons:

1. Many organizations are unable or unwilling to quantify their financial

losses due to security breaches.

2. Lack of historical data. Many security breaches are unreported. Companies are reluctant to disclose these breaches due to management embarrassment, fear of future crimes, and fear of negative publicity. Companies are also wary of competitors exploiting these attacks to gain competitive advantage.

3. Additionally, companies maybe fearful of negative financial consequences resulting from public disclosure of a security breach. Previous research suggests that public news of an event that is generally seen as negative will cause a drop in the firm's stock price.

Risk assessment can be performed using traditional accounting based measures such as the Return on Investment (ROI) approach. However, ROI cannot easily be applied to security investments. To justify investment in IS security, CIOs will need to (1) present evidence that the costs of a potential IS security problem outweigh the capital investment necessary to acquire such a system and (2) prove the expectation that the IS security system's return on investment will equal or exceed that of competing capital investment opportunities. This is difficult to accomplish since if the security measures work—the number of security incidents are low and there are no measurable returns. Accounting-based measures such as ROI are also limited by the lack of time and resources necessary to conduct an accurate assessment of financial loss. Instead, companies' IT resources are devoted to understanding the latest technologies and preventing future security threats. In addition, potential intangible losses such as "loss of competitive advantage" that result from the breach and loss of reputation are not included because intangible costs are not directly measurable.

Therefore, there is need for a different approach to assess the risk of security breaches. One such approach is to measure the impact of a breach on the market value of a firm. A market value approach captures the capital

market's expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure than by the attack itself. Moreover, managers aim to maximize a firm's market value or minimize the risk of loss of shareholder value. Therefore, in this study we elected to use market value as a measure of the economic impact of security breach announcements on companies. In the following section we define a security breach as an unexpected event and discuss the characteristics of DOS attacks<sup>22</sup>.

**c) Impact on consumer trust:**

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long-term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths. According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The perception that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce. Complicating the matter, consumer perceptions of fraud assess the state to be worse than it actually is. Consumer perception can be just as powerful or damaging as fact. Therefore, it has to be handled. Hence users' concerns over fraud prevent many online shoppers from transacting business. Concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of security risk or amateurish commerce seriously jeopardizes potential business.

---

<sup>22</sup> R.Baskerville, 1991, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, *European Journal of Information Systems*, 1(2), pp.121-130.

#### **d) Area ripe for exploitation: National Security:**

Modern military of most of the countries depends heavily on advanced computers. Information Warfare, or IW, including network attack, exploitation, and defense, isn't a new national security challenge, but since 9/11 it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation. Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration.

The Internet has 90 percent junk and 10 percent good security systems. When intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the wide spread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of their country of residence. Most of such crimes have been originating in developing countries. The wide spread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities<sup>23</sup>.

---

<sup>23</sup> Nilkund Aseef et al, Cyber-Criminal Activity and Analysis, White Paper, (2005), Group 2.

## CHAPTER IV – INVESTIGATION OF CYBER CRIMES AND THE LEGISLATIONS RELATED TO THE SAME

### **Applicability of Cr.P.C in investigation of cyber crimes:**

Section 4(2) of the Cr.P.C provides that offences under any other law shall also be investigated, inquired into, tried or otherwise dealt according to the Cr.P.C, subject to any special provisions applicable under the special law. Thus the Cr.P.C generally governs the investigation, trial, etc., of offences under the IT Act also. However, there are certain exceptions to the rule as IT Act prescribes certain special procedure. They are contained in Sections 78 and 80 of the IT Act. They read with Section 81 which provides for overriding effect to the Act hence they prevail over Cr.P.C in those respects. The applicability of Cr.P.C is further clarified by clause (3) of Section 80 itself which stipulates that, subject to the procedure given in this section the procedure provided in Cr.P.C will apply.<sup>24</sup>

### **Definition of investigation:**

The term investigation is defined under Section 2(h) of the Criminal Procedure Code. According to this provision, "investigation" includes all the proceedings under this Code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorised by a Magistrate in this behalf;

A three Judge Bench in H.N. Rishbud v. State of Delhi<sup>25</sup>, while dealing with investigation, has stated that under the Code, investigation consists generally of the following steps:

- (a) Proceeding to the spot,
- (b) Ascertainment of the facts and circumstances of the case,

---

<sup>24</sup> Harshwardhan, Investigation of computer crime: Issues and challenges, 2008 Cri.LJ 2 at p.18.

<sup>25</sup> H.N.Rishbud v. State of Delhi, AIR 1955 SC 196.



(c) Discovery and arrest of the suspected offender,

(d) Collection of evidence relating to the commission of the offence which may consist of:

(i) The examination of various persons (including the accused) and the reduction of their statements into writing, if the officer thinks fit,

(ii) The search of places or seizure of things considered necessary for the investigation and to be produced at the trial, and

(e) Formation of the opinion as to whether on the material collected there is a case to place the accused before a Magistrate for trial and if so taking the necessary steps for the same by the filing of a charge-sheet under Section 173<sup>26</sup>.

#### **Classification of offences under the Information Technology Act, 2000:**

The First Schedule of the Code of Criminal Procedure, 1973 provides the classification of offences. Section 77B of the Information Technology Act, 2000 also provides for the method to classify the offences under the Act. According to this Section, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable." Therefore, the operation of 1st Schedule of the Cr.P.C. has been made inapplicable by insertion of this section<sup>27</sup>.

#### **Who can investigate under the IT Act, 2000:**

The Section 78 of the IT Act is amended by way of the 2008 amendment Act to confer power to investigate offences under the Act from DSP level to Inspector level. This will be instrumental in quicker investigation in the cybercrime cases provided adequate tools and training is provided.

<sup>26</sup> Dr.K.N.Chandrasekharan Pillai, R.V.Kelkar's criminal procedure, Fifth edn., Eastern book company, Lucknow at p.121.

<sup>27</sup> Vakul Sharma, Information technology law and practice, Third edn., Universal publications at p.163.

Section 80 has been amended and power to enter and search in a public place is now vested in any police officer not below the rank of inspector or any authorized officer of central government or state government. Such officer is empowered to arrest without warrant a person found therein who is reasonably suspected of having committed or of committing or being about to commit any offence under this Act.

#### **Preventive action:**

Chapter XI of the Cr.P.C confers power for preventive action. It is broadly applicable to cognizable offences. A person could be arrested and prevented from committing a cognizable offence at a private or public place<sup>28</sup>. These provisions are applicable to the offences under the IT Act also and a similar action, Subject to Section 78 may be taken under the IT Act. Section 80 of the IT Act provides for preventive actions and confers special powers and any person can be arrested on reasonable suspicion. However it is applicable only to public places and would apply irrespective of the facts whether the offence about to be committed at a public place is cognizable or non-cognizable.<sup>29</sup>

#### **Practical aspects involved in investigation of cyber crime:**

In order to understand the practical aspects involved in the investigation of cyber crimes, the researcher, as per the recommendation of the respected guide, approached the Cyber Police Station located in the Carlton house, Bangalore. This is the nodal office for the whole state of Karnataka. The researcher was referred to Mr. Chinnaswamy, DSP, Cyber crimes cell, who gave a very useful insight about the investigation procedure in cyber crimes.

The officer rightly pointed out that after the amendment to the Information Technology Act, 2000, that took place in the year 2008 and notified in the year 2009, Section 78 was duly amended empowering a police officer not below the

---

<sup>28</sup> Refer Section 149-151 of Criminal Procedure Code.

<sup>29</sup> Justice Yatindra Sinha, Cyber laws, 2<sup>nd</sup> edn., Universal Law Publishing Co. at p.23.

rank of Inspector to investigate any offence under the Act.

Therefore, whenever a case is reported, the local police station registers the case and in case they need any technical assistance, they approach the cyber crime police station for the same. The nodal office then procures the technical data from the concerned service provider. Usually, the nodal office deals only with very sensational cases referred by the Government and those crimes that are serious in nature.

Once a cyber crime is reported, the police track the IP address of the computer system using which the crime was committed. Using the IP address, the physical address can be tracked by having access to the Customer Application Form in which the address proof is given. But the problem arises when the address proof given is fake. Usually, criminals use cyber cafes to commit crime. The cyber cafes do not maintain a proper record of the customers irrespective of the notifications issued by the government to that effect.

**Procedure followed while investigating a cyber crime:**

When a cyber crime is reported, police track the place from which the crime has been committed and then proceed to the spot along with a technical expert. After reaching the spot, the expert examines the equipment to detect whether there is prima facie evidence to implicate the accused. On the other hand, if the accused is arrested beforehand and is volunteering to produce the equipment, then a voluntary statement is obtained from the accused. After the equipment is seized, the panchayatdhars or the mahazar witnesses who are present in the spot while the investigation is being conducted, prepare a written document called the mahazar, which would contain a detailed description of the investigation that is conducted. Signatures of the mahazar witnesses are obtained on the mahazar.

After the equipment is brought to the police station, a property form is prepared and sent to the magistrate requesting permission for keeping the

property in the custody of the police till the investigation is over. Once the permission is granted, the equipment is examined by the technical experts to detect the crime that is reported.

**Investigation of cyber crime through electronic evidence:**

- **Internet Protocol Address – IPA**

When a person wishes to connect to the internet, he/she makes a request to the Internet Service Provider (ISP). The ISP verifies the identity of the person seeking to connect, through the user name and password. Connectivity to the internet is given through a gateway. At the time when the internet connectivity is given to the person who requested for it, an IPA is allocated. Every connectivity to the Internet is allocated an IPA that is unique and exclusive.

Therefore, the first action an investigator on receiving a criminal complaint of a cyber crime or other crimes in which a computer and the internet are suspected to have been used, should request the telephone service provider and the ISP to retain the IPA logs etc. of the Internet connectivity that is under investigation.

- **Media access control No. (MAC No.) and International Mobile Equipment Identification No. (IMIE No.):**

Even computers and mobile phone handsets are substantially identifiable through the MAC and IMIE numbers respectively. The IMIE number that is allocated to every mobile phone is not only unique but it also used by the telecom service provider to activate the mobile phone and for enabling the incoming and outgoing phone calls. Once the judge understands the credibility of the identification system through the IPA maintained in the logs records of the ISP, and records of the telecom service provider, many of the facts and circumstances in a particular case may stand proven.

- **Tracking of e-mails and websites:**

The full header view of e-mail provides the entire path of the journey from

its origin to its destination, including the originating IPA etc. There is usually a link provided on the email web page that provides the route followed by the e-mail from its origin to its destination. Since in the perception of our lawmakers there is some certainty that an e-mail that is fed into the electronic mail server by the originator corresponds with the e-mail that is received by the addressee, Section 88A of the Indian Evidence Act, 1872 gives discretion to the court to raise a presumption in this regard.<sup>30</sup>

**Problems involved in application of traditional criminal laws in investigation of cyber crimes:**

In traditional procedural laws, there exist some cooperation in the form of conventional mutual assistance agreements, particularly the procedure of the letter. This procedure in which a State is requested to undertake an investigation on its own territory on behalf of the investigating state is highly time consuming one. But when it comes to cyber crimes, any process that is time consuming will be of practically no use since it becomes easy for the accused to destroy any evidence of his/her act. Some of the specific issues faced by real world law in investigating virtual world crimes are briefly discussed in the following sub paras.

**a) Search and seizure in automated information systems:**

The investigating agencies need to be careful in dealing with possible evidence in computer systems since such evidence is susceptible to easy alteration and often challenged in the courts for authenticity. Association of Chief Police Officers of the United Kingdom provides following principles as guidelines, for police officers handling computers as evidence:

- Principle 1: No action taken by the police or their agents should change data held on computer or other media, which may

---

<sup>30</sup> Vivek Sood. Nabhi's Cyber crimes, electronic evidence and investigation, legal issues, 1<sup>st</sup> revised edn. 2010, a Nabhi Publication at pp.203-213.

subsequently be relied upon in court.

- Principle 2: In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to computer-based evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- Principle 4: The officer in charge of the case is responsible for ensuring that the law and these principles are adhered to.

**b) Duties of active cooperation:**

Even in jurisdictions where there are express provisions as to search and seizure of electronic data contained in a computer or computer systems the level of technical knowledge in traditional investigating agencies make it difficult for carrying out such operations. Computer forensics requires extensive knowledge of computer hardware, operating systems, software and data-processing systems. The availability of security software and encryption software further increases the difficulty in deciphering stored data. In the traditional systems of evidence collection, there are two instruments are being relied upon by investigating agencies to overcome similar problems. They are the duty to surrender seizable objects and the duty to testify.

- Duty to surrender seizable objects:

Section 91 of the CrPC requires any person who is in possession of having or in whose power a document or thing that is necessary or desirable for the purpose of any investigation or trial is believed to be, to attend and produce or to produce such document or thing when a court issues summons or an investigating officer issues a written order to do so. Such duty to cooperate in searches and to surrender the seizable objects can help the investigating officers in

selecting specific data carriers from among the many that are usually stored in the computer centre.

➤ **Duty to testify:**

The second important instrument of active cooperation is the duty to testify. Sections 160-163 of CrPC provide for power of investigating officers to require attendance of witnesses and their examination. Section 29(2) of the Information Technology Act, 2000 confers such a duty of active cooperation upon persons in charge of computer systems or data.

**c) Wire tapping:**

Tapping of telecommunication lines and eavesdropping on computer networks is unavoidable in investigating cyber crimes, especially where data are only transmitted and not permanently stored, or where data merely cross a country or where permanent observation of telecommunication or computer activities is necessary.

Specific power to intercept information transmitted through any computer resources is provided by Section 69 of the Information Technology Act, 2000.<sup>31</sup>

**Tools of investigation of cybercrimes:**

The following are the tools of investigation of cyber crimes:

• **Data Recovery Programs:**

Data recovery programs are software used to extract information from a computer's hard drive after it has been erased or damaged. Most programs can restore deleted files and provide a list of all storage devices currently attached to the computer the drive is in. This type of software is used to recover files that a suspect may have tried to remove, such as evidence of a child pornography ring. Not all data will be

---

<sup>31</sup> S.V.Joga Rao, Law of cyber crimes and information technology law, Edn. 2004, Wadhwa & Company, Nagpur at p.177.

recoverable. The quality of the files retrieved depends on certain factors, like what method was used to delete the files and the physical state of the hard drive itself.

- **Honeypots:**

Honeypots, in cyber crime, are traps set for criminals interested in specific information. Typically, a honeypot is a computer or website that appears to be part of a larger network and is relatively easy to access without proper permission. In reality, the honeypot is isolated and being closely monitored by whoever set the trap. For example, a honeypot that is being designed to trap a credit card fraud ring may contain fake credit card account information and other lures to entice a criminal in the ring to illegally access it. From there, information on the location and the method of the criminal may be revealed to the person monitoring the honeypot.

- **IP Address Tracking:**

An Internet protocol (IP) address is a number assigned to a computer or other device on a network accessing the Internet. This number can reveal specific information about the computer that is using it, such as a general location or even the name of the owner. Tracking software can be used in order to create information logs of IP addresses used by criminals in the commission of a crime. Because IP addresses can be hidden, "bounced" from computer to computer or even altered, success using this software depends on the level of skill of both the person using it and the person committing the crime.

- **Chat Room Monitors:**

Chat rooms are the online gatherings of individuals interested in a particular subject who talk to each other in real time. They are sometimes a target for law enforcement investigations. A popular website for children may lure pedophiles, and an officer or agent will go online



and pose as a member of the chat room in order to catch the pedophile in the act of soliciting a minor. Programs are now used to monitor and record chat sessions, as well as flag any words or phrases specified by the person using the program<sup>32</sup>.

### **Leading electronic evidence before the court of law:**

The step-by-step process involved in leading electronic evidence before the court of law is provided below:

- Admissibility and relevancy:

Admissibility of evidence implies the legal permissibility to adduce the same. Evidence that is barred under the Indian Evidence Act can be said to be inadmissible. The concept of relevancy of a fact implies the bearing it has on the case. Facts that are relevant are exhaustively provided in the India Evidence Act, 1872 from Sections 6-55 in Chapter II.

- Proof of electronic record:

Electronic records have been granted legal status by Section 4 of the IT Act, 2000. Since electronic records are generated in the computer system, for proving the same by primary evidence as stipulated by Section 64 of the Indian Evidence Act, 1872, the computer system would be required to be produced in the court. For avoiding inconvenience to litigants, of having to bring the computer system to the Court as proof of primary evidence of record, Section 65B has been introduced into the Indian Evidence Act, 1872 vide the IT Act, 2000. Section 65B is an exception to the rule of primary evidence in so far as the electronic record is concerned. Sub-section (1) of Section 65B grants admissibility to the

---

<sup>32</sup> Anna Assad, Cyber crime investigation tools available at [http://www.ehow.com/list\\_6529303\\_cyber-crime-investigation-tools.html](http://www.ehow.com/list_6529303_cyber-crime-investigation-tools.html), last visited on 23.5.2013.

secondary evidence of an electronic record.<sup>33</sup>

**Difficulty involved in investigation of cyber crimes:**

The investigation of cyber crimes is complex. The evidence is often in an intangible form. Its collection, appreciation, analysis and preservation present unique challenges to the Investigator. The increased use of networks and the growth of the Internet have added to this complexity. Using the Internet, it is possible for a person sitting in India to steal a computer resource in Brazil using a computer situated in USA as a launch pad for his attack. Distributed attacks are also not unheard of. The challenges in such cases are not only technological, but also jurisdictional.

Of late, we are experiencing more and more of cyber crimes, since many of us have switched over to the fourth mode of communication i.e. Internet from the previous modes viz. gestures, speech and writing. The internet has opened up avenues of commerce, trade and communication like never before. It is the network that deals in billions of transactions each day. These transactions are usually transactions of money, pictures, information and videos. The magnitude of transactions – the sheer volume makes internet not just an easy tool for information exchange, but also an ideal hotbed of crimes.

Internet provides anonymity and safety. Unlike other forms of crimes wherein the person undertakes considerable risk, cyber crime provides the criminal with a cover. He leaves no physical foot-prints, finger-prints or other tangible traces making it extremely difficult to track cyber criminals down.

Cyber crime being technology driven evolves continuously and ingeniously making it difficult for investigators to cope up with changes. Criminals are always one step ahead in the sense that they create technology or come up with technique to perpetrate a particular crime and the law enforcers

---

<sup>33</sup> Dr.Farooq Ahmed, Cyber Law in India, 2<sup>nd</sup> Edn., 2005, New Era Publications at p.302.

then counter such techniques or technologies<sup>34</sup>.

In cyber crime cases, the investigator's challenge is to establish the crime beyond reasonable doubt using digital evidence that exist in cyber space. This requires Computer or Cyber Forensics special skills, equipments, lab and capabilities far different from conventional crime detection.

Computer forensics is extremely important to track and establish proof in all computer related offences. According to Section 79A of the Information Technology Act, 2000, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

The computer forensic field has developed techniques to improve the detection, connection, and classification of digital information. Thus the field includes a multitude of systems to extract useful information from computer media and involves the application of varied tools. The stages in computer forensic investigation are usually as follows:

1. Identifying the doer of the crime
2. Locating the means and equipment through which the crime was committed
3. Collection and extraction of the physical evidence
4. Correlating the evidence to the crime and facilitating the arrest of the wrongdoer.

Chain-of-custody is one of the controls used by courts to satisfy admissibility standards. Chain-of-custody is a process consisting of methodical checklists and procedures during the collection, preservation and analysis of evidence for the purpose of establishing authenticity and reliability of evidence.

---

<sup>34</sup> Cyber crimes, Central bureau of investigation Manual, Chapter 18, para 18.2.

In other words, the evidence offeror tries to prove the chain-of-custody in order to rebut or minimize charges that evidence may be tainted or altered.

Thus the authenticity of physical evidence is shown by accounting for who, what, when, where and how a given piece of evidence was transferred from its initial discovery, through its collection, access, handling, storage and eventual presentation at trial. Chain-of-custody has been institutionalized as a procedure for the seizure of physical evidence by law enforcement, as well as for the handling of digital evidence by computer forensic examiners as a measure of evidence integrity.

The Cyber Crime Investigating Officers are enhancing their technical knowledge by undergoing periodical training organized by Central Bureau of Investigation Academy (CBI), Chaziabad, Tamil Nadu Police Academy (TNPA), Chennai, (Tamil Nadu Police Officers), Government Examiner of Questioned Documents (GEQD), Hyderabad, Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram, National Association of Software and Services Companies (NASSCOM), Chennai, Anna University, Chennai and Computer Emergency Response Team-India (CERT-IN), New Delhi<sup>35</sup>.

#### **Legislations dealing with cyber crimes in India:**

India has enacted the first I.T.Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United Nations. Chapter XI of this Act deals with offences/crimes along with certain other provisions scattered in this Acts .The various offences which are provided under this chapter and under IPC are shown in the following table: -

Sending threatening message by email	Section 506 IPC
--------------------------------------	-----------------

---

<sup>35</sup> Justice K.N.Basha, Seminar and workshop on detection of cyber crime and investigation, 28.06.2010 to 29.06.2010 available at <http://www.hcmadras.tn.nic.in/jacademy/article/Cyber%20Crime%20by%20KNBJ.pdf>, last visited on 22.04.2013.

Sending defamatory message by email	Section 499 IPC
Sending a mail outraging the modesty	Section 509 IPC
Forgery of electronic records	Section 465 IPC
Bogus websites, cyber frauds, phishing	Section 420 IPC
Email spoofing	Sections 465, 419 IPC
Web-jacking	Section 383 IPC
Criminal breach of trust	Sections 406, 409 IPC
Online sale of Narcotics	NDPS Act
Online sale of Weapons	Arms Act
Hacking	Section 66 of IT Act
Pornography	Section 67 of IT Act
Email bombing	Section 66 of IT Act
Denial of Service Attack	Section 43 of IT Act
Virus Attack	Sections 43, 66 of IT Act

**Important Sections of IT Act, 2000:**

Section 44 – Penalty for failure to furnish information, return, etc. - If any person who is required under the Act or any rules or regulations made thereunder to -

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure,

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues,

(c) maintain books of account or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Section 45 (Residuary penalty) further covers all other offences that may possibly arise under the act. It provides that "whoever contravenes any rules or regulations made under the Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees" to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Section 46 (Power to adjudicate – Adjudicating Officer) empowers the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry regarding the commission of the offences laid out in Chapter IX in the manner prescribed by the Central Government. The persons appointed shall possess such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government. Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction. This is also discussed in *S.Sekar v. The Principal General Manager (Telecom), (BSNL)*<sup>36</sup>.

Every adjudicating officer appointed as above shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under Section

---

<sup>36</sup> *S.Sekar v. The Principal General Manager (Telecom), (BSNL), MANU/TN/9663/2007.*

58(2). Further all proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code, 1860 and it shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973.

The adjudicating officer shall offer the offender a reasonable opportunity for making representation in the matter. If, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of the Act governing such offence.

Section 47 prescribes the factors to be taken into account by the adjudicating officer while adjudging the quantum of compensation, namely:

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default; (c) the repetitive nature of the default.

Section 65 - Tampering with computer source documents – Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Tampering with computer source documents was discussed in Syed Asifuddin and Ors. v. The State of Andhra Pradesh and Anr.<sup>37</sup>, Jigar Mayurbhai Shah v. State of Gujarat<sup>38</sup>, Pootholi Damodaran Nair v. Babu<sup>39</sup>, and Ravi Shankar

<sup>37</sup> Syed Asifuddin and Ors. v. The State of Andhra Pradesh and Anr., 2005 Cri L J 4314.

<sup>38</sup> Jigar Mayurbhai Shah v. State of Gujarat, (2008) 2 GLR 1134.

<sup>39</sup> Pootholi Damodaran Nair v. Babu, 2005(2)KLT707.

Srivastava v. State of Rajasthan<sup>40</sup>.

Section 66 (Computer related offences)- This Section deals with hacking the Computer System and states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. It further states that whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both. The case of Nirav Navinbhai Shah v. State of Gujarat and Anr.<sup>41</sup> involved Section 66.

Section 67 – Punishment for publishing or transmitting obscene material in electronic form: This Section was in question in many cases<sup>42</sup>.

Sections 76, 68(2), 69 and 70 have been amended by the Information Technology Amendment Act 2008<sup>43</sup>.

Section 71 (Penalty for misrepresentation) This Section prescribes a penalty for any misrepresentation or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate. It states that such cases shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72 (Penalty for breach of confidentiality and privacy) Again if any person who, in pursuance of any of the powers conferred under the Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without

---

<sup>40</sup> Ravi Shankar Srivastava v. State of Rajasthan, 2005(2)WLC612.

<sup>41</sup> Nirav Navinbhai Shah v. State of Gujarat and Anr., MANU/GJ/8458/2006.

<sup>42</sup> Dr. Prakash v. State of Tamil Nadu and Ors., AIR 2002 SC 3533. Fatima Riswana v. State Rep. by A.C.P., Chennai and Ors., (2005) 1 SCC 582.

<sup>43</sup> Also See Firos v. State of Kerala, AIR 2006 Ker 279.



the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished under Section 72 with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 73 (Penalty for publishing (Electronic Signature) Certificate false in certain particulars) If a Digital Signature Certificate that is false in certain particulars is published or made available by a person to any other person with the knowledge that the Certifying Authority listed in the certificate has not issued it, or the subscriber listed in the certificate has not accepted it, or the certificate has been revoked or suspended, then such person shall be punished under Section 73 with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. A publication that is for the purpose of verifying a digital signature created prior to such suspension or revocation, is not penalized under this Section.

Section 74 (Publication for fraudulent purpose). This Section states that whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 75 (Act to apply for offences or contravention committed outside India). This Section accords extra territorial application to the Act and states that the provisions of the Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. The Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. As per Section 76, any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision

of the Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation.

Section 77 (Compensation, penalties or confiscation not to interfere with other punishment). This Section states that in addition to the penalties prescribed by the IT Act, imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force may also be made. The Act as amended gives a police officer not below the rank of Inspector the power to investigate any offence under the Act.

Section 79 (Exemption from liability of intermediary in certain cases)- This Section declares that no person providing any service as a network service provider shall be liable under the Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. This issue was also discussed in the case of Sanjay Kumar Kedia v. Narcotics Control Bureau and Anr.<sup>44</sup>.

The Amendments brought about by the Information technology Act in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 came up for consideration in a catena of cases<sup>45</sup>.

#### **Developments in the IT law:**

One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law any where in the World. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of I.T. Act and amendments made to Indian Penal Code, problems associated with cyber crimes continue to persist.

---

<sup>44</sup> Sanjay Kumar Kedia v. Narcotics Control Bureau and Anr., (2008)2 SCC 294.

<sup>45</sup> Refer to State of Punjab and Ors. v. Amritsar Beverages Ltd. and Ors., (2006) (7) SCC 7.

1. Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyber space the territorial boundaries seem to vanish. Thus the concept of territorial jurisdiction as envisaged under S.16 of Cr.P.C. and S.2 of the I.P.C. will have to give way to alternative method of dispute resolution.

2. Loss of evidence is a very common & expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.

3. Cyber Army: There is also an imperative need to build a high technology crime & investigation infrastructure, with highly technical staff at the other end.

4. A law regulating the cyber-space, which India has done.

5. Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

6. Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the P.I.L. (Public Interest Litigation), which the Kerala High Court has accepted through an email.

'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislate the laws and by-laws also are not perfect. The laws therefore enacted by them cannot be perfect. The cyber law has emerged from the womb of globalisation. It is at the threshold of development. In due course of exposure through varied and complicated issues it will grow to be a piece of its time

legislation<sup>46</sup>.

The need for a comprehensive amendment was consistently felt and after sufficient debate and much deliberation, the I.T. Amendment Act 2008 was passed. The ITA, 2008 got the President's assent in February 2009 and was notified with effect from 27.10.2009. The new IT Amendment Act 2008 has brought a large number of cyber crimes under the ambit of the law. Some of the significant points in the Amendment Act include introduction of corporate responsibility for data protection with the concept of 'reasonable security practices' (Sec.43A), recognition of Computer Emergency Response Team – India (CERT-In) as the national nodal agency empowered to monitor and even block web-sites under specific circumstances, introduction of technological neutrality replacing digital signatures with electronic signatures etc. Besides, the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

The IT Act provides legal recognition for transactions carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce", involving the use of alternatives to paper-based methods of communication and storage of information. The IT Act facilitates electronic filing of documents with the Government agencies.

In the present global situation where cyber control mechanisms are important we need to push cyber laws. Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber crime. The 7 stage continuum of a criminal case starts from perpetration to registration to reporting, investigation, prosecution, adjudication and execution. The system can not be stronger than the weakest link in the chain. In India, there are 30 million policemen to train apart from 12,000 strong Judiciary. Police in India are

---

<sup>46</sup> V. Shiva Kumar, Cyber crime-prevention and detection available at <http://www.cidap.gov.in/documents/Cyber%20Crime.pdf>, last visited on 22.4.2013.

trying to become cyber crime savvy and hiring people who are trained in the area. Each police station in Delhi will have a computer soon which will be connected to the Head Quarter. The pace of the investigations however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and district judiciary. IT Institutions can also play a role in this area.

Technology nuances are important in a spam infested environment where privacy can be compromised and individuals can be subjected to become a victim unsuspectingly. We need to sensitize our investigators and judges to the nuances of the system. Most cyber criminals have a counter part in the real world. If loss of property or persons is caused the criminal is punishable under the IPC also. Since the law enforcement agencies find it is easier to handle it under the IPC, IT Act cases are not getting reported and when reported are not necessarily dealt with under the IT Act. A lengthy and intensive process of learning is required.

A whole series of initiatives of cyber forensics were undertaken and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems can get invented. We need to move faster than the criminals.

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

For this India needs total international cooperation with specialised agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analysed and the report presented in court is based on this evidence. It has to

maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it. The law is stricter now on producing evidence especially where electronic documents are concerned.

The computer is the target and the tool for the perpetration of crime. It is used for the communication of the criminal activity such as the injection of a virus/worm which can crash entire networks.

The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC.<sup>47</sup>

### **Criticism on the laws relating to cyber crimes in India:**

#### **Jurisdiction:**

Territorial limitation on the internet becomes of peripheral nature in the virtual medium as the web pages on the net can reach almost every province in the nation and conceivably almost every nation on the globe. This is where the point of friction between the cyber world and the territorial world begins as in the territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world.

A judicial system can function effectively if it is well regulated; it is these regulations that identify every functional aspect of the judicial system including the jurisdiction of the courts. A court in order to deliver effective judgments must have proper and well defined jurisdiction, as without a jurisdiction the

---

<sup>47</sup> Talwant Singh, Cyber law and information technology, available at <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>, last visited on 15.4.2013.

court's judgments would be ineffective. Jurisdictions are of two types namely, Personal and Subject Matter jurisdiction, and for a judgment to be effective both these types must exist contemporaneously. Further the conventional requirement as to a party can sue another is at the place where the defendant resides or where the cause of action arises. This itself is the problem with Internet jurisdiction as on the net it is difficult to establish the above two criteria's with certainty.

Issues of this nature have contributed to the complete confusion and contradiction that plague judicial decisions in the area of Internet jurisdiction.

The IT Act 2000 passed in India is a perfect example of the ambiguous law in the area of jurisdiction in the context of the Internet. Section 1(2) provides that the act shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person. Similarly Section 75(2) provided that this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Such a provision appears to be against the principles of justice.

Going to jurisdiction and pass a judgment as per the above provisions of the IT Act 2000, the other question that arises is whether the foreign courts will implement such a judgment. In case of the above predicament the only way to resolve such a dispute is by means of having an extradition treaty with the host nation and India, further it has been suggested by that the Indian court develop justifiable ground on which the extra-territorial jurisdiction may validly be exercised as done by the American Judiciary.

From the above it becomes necessary to appreciate the complexities involved and thus it becomes indispensable to understand the nature of the Cyber crime, and whether the existing penal laws are sufficient.

When Macaulay came up with the Indian penal code in 1860 the notion of Cyber Crimes was completely unknown. Further until the IT Act 2000 was enacted there was no legal provision viz. Cyber Crimes; this was the sole rationale along with recognizing transactions carried on by means of electronic communications to augment the e-commerce, with which the IT Act 2000 was enacted. Further a blanket provision was made under section 77 of the IT Act 2000 which provides that the penalties or confiscations provided under the IT Act 2000 will not release an offender from liability under any other law, in short the substantive provisions of the IPC are still applicable to Cyber Crimes committed in India<sup>48</sup>.

**Criminal liability under Indian Criminal law and the information technology Act, 2000:**

The Indian Criminal Law hovers around the Indian Penal Code, though there are other statutes which provide for criminal liability, but the Indian Penal Code is the sole authority in regard to deciding the conditions required of fulfill criminal liability. Various expressions have been used in defining offences under the Indian Penal Code like 'intention', 'knowledge', etc., but in spite of this clinical treatment of mens rea experience has shown that the courts have imported the Common law maxim of mens rea in the process of interpreting the offence defined under the Indian Penal Code and various other special statutes. Thus the Courts in India have been treating the concept of mens Rea on offence-to-offence basis. Thus it can be said that the maxim "actus non facit reum nisi mens sit rea" as a maxim has no significance to the offences under the Indian Penal Code. Where the code has not indicated any peculiar guilty intent or knowledge etc then the court presumes, by considering the general definition that such an omission was made with some specific intention. In such case it would be unfair to import the maxim and arrive at a judgment declaring the offender guilty.

---

<sup>48</sup> Refer Supra note 1 at pp.2-8.



The Indian Law Commission in its 47th Report has mentioned that as a result of the transition process that the society was going through i.e. from a simple to an industrialized society it has become incumbent to contain the malpractices that were prevailing in the society then as such malpractices were unknown before for instance Unfair Trade Practices, Adulteration in Food, drugs etc, thus to restrain the emerging situation the judiciary and the parliament played a pivotal role in introducing the concept of Strict Liability because it is difficult to prove guilty intension of the offender in such socio-economic crimes. The effect of this was that with the imposition of Strict Liability under Criminal Law was that the burden of proof shifted from the prosecution to the defendant, and the Guilty mind need not be proved example in crimes like hacking it is almost impossible to prove guilty mind.

In regards to the Cyber Crimes under the Information Technology Act, 2000 the Liability is divided into three categories. This has been done in order to avoid broad criminalization of all the wrongful acts in the virtual medium. Firstly there are certain wrongful acts that do not attract criminal liability and mens rea is not applicable to them, such acts are subject to civil penalties and strict liability is imposed on the wrongs of this category e.g. failure to maintain books of accounts, or contaminating the computer with viruses etc.

Secondly there are certain acts where mens rea has been made and fundamental part of the definition of the offence, thus expressions like 'knowledge', 'intension' etc are included in the definition of such offences e.g. tampering with the computer, publishing for fraudulent purposes etc. Lastly there are some acts or omissions that are made criminally liable with strict liability e.g. Penalty for breach of confidentiality and privacy, penalty for misrepresentation etc<sup>49</sup>.

---

<sup>49</sup> Refer Sections 43-45, 65-74 of Information Technology Act, 2000, Sections 154-157 of the Criminal Procedure Code.

## **Cyber crime convention:**

### **a) Purpose of the convention:**

The primary purpose of the Convention is to harmonize domestic substantive criminal law offenses and investigative procedures. The Convention drafters' principal concerns were two-fold. First, they wanted to ensure crime definitions were flexible enough to adapt to new crimes and methods of committing existing crimes as they evolve. Second, the drafters wanted the Convention to remain sensitive to the legal regimes of domestic states. These concerns were especially challenging in the human rights area because states have different moral and cultural values. For example, European nations have a much higher degree of privacy protection than the United States. The United States, on the other hand, has stronger speech protection than other nations. To further its purpose, the Convention also empowers parties to restrict or eliminate criminalization of certain offenses and limit investigative procedures by reservation. The Convention's drafters, thus, attempted to balance crime definitions and the investigative needs of law enforcement with individual rights<sup>50</sup>.

### **b) Evolution of cybercrime convention:**

There are three multilateral organizations that focused on international cyber crime policy: the CoE, the European Union (EU) and the G-8. The Organization for Economic Cooperation and Development (OECD) and the United Nations (UN) also participated, but to a lesser extent.

In response to the increase in cyber crime the CoE's Committee of Ministers adopted Recommendation No. R. (89) 9 ("R89") in 1989, which required that member states consider computer crimes when reviewing old and enacting new legislation. In 1995, the CoE adopted Recommendation No. (95)

---

<sup>50</sup> Shannon L.Hopkins, Cybercrime convention: A Positive beginning to a long road ahead, Journal of high technology law, Vol.II.,No.1, pp.105-110.

13 ("R95") establishing procedures for applying R89. Investigations were still slow and difficult to coordinate, resulting in the untimely information retrieval necessary to combat cyber attacks. Moreover, many countries lacked criminal cyber law statutes. Countries with such laws found their laws were outdated.

In 1997, the CoE formed a Committee of Experts on Crime in Cyberspace ("PC-CY") in response to prior failed efforts to prevent and deter cyber attacks or address the damaging consequences of such acts. The United States Department of Justice (DOJ) also significantly participated in this effort. The CoE finalized the Convention on November 8, 2001 and opened it for signature on November 23, 2001. Twenty-six of the forty-three European member states signed the Convention, along with four non-members states, Canada, Japan, South Africa and the United States. The Convention will become effective when at least five states ratify it, three of which must be European member states<sup>51</sup>.

**c) Need for cybercrime convention:**

Financial gain motivates many cyber criminals. Financial experts agree that cybercrime is most prevalent in the United States because of its financial wealth and the volume of commercial transactions occurring within its borders. Criminals also target the U.S. because of its strong First Amendment protections. Indeed, the U.S. is known amongst the western world as a "haven" for racial and hate speech.

Globally, cyber crimes constitute more than \$15 billion in damages every year. Most organizations do not report cyber crimes because they fear exposure would make them vulnerable to future attacks by copycats or cause a loss of public confidence. The cost and difficulty associated with investigations also hinders a company's willingness to report crimes. Experts predict that developing nations will need to experience significant technological growth over the next decade to be "self-sufficient and more competitive" in an international

---

<sup>51</sup> Baron F Ryan, A critique of the international cybercrime convention, 10, *Commlaw conspectus*, 2002, at pp.263, 269.

economy. Developing countries could thus eventually direct more cyber crimes to the United States, although financial constraints will most likely hinder such growth.

Cyber criminals range in both age and skill level. Studies show, however, that employees are the largest threat. Ostensibly, ex-employees, as corporate insiders, can easily exploit their knowledge of a company's computer network. For example, an employee may steal a company's source code by entering the corporate network remotely through unauthorized access using confidential passwords. Companies could prevent or at least mitigate computer fraud if they focus more on security through password controls, employee training and background checks.

Many states have enacted cyber crime laws. Those laws, however, were confined to a specific territory and were frequently outdated. Perpetrators of crimes have thus gone unpunished. Until we are able to cope with the fast-paced changes of the Internet, new kinds of crimes may continue to go unpunished. Those countries that actually have computer crime legislation will continue to operate under a conglomeration of varied and often disjointed laws. The CoE adopted the Convention in response to the need for harmonization. The Convention is a welcome and necessary advance to international criminal laws. It is, however, largely "aspirational" and fails to provide substantive guidance for defining precisely what conduct constitutes a cyber crime. The Convention also does not identify what specific legal procedures states should apply when investigating and prosecuting cyber crimes<sup>52</sup>.

The Convention is a welcome and long-overdue start towards addressing the exigent circumstances evolving from the Internet revolution. The CoE deserves much credit in accepting such a significant and valuable task. Computer crimes are difficult to solve due to the absence of geographical borders and the

---

<sup>52</sup> Sofaer D. Abraham, et al., A proposal for an international convention on cyber crime and terrorism, Hoover institution, et al., available at <http://oas.org.iuridico/english/monograph.htm> last visited on 23.4.2013.

inherent ability to swiftly transfer and manipulate information instantly. Nevertheless, technological advances will continue to challenge law enforcement officials. As long as long signatories are permitted to codify cyber criminal laws domestically and countries remain unsubscribed to the Convention, authorities may be unable to obtain sufficient evidence to prosecute crimes.

We must reach a global consensus to harmonize not only the crimes themselves but also the investigative and prosecutorial procedures that will enable law enforcement to prevent and convict cyber crimes. Success will hinge upon the cooperation of all countries, both parties to the Convention and those that are not.

## CHAPTER V – CASE STUDIES RELATED TO CYBER CRIMES

### Case studies related to cyber crimes:

#### 1. **Avishek Goenka v. Union of India<sup>53</sup> (PIL for ensuring KYC norms while issue of SIM card):**

The petitioner is a businessman engaged in the business of distribution of pre-paid virtual and tangible calling value for mobile phone subscribers and also sells new customer acquisition packs and follows it up, by collection of customer application forms and executing tele-calling, to verify customer credentials. In this Public Interest Litigation, the petitioner has attempted to highlight the grave issue of non-observance of norms/regulations/guidelines related to proper and effective subscriber verification by various service providers. In fact, according to the petitioner, there is rampant flouting of norms/regulations/guidelines relating to this subject matter and there is no proper verification of the subscribers prior to selling of the pre-paid mobile connections to them.

The Telecom Regulatory Authority of India is the regulatory body for the telecommunications sector in India and the Union of India has responsibility to issue guidelines and frame regulations and conditions of licence, in consultation with the TRAI, to ensure coordination, standardization and compliance with the regulations, as well as protecting the security interests of the country.

The petitioner has averred that the telecom sector has witnessed the most fundamental structural and institutional reforms since 1991. This sector has grown significantly in the last few years. As per the Annual Report for 2009-2010 of the Department of Telecommunication, Ministry of Communications and IT, Government of India, as on 31st December, 2009, the Indian telecom sector had about 5622.11 million connections. The tele-density per hundred population, which is an important indicator of telecom penetration in the country, has

---

<sup>53</sup> Avishek Goenka v. Union of India, W.P.(Civil) No.258 of 2010 before the Supreme Court of India, judgment delivered on 27 April 2012.

increased from 2.32 per cent in March, 1999 to 47.88 per cent in December, 2009. The Eleventh Five Year Plan for 2007-2012 had provided a target of 600 million connections, but the industry has already provided around 700 million connections, thus far exceeding the target. Different random studies in relation to pre-paid Subscriber Identity Module (SIM) cards show widespread violation of guidelines for Know Your Customer (KYC) and even other common guidelines. The SIM cards are provided without any proper verification, which causes serious security threat as well as encourages malpractices in the telecom sector. It appears that 65 per cent of all pre-paid SIM cards issued in Jammu & Kashmir and 39 per cent of all pre-paid SIM cards in Mumbai, may have been issued without verification; which means that 1 out of every 6 pre-paid SIM cards is issued without proper verification. The averment is that such unverified SIM cards are also used in terrorist attacks.

The Petitioner also avers that around 80 per cent of the pre-paid SIM cards may be purchased in pre-activated form which is in violation of the notifications issued by the DoT, dated 22.11.2006 and 23.3.2009 respectively, banning the sale of pre-activated SIM cards. Another significant fact that has been brought out in this petition is that, pre-paid SIM cards, which are the most commonly issued without verification, constitute 96 per cent of the total SIM cards sold. This indicates the seriousness of the problem as well as the security hazard that emerges from the telecom sector.

As a result of this PIL, the DoT accepted to constitute a joint expert committee to discuss and resolve issues re-verification of SIM card, about the need for enhancing the penalty for violating the instructions/guidelines including sale of pre-activated SIM cards, etc.

## **2. Shri Sourabh Jain v. ICICI Bank<sup>54</sup> (SIM card used in banking fraud):**

In this case, from the Complainant's savings bank account with Pune's

---

<sup>54</sup> Shri Sourabh Jain v. ICICI Bank, Complaint No.6 of 2011 dated 12.12.2011 before the office of the adjudicating officer, Government of Maharashtra.

Shivajinagar Branch of ICICI bank, Rs.2.02 lakh was transferred on 15/10/2010 and 16/10/2010 in 15 fraudulent transactions into unknown ICICI Bank's accounts. The Complainant filed a Police complaint with Shivajinagar Police Station. According to the police, the money was transferred using the internet banking id, password and transaction password and all the addresses provided for the accounts where money was transferred are fake/non-existent. Report has been sent to magistrate for classifying the case in "A" class. According to the Complainant, ICICI bank failed to trace the accounts and to provide IP addresses of the same.

The adjudicating officer considered that the fraudulent transactions in this case could not be accomplished without the connivance or negligence of someone from the ICICI bank. The adjudicating officer could establish a clear link between the phishing mail and the fraudulent transfers and withdrawals. It cannot be said that the phishing mail was sent by someone who ultimately did not want to be the beneficiary of the funds that are involved in the case. ICICI bank cannot shy away from its responsibility of securing the personal and sensitive information of its customers from external and internal fraudsters. It is clear that the personal and sensitive information of the Complainant was compromised by the ICICI bank and it also facilitated the transfer of funds from the Complainant's accounts to multiple other ICICI bank accounts of which the bank had no genuine KYC documents.

The adjudicating officer also noticed that the telecom company in the present case has not appreciated the government guidance issued in relation to the SIM cards. A telecom company is required to verify the details of an applicant before issuing a SIM card. They should maintain the records of each holder of their SIM card. This information also includes the e-mail address of the SIM card holder. But the company has failed to take any of the safety measures in the present case.

The adjudicating officer has also observed that most of the banks in USA



and in other developed nations INSURE their customers against online/ATM frauds, beyond a liability of 50 dollars. Section 909 of the "Electronic Fund Transfer Act" of USA dealing with consumer liability is really loaded in favour of the consumer. The adjudicating officer has observed that in India also, the banks should not only educate the consumers about the precautions to be taken while using internet banking, but will also insure the customers against possible frauds.

Finally the adjudicating officer has passed an award holding that ICICI has failed to prevent the offence under Section 43 of IT Act, by its willful negligence on multiple counts and thus it is guilty of offences in Section 85 read with Sections 43 and 43A of the IT Act, 2000 and should share the maximum responsibility in making good the losses incurred by the complainant.

The authority also ordered special training classes for all the personnel posted in cybercrime cells across the state, and to ensure that sufficient manpower is available to investigate cybercrimes.

### **3. Amit Dilip Patwardhan v. Rud India Chains<sup>55</sup>:**

The case relates to hacking of bank system. The Complainant has complained that his ex-employer hacked his bank system and obtained a bank statement. However, the bank has denied any role. But the bank has done absolutely no investigation on its own to find out how this has occurred. This speaks volumes about the apathy of the bank regarding the privacy of its customers' sensitive data.

Therefore, the authority has decided that the bank statement has not come from physical records kept with the bank, but definitely from the electronic records with the bank. Hence the IT Act definitely comes into play. Therefore, both the ex-employer and the bank were held guilty under Section 43(b) of the

---

<sup>55</sup>Amit Dilip Patwardhan v. Rud India Chains, Complaint No.1 of 2013 dated 06.01.2013 before the office of the adjudicating officer, Government of Maharashtra.

IT Act, read with Section 66.

**4. Anjali Vikas Lodha v. Bank of India, MIT branch, Pune<sup>56</sup> (absence of CCTV camera in ATM centre case):**

There were unauthorised fraudulent ATM withdrawals from the account of the Complainant from a particular ATM centre. The said ATM had no security personnel and CCTV camera for security.

Therefore, the authority held that if the Security Guard and CCTVs had been in place, it would have helped the investigating agency in apprehending the person who had done the transactions. Not securing ATM is a clear breach of its responsibility. Hence, omission by the bank is violative of Section 43A of the IT Act. Therefore, a compensation of Rs.25,000/- was awarded to the complainant.

**5. Muralidhar S.Gawande v. Corporation Bank, Karvenagar Branch<sup>57</sup>:**

In a similar case of ATM transaction fraud, the adjudicating authority has observed that, as per the "Guidelines on information security, electronic banking, technology risk management and cyber frauds" issued by the RBI, detailed instructions are given to Banks on Fraud risk management and the need for strong KYC norms to prevent cybercrimes. These have to strictly observed by the banks in order to prevent incurring liability under the IT Act, 2000.

**6. Pune Citibank Mphasis Call Center Fraud:**

US \$ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but

---

<sup>56</sup> Anjali Vikas Lodha v. Bank of India, MIT Branch, Pune, Complaint No.7 of 2012 dated 29.03.2012 before the office of the adjudicating officer, Government of Maharashtra.

<sup>57</sup> Muralidhar S.Gawande v. Corporation Bank, Karvenagar Branch, Complaint No.8 of 2012 dated 19.03.2012 before the office of the adjudicating officer, Government of Maharashtra.

when it happens in India it is a serious matter and we cannot ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering.

The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers.

All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

There is need for a strict background check of the call center executives. However, best of background checks cannot eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilty of not doing this.

#### **7. Bazee.com case:**

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet, Service Provider and

Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.<sup>58</sup>

#### **8. State of Tamil Nadu v. Suhas Katti<sup>59</sup>:**

The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

The Defence argued that the offending mails would have been given

---

<sup>58</sup> See also Pratap Ravindran, Baazee.com case-Why was IPC not invoked?, Dec 21, 2004, Business line, The Hindu, available at <http://www.thehindubusinessline.in/2004/12/21/stories/2004122100110900.htm>, last visited on 20.4.2013.

<sup>59</sup>State of Tamil Nadu v. Suhas Katti, CC.No.4680/2004, Charge sheet filed on 24.3.2004 under S.67 of IT Act, 2000, Ss.469, 509 IPC before the Hon'ble Addl. CMM Egmore.

either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:

“ The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.”

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

#### **9. The Bank NSP Case:**

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as “indianbarassociations” and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

### **10. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra<sup>60</sup>:**

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important ex-parte injunction.

In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any

---

<sup>60</sup> SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra , Suit No.1279/2001, Delhi High Court.

information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

#### **11. The Parliament attack case<sup>61</sup>:**

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents.

The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.

The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

#### **12. Case of sony.sambandh.com:**

India saw its first cybercrime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called

---

<sup>61</sup> State v. Mohd. Afzal and others, 107(2003) DLT 385.

www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone.

She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless head phone. In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted.



The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

### **13. Nasscom v. Ajay Sood & others:**

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared 'phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages.

Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi HC stated that even though there is no specific legislation in India to penalise phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not

only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image.

The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association.

The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognised the trademark rights of the plaintiff and passed an ex-parte ad-interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

This case achieves clear milestones: It brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no "damages culture" in India for violation of IP rights; This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted

from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones: It brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no "damages culture" in India for violation of IP rights; This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.<sup>62</sup>

#### **14. Infinity e-Search BPO Case:**

The Gurgaon BPO fraud has created an embarrassing situation for Infinity e-Search, the company in which Mr Karan Bahree was employed.

A British newspaper had reported that one of its undercover reporters had purchased personal information of 1,000 British customers from an Indian call-center employee. However, the employee of Infinity eSearch, a New Delhi-based web designing company, who was reportedly involved in the case has denied any wrongdoing. The company has also said that it had nothing to do with the incident.

In the instant case the journalist used an intermediary, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data is itself not substantiated by the journalist.

---

<sup>62</sup>Nasscom v. Ajay Sood & others, 119 (2005) DLT 596, 2005 (30) PTC 437 Del.

In this sort of a situation we can only say that the journalist has used "Bribery" to induce a "Out of normal behavior" of an employee. This is not observation of a fact but creating a factual incident by intervention<sup>63</sup>.

---

<sup>63</sup> Talwant Singh, Cyber law and information technology, available at <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>, last visited on 15.4.2013.

## CHAPTER VI - METHODS TO EFFECTIVELY COMBAT CYBER CRIMES

### **Methods to effectively combat cyber crimes:**

In the present global situation where Cyber control mechanisms are important we need to push "Cyber Laws". Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber crime. In India, there are 30 million policemen to train apart from 12,000 strong Judiciary. Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. Many police stations in Delhi have computers which will be soon connected to the Head Quarters. Cyber Police Stations are functioning in major Cities all over the Country. The pace of the investigations can become faster; judicial sensitivity and knowledge need to improve. IT Institutions can also play a role in this area. Technology nuances are important in a spam infested environment where privacy can be compromised and individuals can be subjected to become a victim unsuspectingly. Most cyber criminals have a counter part in the real world. If loss of property or persons is caused the criminal is punishable under the IPC also. Since the law enforcement agencies find it is easier to handle it under the IPC, IT Act cases are not getting reported and when reported are not necessarily dealt with under the IT Act. A lengthy and intensive process of learning is required. A whole series of initiatives of cyber forensics were undertaken and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems can get invented. We need to move faster than the criminals. The real issue is how to prevent cyber crime. For this, there is need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary.

The challenge in cyber crime cases includes getting evidence that will stand scrutiny in a foreign court. For this India needs total international

cooperation with specialized agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analyzed and the report presented in court is based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it. The law is stricter now on producing evidence especially where electronic documents are concerned. The computer is the target and the tool for the perpetration of crime. It is used for the communication of the criminal activity such as the injection of a virus/worm which can crash entire networks.

The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC. As per the report of National Crime Records Bureau, in 2005, a total 179 cases were registered under IT Act 2000, of which about 50 % (88 cases) were related to Obscene Publications / Transmission in electronic form, normally known as cyber pornography. 125 persons were arrested for committing such offences during 2005. There were 74 cases of Hacking of computer systems during the year wherein 41 persons were arrested. Out of the total (74) Hacking cases, those relating to Loss/Damage of computer resource/utility under Sec 66(1) of the IT Act were 44.6 % (33 cases) whereas the cases related to Hacking under Section 66(2) of IT Act were 55.4 % (41 cases). Tamil Nadu (15) and Delhi (4) registered maximum cases under Sec 66(1) of the IT Act out of total 33 such cases at the National level. Out of the total 41 cases relating to Hacking under Sec. 66(2), most of the cases (24 cases) were reported from Karnataka followed by Andhra Pradesh (9) and Maharashtra (8). During the year, a total of 302 cases were registered under IPC Sections as compared to 279 such cases during 2004 thereby reporting an increase of 8.2 % in 2005 over

2004. Gujarat reported maximum number of such cases, nearly 50.6 % of total cases (153 out of 302) like in previous year 2004 followed by Andhra Pradesh 22.5 % (68 cases). Out of total 302 cases registered under IPC, majority of the crimes fall under 2 categories viz. Criminal Breach of Trust or Fraud (186) and Counterfeiting of Currency/Stamps (59). Though, these offences fall under the traditional IPC crimes, the cases had the cyber tone wherein computer, Internet or its related aspects were present in the crime and hence they were categorized as Cyber Crimes under IPC.

Out of the 53,625 cases reported under head Cheating during 2005, the Cyber Forgery (48 cases) accounted for 0.09 %. The Cyber frauds (186) accounted for 1.4 % out of the total Criminal Breach of Trust cases (13,572). The Forgery (Cyber) cases were highest in Andhra Pradesh (28) followed by Punjab (12). The cases of Cyber Fraud were highest in Gujarat (118) followed by Punjab (28) and Andhra Pradesh (20). A total of 377 persons were arrested in the country for Cyber Crimes under IPC during 2005. Of these, 57.0 % (215) of total such offenders (377) were taken into custody for offences under 'Criminal Breach of Trust/Fraud (Cyber)', 22.0 % (83) for 'Counterfeiting of Currency/Stamps' and 18.8 % (71) for offences under 'Cyber Forgery'. The States such as Gujarat (159), Andhra Pradesh (110), Chhattisgarh and Punjab (51 each) have reported higher arrests for Cyber Crimes registered under IPC. Bangalore (38), Chennai (20) and Delhi (10) cities have reported high incidence of such cases (68 out of 94 cases) accounting for more than half of the cases (72.3%) reported under IT Act, 2000. Surat city has reported the highest incidence (146 out of 163 cases) of cases reported under IPC sections accounting for more than 89.6 %. The latest statistics show that Cyber Crime is actually on the rise.

However, it is true that in India, Cyber Crime is not reported too much about. Consequently there is a false sense of complacency that Cyber Crime does not exist and that society is safe from Cyber Crime. This is not the correct picture. The fact is that people in our country do not report Cyber Crimes for many reasons. Many do not want to face harassment by the police. There is

also the fear of bad publicity in the media, which could hurt their reputation and standing in society. Also, it becomes extremely difficult to convince the police to register any Cyber Crime, because of lack of orientation and awareness about Cyber Crimes and their registration and handling by the police. A recent survey indicates that for every 500 Cyber Crime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a Cyber Crime. The establishment of Cyber Crime cells in different parts of the country was expected to boost Cyber Crime reporting and prosecution. However, these cells haven't quite kept up with expectations. Netizens should not be under the impression that Cyber Crime is vanishing and they must realize that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals roam freely to execute their criminal's intentions encouraged by the so-called anonymity that internet provides. The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating Cyber Crime. There have only been few Cyber Crime convictions in the whole country, which can be counted on fingers. We need to ensure that we have specialized procedures for prosecution of Cyber Crime cases so as to tackle them on a priority basis. This is necessary so as to win the faith of the people in the ability of the system to tackle Cyber Crime. We must ensure that our system provides for stringent punishment of Cyber Crimes and cyber criminals so that the same acts as a deterrent for others<sup>64</sup>.

It is not so easy and possible to eliminate cyber crime once for all in view of the latest scientific development. However, it is quite possible to combat and check the cyber crimes. To achieve that object, the first and foremost requirement is the awareness among the public about the cyber crimes and the precautions to prevent the same.

---

<sup>64</sup> Anup Gridhar, Impact of cyber laws in India available at <http://anupgirdhar.net/?q=node/3>, last visited on 15.04.2013.



Saileshkumar<sup>65</sup> Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advises the five "P" mantras for online security, viz., Precaution, Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things :-

- 1.to prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
- 2.always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- 3.always use latest and up date anti virus software to guard against virus attacks.
- 4.always keep back up volumes so that one may not suffer data loss in case of virus contamination
- 5.never send your credit card number to any site that is not secured, to guard against frauds.
- 6.always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- 7.it is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- 8.web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
- 9.use of firewalls may be beneficial.

---

<sup>65</sup> Justice K.N.Basha, Seminar and workshop on detection of cyber crime and investigation, 28.06.2010 to 29.06.2010 available at <http://www.hcmadras.tn.nic.in/jacademy/article/Cyber%20Crime%20by%20KNBJ.pdf>, last visited on 22.04.2013.

10. web servers running public sites must be physically separate protected from internal corporate network.

### **Importance of data protection:**

Information stored on the owner of the computer would be his property and must be protected there are many ways such information can be misused by ways like 'unauthorized access, computer viruses, data typing, modification erasures etc. Legislators had been constantly confronted with problem in balancing the right of the individuals on the computer information and other people's claim to be allowed access to information under Human Rights. The first enactment in this regard was Data Protection Act by Germany in the year 1970. This was widely accepted by the world and also contributed to the Information Technology Act.

### **Origin and development of laws on data protection:**

The origin of laws on data protection dates back to 1972 when United Kingdom formed a committee on privacy which came up with ten principles, on the bases of which data protection committee was set up. Data Protection Act, 1984 (DPA) was United Kingdom's response to the Council of Europe Convention 1981, this Act lacked proper enforcement mechanism and has done little to enforce individual's rights and freedoms. European Union directive in 1995, European Convention of Human Rights (ECHR), Human Rights Acts, and further introduction of Data Protection Act, 1998 have done much in the field of Data protection in today's date. Data Protection Act has following aims and objectives:

Personal information shall only be obtained for lawful purpose, it shall only be used for that purpose, mustn't be disclosed or used to effectuate any unlawful activity, and must be disposed off when the purpose is fulfilled.

Though Data Protection Act aims at protecting privacy issues related to the information but still we find no mention of the word "privacy" in the Act, nor is

it defined, further the protection comes with various exemptions, including compulsory notification from the Commissioner in certain cases of the personal data. Due to the change in the regime of information technology for the date European Convention came, on which the Act is based amendments in the Act is advised for matching the present situation and curbing the crime in efficient way.

There is no Data Protection Act in India, the only provisions which talk about data protection are Section 72 and Section 43 of Information Technology Act, 2000. There must be a new Law to deal with the situation for a person to know that the Controller is processing his data concerning him and also that he must know the purpose for which it has been processed. It is a fundamental right of the Individual to retain private information concerning him provided under Article 21 of the Indian Constitution, which says: "No person shall be deprived of his life or personal liberty except according to procedure established by law". And due to the increasing trend of the Crime rate in the field separate legislation is required in this context for better protection of individuals<sup>66</sup>.

#### **Cybercrime countermeasures:**

- **Technical:**

There are a variety of different technical countermeasures that can be deployed to thwart cybercriminals and harden systems against attack. Firewalls, network or host based, are considered the first line of defense in securing a computer network by setting Access Control Lists (ACLs) determining which what services and traffic can pass through the check point.

Antivirus can be used to prevent propagation of malicious code. Most computer viruses have similar characteristics which allow for signature based detection. Heuristics such as file analysis and file emulation are also used to identify and remove malicious programs. Virus definitions should be regularly

---

<sup>66</sup> C. Suman and Duvva Pavan Kumar, 'Data Protection - An overview', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.

updated in addition to applying operating system hotfixes, service packs, and patches to keep computers on a network secure.

Cryptography techniques can be employed to encrypt information using an algorithm commonly called a cipher to mask information in storage or transit. Tunneling for example will take a payload protocol such as Internet Protocol (IP) and encapsulate it in an encrypted delivery protocol over a Virtual Private Network (VPN), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), or Internet Protocol Security (IPSec) to ensure data security during transmission. Encryption can also be employed on the file level using encryption protocols like Data Encryption Standard (DES), Triple Data Encryption Algorithm (3DES), or Advanced Encryption Standard (AES) to ensure security of information in storage.

Additionally, network vulnerability testing performed by technicians or automated programs can be used to test on a full-scale or targeted specifically to devices, systems, and passwords used on a network to assess their degree of secureness. Furthermore network monitoring tools can be used to detect intrusions or suspicious traffic on both large and small networks.

Physical deterrents such as locks, card access keys, or biometric devices can be used to prevent criminals from gaining physical access to a machine on a network. Strong password protection both for access to a computer system and the computer's BIOS are also effective countermeasures to against cyber-criminals with physical access to a machine.

- **Counter-Terror Social Network Analysis and Intent Recognition:**

The Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR) project uses the Terrorist Action Description Language (TADL) to model and simulate terrorist networks and attacks. It also models links identified in communication patterns compiled from multimedia data, and terrorists' activity patterns are compiled from databases of past terrorist threats. Unlike other proposed methods, CT-SNAIR constantly interacts with the user, who uses the system both to investigate and to refine hypotheses.

Multimedia data, such as voice, text, and network session data, is compiled and processed. Through this compilation and processing, names, entities, relationships, and individual events are extracted from the multimedia data. This information is then used to perform a social network analysis on the criminal network, through which the user can detect and track threats in the network. The social network analysis directly influences and is influenced by the intent recognition process, in which the user can recognize and detect threats. In the CT-SNAIR process, data and transactions from prior attacks, or forensic scenarios, is compiled to form a sequential list of transactions for a given terrorism scenario.<sup>67</sup>

- **Economic:**

The optimal level of cyber-security depends largely on the incentives facing providers and the incentives facing perpetrators. Providers make their decision based on the economic payoff and cost of increased security whereas perpetrators decisions are based on the economic gain and cost of cyber-crime. Potential prisoner's dilemma, public goods, and negative externalities become sources of cyber-security market failure when private returns to security are less than the social returns. Therefore the higher the ratio of public to private benefit the stronger the case for enacting new public policies to realign incentives for actors to fight cyber-crime with increased investment in cyber-security<sup>68</sup>.

---

<sup>67</sup> C.Weinstein,, et al., Modeling and Detection Techniques for Counter-Terror social network analysis and intent recognition, Proceeding from the aerospace conference, Piscataway at p.7.

<sup>68</sup> Ibid at p.8.

## CHAPTER VII – CONCLUSION AND SUGGESTIONS

When the NCRB statistics are referred, it can be observed that the number of cases related to cyber crimes are increasing year after year. Recently, in a case involving ATM fraud, the amount involved was around 45 million dollars and more than 27 countries were affected by the same. This shows an alarming need for an effective legislation and also best investigation techniques to ensure that these cyber criminals do not go scot-free. The information technology Act that was enacted in the year 2000 based on the UNCITRAL model law had only limited provisions (Sections 65-67) in order to deal with cyber crimes. Later on, it was not sufficient to effectively deal with the ever-increasing types of cyber crimes. Therefore, later in the year 2006, need was felt to amend the same. Accordingly, the 2008 amendment came into force in Feb 2009.

As far as the investigation aspects are concerned, the provisions of the IT Act were amended to make the system function more efficiently. For instance, Section 78 of the Act was amended to give the power to investigate to a police officer not below the rank of an inspector. Initially, only a police officer not below the rank of a Deputy Superintendent of Police alone can investigate into cyber crimes. Due to the large volume of cases that were reported, it was very difficult for the DSPs to handle all the cases.

When a cyber crime is reported and the criminal is convicted, the criminal gets punished. But the victims of the crime do not obtain any remedy. Section 43 of the IT Act provides for a civil remedy against the cyber criminals. The IT Secretary of the State can adjudicate the complaint and award compensation for the same. This enables the victims of the crime to get some remedy.

The process of investigation of cyber crimes is also faced with various difficulties. Mainly under reporting of crimes by organisations like banks and companies in order to prevent negative publicity proves a hindrance for effective investigation of crimes.

It should also be understood that cyber crimes cannot be limited to any boundary. A concerted effort of investigative agencies of all the countries will prove to be an effective way to combat the same.

## ANNEXURE - BIBLIOGRAPHY

### LIST OF STATUES AND CONVENTIONS:

1. European Convention on Cybercrime, 2001
2. The Constitution of India, 1950
3. The Criminal Procedure Code, 1973
4. The Indian Evidence Act, 1872
5. The Indian Penal Code, 1960
6. The Information Technology (amendment) Act, 2008
7. The Information Technology Act, 2000
8. UNCITRAL model law
9. US electronic fund transfer Act

### LIST OF CASES:

1. Amit Dilip Patwardhan v. Rud India Chains, Complaint No.1 of 2013 dated 06.01.2013 before the office of the adjudicating officer, Government of Maharashtra.
2. Anjali Vikas Lodha v. Bank of India, MIT Branch, Pune, Complaint No.7 of 2012 dated 29.03.2012 before the office of the adjudicating officer, Government of Maharashtra.
3. Avishek Goenka v. Union of India, W.P.(Civil) No.258 of 2010 before the Supreme Court of India, judgment delivered on 27 April 2012.
4. Dr. Prakash v. State of Tamil Nadu and Ors., AIR 2002 SC 3533.
5. Fatima Riswana v. State Rep. by A.C.P., Chennai and Ors., (2005) 1 SCC 582.
6. Firos v. State of Kerala, AIR 2006 Ker 279.
7. H.N.Rishbud v. State of Delhi, AIR 1955 SC 196.
8. Jigar Mayurbhai Shah v. State of Gujarat, (2008) 2 GLR 1134.



9. Muralidhar S.Gawande v. Corporation Bank, Karvenagar Branch, Complaint No.8 of 2012 dated 19.03.2012 before the office of the adjudicating officer, Government of Maharashtra.
10. Nasscom v. Ajay Sood & others, 119 (2005) DLT 596, 2005 (30) PTC 437 Del.
11. Nirav Navinbhai Shah v. State of Gujarat and Anr., MANU/GJ/8458/2006
12. Pootholi Damodaran Nair v. Babu, 2005(2)KLT707.
13. Ravi Shankar Srivastava v. State of Rajasthan, 2005(2)WLC612.
14. S.Sekar v. The Principal General Manager (Telecom), (BSNL), MANU/TN/9663/2007
15. Sanjay Kumar Kedia v. Narcotics Control Bureau and Anr., (2008)2 SCC 294.
16. Shri Sourabh Jain v. ICICI Bank, Complaint No.6 of 2011 dated 12.12.2011 before the office of the adjudicating officer, Government of Maharashtra.
17. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, Suit No.1279/2001, Delhi High Court.
18. State of Punjab and Ors. v. Amritsar Beverages Ltd. and Ors., (2006) (7) SCC 7.
19. State of Tamil Nadu v. Suhas Katti, CC.No.4680/2004, Charge sheet filed on 24.3.2004 under S.67 of IT Act, 2000, Ss.469, 509 IPC before the Hon'ble Addl. CMM Egmore.
20. State v. Mohd. Afzal and others, 107(2003) DLT 385.
21. Syed Asifuddin and Ors. v. The State of Andhra Pradesh and Anr., 2005 Cri L J 4314.

**LIST OF JOURNALS:**

1. All India Reporter
2. Criminal Law Journal
3. Delhi Law Times
4. European Journal of Information Systems

5. Gujarat Law Review
6. International Journal of Computer Sciences (IJCSI)
7. Journal of High Technology Law
8. Karnataka Law Times
9. Supreme Court Cases
10. T.C.Panda/ International Journal of Engineering research and Applications (IJERA)

**LIST OF BOOKS:**

1. Dr.Farooq Ahmed, Cyber Law in India, 2<sup>nd</sup> Edn., 2005, New Era Publications.
2. Dr.K.N.Chandrasekharan Pillai, R.V.Kelkar's criminal procedure, Fifth edn., Eastern book company, Lucknow.
3. Justice Yatindra Sinha, Cyber laws, 2<sup>nd</sup> edn., Universal Law Publishing Co.
4. S.V.Joga Rao, Law of cyber crimes and information technology law, Edn. 2004, Wadhwa & Company, Nagpur.
5. Vakul Sharma, Information technology law and practice, Third edn., Universal publications.
6. Vivek Sood, Nabhi's Cyber crimes, electronic evidence and investigation, legal issues, 1<sup>st</sup> revised edn. 2010, a Nabhi Publication.

**LIST OF ARTICLES:**

1. Anup Gridhar, Impact of cyber laws in India available at <http://anupgridhar.net/?q=node/3>, last visited on 15.04.2013.
2. Baron F Ryan, A critique of the international cybercrime convention, 10, Commlaw conspectus, 2002, at pp.263, 269.
3. C. Suman and Duvva Pavan Kumar, 'Data Protection - An overview', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.

4. C.Weinstein,, et al., Modeling and Detection Techniques for Counter-Terror social network analysis and intent recognition, Proceeding from the aerospace conference, Piscataway at p.7.
5. Common attack pattern enumeration and classification, APEC available at <http://capec.mitre.org/index.html>, last visited on 25.3.2013.
6. Computer hope, Data theft, 2012 available at <http://www.computerhope.com/jargon/d/ datathef.htm> last visited on 3.4.2013.
7. Cyber crimes, National Crime Prevention Council available at <http://www.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf>, last visited on 22.4.2013
8. Danish Irani et al, PuCollege of Computing Georgia Institute of Technology Atlanta, "Evolutionary Study of Phishing"; eCrime Researchers Summit, 2008.
9. DSL Reports, Network Sabotage, 2011 Available at: <http://www.dslreports.com/forum/r26182468-Network->
10. Harshwardhan, Investigation of computer crime: Issues and challenges, 2008 Cri.LJ 2 at p.18.
11. Hemraj Saini and Yerra Shankar Rao, Cyber-Crimes and their impacts: A Review, T.C.Panda/ International Journal of Engineering research and Applications (IJERA), Vol.2, Issue 2, Mar-Apr.
12. Justice K.N.Basha, Seminar and workshop on detection of cyber crime and investigation, 28.06.2010 to 29.06.2010 available at <http://www.hcmadras.tn.nic.in/jacademy/article/Cyber%20Crime%20by%20KNBJ.pdf>, last visited on 22.04.2013.
13. Kevin G. Coleman, Cyber Intelligence: The Huge Economic Impact of Cyber Crime, 19.09.2011 available at: <http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/>, last visited on 30.3.2013.
14. Legal Info, Crime Overview Aiding And Abetting Or Accessory, (2009) available at <http://www.legalinfo.com/content/criminal-law/crime->

- overview-aiding-and-abetting-or-accessory. html, last visited on 22.3.2014.
15. M.Loganathan and Dr.E.Kirubakaran, A study on cyber crimes and protection, IJCSI, Vol.8, Issue 5, No. 1, Sep 2011 available at <http://ijcsi.org/papers/IJCSI-8-5-1-388-393.pdf>, last visited on 22.4.2013.
  16. Oracle, Security overviews, 2003 available at [http://docs.oracle.com/cd/B13789\\_01/network.101/b10777/overview.htm](http://docs.oracle.com/cd/B13789_01/network.101/b10777/overview.htm), last visited on 2.4.2013.
  17. PTI Contents, India: A major hub for cybercrime, (2009) Available at: <http://business.rediff.com/slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm>, last visited on 14.4.2013.
  18. R.Baskerville, 1991, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1(2), pp.121-130.
  19. Sabotage-or-incompetent-managers-trying-to-, last visited on 10.4.2013.
  20. Shannon L.Hopkins, Cybercrime convention: A Positive beginning to a long road ahead, Journal of high technology law, Vol.II.,No.1, pp.105-110.
  21. Sofaer D. Abraham, et al., A proposal for an international convention on cyber crime and terrorism, Hoover institution, et al., available at <http://oas.org/juridico/english/monograph.htm> last visited on 23.4.2013.
  22. Talwant Singh, Cyber law and information technology, available at <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>, last visited on 15.4.2013.
  23. V. Shiva Kumar, Cyber crime-prevention and detection available at <http://www.cidap.gov.in/documents/Cyber%20Crime.pdf>, last visited on 22.4.2013.
  24. Vishal Dhotre, Crimes against individuals in India and IT Act available at [http://www.siu.edu.in/Research/pdf/Vishal\\_Dhotre.pdf](http://www.siu.edu.in/Research/pdf/Vishal_Dhotre.pdf), last visited on 22.4.2013.