CHAPTER - 5

FINDINGS, SUGGESTIONS AND CONCLUSION
CHAPTER-5

FINDINGS, SUGGESTIONS and CONCLUSION

In this chapter, detailed findings of this study are discussed. On the basis of the findings, suggestions are mentioned. Finally, conclusions are drawn on the basis of the analysis of the findings and supported by the theories that are applicable and the articles that are published on the topic.

5.1 FINDINGS

This research has emphasised on two aspects; a Criminological assessment on the Information Technology Act, 2000, and Cyber Crimes. One line of enquiry comprised of an opinion of the respondents on the effectiveness, lacunae and the suggested alterations of the Information Technology Act-2000. The other line of enquiry has been focused on the way in which the society at large perceives the problem of Cyber Crime.

This research into the cyber Crimes has predominantly focused on key aspects such as the vulnerability to Cyber Crimes, Crime Avoidance, incidence reaction, and the opinion relating to the globalization of the legal mechanism, as the problem of cyber crime transgresses all known sovereign boundaries. In addition to these, the research also attempts to know the role of the Law Enforcement, cyber security and related issues.

According to this research, the following findings are presented and discussed under the following heads:

Part-A

Findings on descriptive analysis pertain to the Socio-personal characteristics of the respondents, efficacy of the Information Technology Act-
2000 in dealing with the problems which Cyber Crimes Pose and other variables which help to link in findings of objectives and testing of hypothesis.

1) Socio-personal Characteristics of the respondents.

2) Experiences of Cyber Crime and the reaction of the respondents to it;
   a) Respondent who have come across cyber crimes;
   b) Types of cyber crimes encountered by the respondents;
   c) Respondents reaction to cyber crimes;
   d) Whether cyber crimes are committed by known persons, insiders or disgruntled employees in an organisation;
   e) Loss due to cyber crime;
   f) Vulnerability to cyber crime;
   g) Preventive measures to cyber crimes by individuals and organisations;
   h) Need for creating Awareness about Cyber Crimes and responsibility among the users of the Cyberspace;
   i) Personnel in Cyber Crime Police Station are well trained and equipped in handling Cyber Crimes;

3) The Information Technology Act-2000
   a) Awareness of the Act;
   b) Adequacy relating to its punitive provisions;
   c) Capability in the Act to prevent Crime;
   d) Incorporation of provisions related to Intellectual Property Right Protection, Trademark and Copyright protection;
   e) International or Transnational Law;
   f) Role of Non-Governmental efforts in enforcing the Act.

Part-B- Findings and testing of hypothesis:

The hypothesis is tested using the assimilated data collected during this research.
1) Socio-personal characteristics of the respondents:

Details about the respondent’s socio-personal characteristics such as sex, age, education, sphere of employment and knowledge of Cyber Crimes and the Information Technology Act-2000 are analysed.

Sex: Out of the three hundred respondents, an equal number of male and female respondents ie., 150 female and 150 male respondents were chosen for the study.

Educational levels: This distribution is indicated in Table 4.2. Most of the respondents are professionally qualified persons, such as B.E and B Tech. The general graduates are B.Sc., B.Com, BBM and BA Graduates. The post graduates included here are the M.E, M Tech, M.Sc etc. All the doctorates are in the Professional and Computer engineering fields. The distribution of the variables is indicative that the majority of the respondents are Graduate Engineers, who have a professional qualification (74%).

Area of Employment: This distribution is indicated in Table 4.3. All the respondents were employed in Bangalore City at the time of Data collection. 46% are from the areas of Software Design and Development, 03% Hardware development, 27% Information Technology Enabled Services (TIES), 09% Business Process Outsourced Companies (B P O’s), 04% Banks and Financial Institutions and 11% others such as Sales, training etc. (N=300)
2) Experiences of Cyber Crime and the reaction of the respondents to it;

a) Respondent who have come across cyber crimes:

The findings of Table 4.15 show that out of 300 respondents, an overwhelming majority of 81% have come across Cyber Crimes during the course of their occupation. 19% of the respondents have not come across Cyber Crimes during their occupation. In this, the numbers of male and female respondents are exactly equal.

b) Types of cyber crimes encountered by the respondents:

The findings of Table 15-A indicate the types of Cyber Crimes encountered by the respondents. The details of the analysis are as following:

i. 23% or the largest type of Cyber Crime which the respondents were a victim of is the Virus/Worm Attacks, of which 22% were male and 24% female. The near equality in the numbers suggests that the virus/worm attacks are predominantly on the Computer System or on the Computer network and hence is not biased towards any gender in particular.

ii. 22% of the respondents were a victim of e-mail Bombing. In this the number of male victims is 19% and 25% are female victims. While most of the e-mail bombing attacks
are aimed at organisations, some are personal also, as indicated by the greater numbers of female victims.

iii. 13% of the respondents have encountered the Trojan attack. 15% of them were male and 10% female. This attack is similar to the virus/worm attack and is mainly organisational rather than individual. Hence no significance to the gender of the respondents may be attached.

iv. 11% of the respondents were victims of Web jacking. The number of male victims was 12% and females 10%. Web jacking is the precursor for phishing attacks, wherein a fake website is created after the taking over of hijacking the legal website. The phenomenon of phishing attack was not commonly seen during the period of the data collection for this research. However, a slightly higher numbers of males indicate that they have not been careful in cross verification of the details.

v. 10% of the respondents have responded that they were victims of Data diddling. The numbers of males and females are equally distributed. This is the result of hacking, and hence more of an organisational rather than a personal type of a Cyber Crime.

vi. 09% of the respondents have indicated that they have been victims of Logic Bombs. This is also an organisational rather than a personal type of a Cyber Crime.

vii. 07% of the respondents have indicated that they were victims of Internet Time Theft. Of these there were 7% females and 6% males. The near male female nature of this personal type of a Cyber Crime indicated that the offender and victims are anonymous.
viii. 04% of the respondents have responded that they have been victims of Salami attacks. Once again, this is also an organisational rather than a personal type of a Cyber Crime.

ix. 01% of the respondents have indicated that they are victims of obscene mail. In this category of cyber crime, all the respondents who have indicated that they were a victim are female.

c) Respondents reaction to cyber crimes;

The findings in Table 4.17 indicate to the reaction of the respondent to cyber crime. 46% of the respondents have responded that they would react to cyber crimes in more than one way. In this, there is an near equal number of male and female respondents. 47% are female and 45% are male respondents. They would react in more than one way, when they were a victim of Cyber Crimes. The reason is that the nature of the crime, whether it is an organisational one or a personal one is the indicating factor.

Out of the 54% of the respondents who have indicated otherwise, the distribution is that 28% have indicated that they would react to it on their own initiative. In this, 33% are males and 23% Females. Reaction by own initiative is similar to the right of private defence of property. It would be in the form of installing anti-Malware programmes, firewalls filters etc. The point of significance is that more male respondents have indicated that they would react to Cyber Crimes on their own. Cyber crimes being mostly impersonal in its forms are the reasons why this response is possible, while conventional crimes cannot.
22% of the respondents have opined that they would inform the superior personnel within their organisation. This is mainly crimes against organisations or even personal, where most of the IT Industry protects their own employees from personal attacks. 17% of the respondents were male while 27% of the respondents were female. The point of significance here is that the female respondents perhaps, are more comfortable in confiding to a senior colleague or an authorised person within their own organisation. Or, it may simply be the organisational protocol.

04% of the respondents have indicated that they ignore a cyber crime, as long as it is not serious and highly derisive of their character.

The most significant finding is that not a single respondent has opined that they would approach or contact the Police in this regard.

d) Whether cyber crimes are committed by known persons, insiders or disgruntled employees in an organisation;

The findings of Table 4.20 indicate that 81% of the respondents have opined that Cyber Crimes are not caused by known persons, insiders and disgruntled employees or ex-employees of the organisation. This is contrary to the belief of offender-victim relationship. Out of these, the males were 80% and females 81% who held their opinion.

19% of the respondents have opined that they believe that crimes are committed by insiders, disgruntled employees and known persons.

e) Loss due to Cyber Crime.
The findings of Table 4.21 indicate the opinion of the respondents as to the loss due to Cyber Crime. 76% of the respondents have opined that Cyber Crimes cause losses of money, credibility and reputation, service quality and loss of competitive edge in firms. Thus, cyber crimes indicate a multiple loss.

11% of the respondents have indicated that the main loss is money while another 11% have indicated that the loss is of credibility and money only. A negligent 02% have indicated that cyber crimes lead to loss of competitive edge. This is due to the factor of the Cyber security in organisation.

f) Vulnerability to cyber crime.

The findings of Table 4.22 indicate that 59% of the respondents are of the opinion that women and children are more vulnerable to obscene Cyber Crime. It is possible that men ignore it simply and are not targets. Among this, 67% are female respondents.

g) Preventive measures to cyber crimes by individuals and organisations.

The findings of Table 4.16 reveal that 97% of the respondents have indicated that their organisations have a specific protocol in handling Cyber Crime. This is a preventive measure and every firm must possess its own safety and security measures. In order to accomplish this, a sequence of reactions, also known as protocol is initiated. This is an extremely confidential issue and all personnel will be exposed to it on a need-to-know basis.
The findings of Table 4.18 also indicate the respondent’s opinion regarding the Cyber Security System. 98% of the respondents were of the opinion that every organisation should have their own preventive measures.

The overwhelmingly large numbers of opinions in Table 4.16 and Table 4.18 signify that Cyber Crime prevention is a matter of individual/organisational domain. Hence, several Cyber Security Consultants have come into existence.

h) Need for creating Awareness about Cyber Crimes and responsibility among the users of the Cyberspace.

The findings of Table 4.24 show that 90% of the respondents are of the opinion that there is a need for creating awareness Cyber Crimes and the responsibilities of the users of Cyberspace. In the United States of America, the Department of Justice and the Information Technology Association of America (ITAA) have associated themselves in order to campaign and raise awareness levels of Cyber Crimes and the responsibilities of the net users. This is a continuous process and enables in loss prevention due to Cyber Crime. The Police use this method in creating Crime Prevention Week/Fortnight/Month for conventional crimes.

Findings of Table 4.23 have indicated to the contrary. 63% of the respondents have indicated that mere education of women and children is insufficient in the prevention of obscene attacks on women and children. Amongst these, 72% are male and 55% are female respondents. The point of significance here is that irrespective of raising the levels of education
and awareness of women, crimes do take place, which include Cyber Crimes also.

i) Personnel in Cyber Crime Police Station, Bangalore City, are well trained and equipped in handling Cyber Crimes.

The findings of Table 4.25 indicate that 74% of the personnel in Cyber Crime Police Station are not well trained and equipped in handling Cyber Crimes; 13% felt that Personnel in Cyber Crime Police Station, Bangalore City are well trained and equipped in handling Cyber Crimes; while 13% of the respondents did not respond to this question, as they were not aware of the existence of a Cyber Crime Police Station in Bangalore City.


The findings are related to the features of the Act.

a) Awareness of the Act.

The findings of Table 4.4 show that 81% are aware of the existence of the Information Technology Act-2000. The significance of this distribution is that the respondents are not only educated but aware of the law in their sphere of employment. It follows the dictum that “ignorance of a fact is excusable; ignorance of law is not excusable”.


b) Adequacy relating to its punitive provisions.

A series of questions were asked to the respondents. The punitive provision and the penalty were described. The options of the responses were tri-polar; the responses were to signify the adequacy, inadequacy or excessiveness of the provision and penalty. The following are the findings:

i. The findings of Table 4.5 shows the opinion regarding S.43 of the Information Technology Act-2000. The section lays down punishment for damage to computer, computer Systems etc. 53% of the respondents have indicated adequacy, 44% inadequacy. The provision of law indicates both punishment and compensation up to Rupees One Crore. The offences which are covered under this provision are Denial of Service attacks, Viruses and other Malware Data Diddling, e-mail hijacking and Web jacking etc. It also includes physical damage to the computer, computer system or network. Those respondents who opine the inadequacy of this provision perhaps are of the opinion that it should be punitive as well as compensatory.

ii. The Findings of Table 4.6 shows the opinion regarding S.65 of the Information Technology Act-2000. The section lays down punishment for Tampering with Computer Source Document. 81% of the respondents have indicated that the punishment of 3 years of imprisonment and fine up to One Lakh Rupees as inadequate. Tampering with the Computer Source Code
leads to loss of data, which has infinite value and no amount of punishment is adequate as a deterrent.

iii. The findings of table 4.7 show the opinion regarding S.66 of the Information Technology Act-2000. The section lays down punishment for hacking. 57% of the respondents have indicated that the punishment of imprisonment of 3 years and fine of two lakh rupees is inadequate. Hacking is a crime which typifies the problems of cyber crime, as the crime that is committed is of trans-national in nature, with issues such sovereignty and anonymity involved within it. The favour shown towards the enhancement of the punishment perhaps is due to the fact that when a hacker is caught, the punishment must be severe. Stringent punishment should be imposed, rather than fine and light period of imprisonment to punish the offenders.

The skepticism of the possibility and probability of the process of law, such as investigation and trial of the culprit is also evident here.

iv. The findings of table 4.8 show the opinion regarding S.67 of the Information Technology Act-2000. The section lays down punishment for publishing of Information which is obscene, in electronic form. 50% of the respondents have indicated that the punishment on the first conviction of imprisonment description for a term which may extend to five
years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees, as adequate.

On the contrary, 43% of the respondents have also opined that the punishment as inadequate.

v. The findings of table 4.9 show the opinion regarding S.72 of the Information Technology Act-2000. The section lays down punishment for Breach of confidentiality and privacy with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. 59% of the respondents have opined as adequate, though the fact remains that this section has been inadequately defined.

vi. The findings of table 4.10 show the opinion regarding S.85 of the Information Technology Act-2000. The section lays provisions for offences by companies. 85% of the respondents have indicated agreement to the existence of the provisions that companies should be liable for penalty.

vii. The findings of table 4.11 show the opinion regarding S.79 of the Information Technology Act-
2000. The section lays down provision that a network service provider not to be liable in certain cases. 66% of the respondents disagree with this provision.

c) Capability in the Act to prevent Crime

The findings of table 4.12 indicate the opinions of the respondents to the question as to whether Information Technology Act-2000 is capable of preventing Cyber Crimes. 95% of the respondents opine that it is incapable, as there is no scope for preventive aspect of the law.

d) Incorporation of provisions related to Intellectual Property Right Protection, Trademark and Copyright protection;

The findings of Table 4.14 show that 89% of the respondents opine that the relevant provisions of the Intellectual Property Right Protection should be incorporated within the Act. Some provisions relating to Software Piracy, Cloning of magnetized strips, theft of intellectual property and issues related to these are not addressed in the Act.

e) International or Transnational Law.

The findings of Table 4.13 indicate that 83% of the respondents are of the opinion that there is a need for International or Trans-National
Law. This is due to the fact of the Trans-National nature of the offences. Many offences such as Cyber Frauds, Money Laundering and Cyber Terrorism cannot be tackled due to the sovereignty issues.

f) Role of Non-Governmental efforts in enforcing the Act.

The findings of Table 4.19 indicate that 96% of the respondents are of the opinion that Governments or Law Enforcement Agencies alone cannot tackle the problems of Cyber Crimes. There must be a private-public partnership in dealing with problems caused by Cyber Crimes.

Part-B

Findings and testing of hypothesis:

The major findings of hypothesis testing are presented under headings pertaining to each hypothesis separately. ‘Simple Percentage’ method of testing of the hypothesis has been done in this study. The hypotheses are tested as positive or negative by calculating the higher percentage of the respondents’ response from the appropriate tables.

Findings of the First Hypothesis:

FIRST HYPOTHESIS:

Computer and cyber space are usually used to commit crimes on the premise that the incidents are rarely detected, due to its anonymity and the fact that crimes may be committed in one country
and its effects may be felt in another and the varied nature of the trans national laws, technologies to prevent and detect these crimes.

The following Tables are used as proof of this hypothesis:

The findings of Table 4.15 show that more percentage of the respondents (81%) have encountered Cyber Crime and lesser percentage (19%) have not encountered Cyber Crimes.

The findings of Table 4.15A further reiterate that almost all these crimes are random, unspecific attacks. Virus/Worm attacks were the largest single type (23%), followed by Trojan Attack (13%), Web Jacking (11%), Data Diddling (10%), Logic Bomb (09%), Internet Time Theft (07%) and Salami Attack (04%). The specified attacks are distributed in the form of e-mail bombing (22%) and Obscene Mail (01%).

**Hence the First Hypothesis is positive.**

In support of this, a report by Microsoft, a leading software company indicates that:

**Microsoft Research Reveals New Trends in Cybercrime**

> “Greater intra organizational planning and collaboration needed as security and privacy threats converge”.

**SAN FRANCISCO and LONDON — Oct. 23, 2007** — Microsoft Corp. today released research showing an acceleration in the number of security attacks designed to steal personal information or trick people into providing it through social engineering.

---

Microsoft’s most recent Security Intelligence Report, a comprehensive analysis of the threat landscape, shows that attackers are increasingly targeting personal information to make a profit and are threatening to impact people’s privacy. The report found that during the first half of 2007, 31.6 million phishing scams were detected, an increase of more than 150 percent over the previous six months. The study also shows a 500 percent increase in Trojan downloaders and droppers, malicious code used to install files such as Trojans, password stealers, keyboard loggers and other Malware on users’ systems. Two notable families of Trojans detected and removed by the Microsoft Malicious Software Removal Tool are specifically targeted at stealing data and banking information.

Hence, the findings of this research and the report of Microsoft research report prove that the First Hypothesis is positive.

SECOND HYPOTHESIS

Cyber crimes are mainly committed for economic gain and defamation of the intended victim.

The following Tables are used as proof of this hypothesis:

The findings of Table 4.21 indicate that a vast majority (76%) of the respondents are in agreement to this. The responses were nearly equal amongst the male and female respondents. The reason behind this is perhaps that an individual or an organisation
looses monetarily, its or their credibility and reputation, service quality and as well as competitive edge, due to Cyber Crime.

This finding is supported by an article of Computer Crime Research center:

**Cybercrime cost about $400 billion**

Date: **July 06, 2005**  
Source: **Miami Herald**

SANTA CLARA, Calif. /PRNewswire-FirstCall/ -- McAfee, Inc. (NYSE: MFE - News), the leader in Intrusion Prevention and Security Risk Management solutions, today announced the results and availability of the McAfee® Virtual Criminology Report, which examines how a new class of criminals are using the Internet in new, systematic and professional ways to commit illegal acts. According to the findings, information theft is the most damaging category of Internet crime, while viruses have been the most costly for businesses.

The report, commissioned by McAfee, discusses how organized crime and cybercrime are developing, and looks at the future threat this activity could pose to home computers, government computer networks, and to computer systems in the business sector. The report reveals a hierarchy of cyber criminals, discussing the recent evolution of the amateur cyber delinquent to the professional cyber gang.

"As companies and consumers continue to move towards a networked and information economy, more opportunity exists for cyber criminals to take advantage of vulnerabilities on networks and computers," said Chris Christiansen, program vice president, IDC. "Understanding who

---

15 http://www.computerresource.center.html
these criminals are and how they attack provide great insight into implementing and practicing good security hygiene."

Prior to 2000, cyber criminals acting alone committed the majority of cybercrimes, usually in an attempt to attain notoriety within the cyber world. However, in recent years, a shift has occurred as criminals and not just amateurs are committing cybercrimes. This is due in large part to the potentially huge financial gains that can be made from the Internet with relatively little risk. The report goes on to examine the different tactics and tools used by these cyber criminals, and future areas of attack.

Some of the report's most compelling highlights include:

- The FBI estimates that cybercrime cost about $400 billion in 2004.
- In an investigation, codenamed "Operation Firewall," U.S. and Canadian authorities announced the arrest of 28 people from six countries involved in a global organized cybercrime ring. They operated Websites to buy and sell credit card information and false identities. They bought and sold almost 1.7 million stolen credit card numbers. Of these stolen credit cards, financial institutions have estimated their losses to be $4.3 million.
- The use of pseudonyms or online identities provides an anonymity that is attractive to criminals. Sources estimate that perhaps only 5% of cyber criminals are ever caught or convicted.
- "The McAfee Virtual Criminology Report paints a clear picture of the growing threats and criminal actions taking place via the Internet," said Jimmy Kuo, research fellow with McAfee AVERT. "It is imperative that companies, government agencies and consumers alike take notice of this expanding class of criminals and take the appropriate actions to secure their networks and personal computers."
Cyber criminals are stealing identities by extracting personal identification information or credit information from a company's database and affecting thousands of consumers. They can also extract a company's own financial information or steal valuable intellectual property. While viruses began as a means for hackers to demonstrate their prowess, they have become the leading delivery vehicle for attack by cyber criminals. The goal of many cyber criminals is to infect thousands of computers and turn them into a network of devices that have been compromised by worms or viruses and attack in unison on command. Those who succeed in creating such a "bot-network" or "bot-net," now have access to a very powerful tool for crime. Such access has become easier, as spammers, hackers, and other cyber criminals are able to acquire or rent "bot-nets" -- some "bot-net" owners will rent their networks for $200-$300 an hour. "Bot-nets" are crucial to executing distributed denial of service attacks, spam and phishing scams, which makes them the growing weapon of choice for fraud and extortion.

In its early stages, the Internet was designed mainly for a finite group of users who used it as a way to exchange ideas and information among a relatively small community. The value and impact of Internet activities has escalated dramatically with its continued commercialism and expansion. In 2004, e-commerce reached $70 billion in the U.S, an increase of 24% over 2003.

The report credits the growth of online banking and commerce as part of the draw for cyber criminals. It discusses the many ways that criminals take advantage of vulnerabilities in networks and computers to gain access to valuable information, such as personal identification information, financial data and intellectual property.

Growth in cybercrime is also attributed to the anonymity and global connectivity, which enables cyber criminals from all over the world
to engage in traditional crimes such as extortion, drug-running or pornography on a global stage. Simultaneously, the study reports that while cyber criminals become more advanced, today's law enforcement agencies are struggling to keep pace, as many lack the necessary tools to operate effectively in cyberspace.

A few cases to illustrate this are:

Express News Service
First Published : 28 Jun 2009 11:07:50 AM IST

BANGALORE: Four cyber crime cases registered in Cyber Crime Police station of CID (Criminal Investigation Department). A loss of about Rs 4 lakhs through phishing and hacking cases were reported.

The hackers have drawn an amount of Rs 2.20 lakh from Srinath Imarati, an administrative officer with a private firm, Bearing Point, to four other accounts by making 10 transactions. His account was with ICICI bank of CMH road branch.

He received a ‘phishing’ e-mail in the name accountsupdate@icici.com which asked for passwords and other details. He believed the mail and gave details through e-mail. On 22nd he noticed his account was debited of Rs 2,20,500. After consulting the bank officials, he lodged a complaint with CID’s Cyber police.

In another incident, Girish C Rath has lost Rs 49,000 from his Axis bank account. He got to know that some miscreants did an unauthorised transfer of money to their accounts by hacking his e-banking password.

---

In yet another case, Subrahmanya, a senior consultant with WIPRO has registered a complaint with Cyber Crime Police about hacking of his HDFC account and transferred Rs 28,000 to other account.

In another case, Prasanna Kumar, an engineer of ITPL has lost his Rs 58,000 when he was in South Korea on official duty. The money was transferred by hacking the e-mail ID to one MS Aimsing Shankhil’s account.

The hacker had changed the e-mail ID prasana_rpk@yahoo.co.in to rippychuppy@ gmail.com and has also changed the mobile number from the account details.

**Another instance of Cyber crime is as following:**

Sunil Nalwade has posted the following case of fraud in 37

http://hublidwdcybersecurity.blogspot.com

A city doctor fell prey to an online lottery fraud and lost Rs 30,157 to seven foreign conmen. The conmen lured Dr Vadiraja B.N. by sending him an e-mail that he had won $ 5 Lakh in a lottery. On April 17, 2007, Dr Vadiraja was informed about the prize money by a mail from one Ayodam, who claimed to be the vice-president of International Promotions, Japan Jumbo Draw, Hong Kong. His accomplices were Dr Tony Cheung, Clement Wang, Ella Doris, Dr Young Chu, Tschipanda Mande and Mashun Khamrag.

Later, the doctor was told that the lottery money had been transferred to commerce bank of Philippines for onward transfer to his account in Bangalore. He was asked to remit $750 to the bank account of Tschipanda. The doctor followed their instructions promptly. He grew suspicious when he was again asked to remit $1,650. After enquiry, he realised the lottery was fake.

37 http://hublidwdcybersecurity.blogspot.com
This case from Hubli was registered in the Cyber Crime Police Station, Bangalore:

**Cases on Cyber Defamation:**

This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person’s friends.

India’s first case of cyber defamation was reported when a company’s employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

The company was able to identify the employee with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

In another case, A, (Name not disclosed) a Computer Science graduate from Hyderabad was recruited by Campus Selection Process into Wipro, a leading IT Company. He was to report himself for training at Bangalore on a designated date. Upon arriving at the designated place, he was informed that the letter of intent to employ was cancelled and no reason was attributed. Upon A’s persistent appeals to know the reason, he was shown a printout of an e-mail sent by him in derogatory language on to the person who was a lady, who had conducted the final interview. A lodged a complaint with the Cyber Crime Police Station, Bangalore. The case was taken up as an ‘Enquiry’ and a tracker e-mail was sent.
A's e-mail had been hijacked, by cracking the password. Eventually, it lead to the arrest of B, who, out of jealousy had perpetuated the act.

The findings, survey report and cases indicate that the Second Hypothesis is positive.

THIRD HYPOTHESIS:

Victims do not readily come forward to report cyber crime, especially, the corporate bodies, for the reason of loss of credibility and further businesses; futility of the whole process, as the crime has trans-national dimensions and there is no law to act beyond the sovereign boundaries.

The following Tables are used as proof of this hypothesis:

The findings of Table 4.17 indicate the respondent's response to Cyber Crime. A significant number (46%) of the respondents have opined that they would firstly react to it on their own initiative; next, they would inform a superior ranked person within their organisation; or simply ignore it.

When individually sought, the most responses were (28%) that they would react to it on their own initiative. This is because of the empowerment and the literacy levels of the respondent. An educated victim reacts suitably to a cyber crime, in a similar manner to the right of private defence.

Organizationally, the protocol may dictate the information of the crime to a higher ranking person within the organisation. Hence the significant numbers of respondents (22%) have sought this option.
This indicates that the least option as a response to cyber crime would be to inform the Police about it. Thus, not a single respondent has indicated that the first response to Cyber Crime is to report it to the Police.

The findings of Table 4.12 indicate that an overwhelming number (95%) of the respondents are of the opinion that the Information Technology Act-2000 is incapable of preventing Cyber Crimes. This is due to the trans-national nature of the offence.

Further, the findings of Table 4.13 indicate that an overwhelming majority (83%) of the respondents opine that there is a need for an International Law, especially in light of the transnational frauds, money laundering, Cyber Terrorism and the use of the cyber space for illegal activities.

Cases:

Case: 1. Dr. C, (Names Withheld on request) Reader in Geography, Institute of Development Studies, University of Mysore, was one of the victims of his e-mail being hijacked. Several of his friends called him over telephone, asking him as to why he has sent such messages over the e-mail. Upon hearing this, he tried to open his e-mail ID, but could not, as the password was not being accepted. The messages were pertaining to ‘Jihad’ and how Islamic militants would destroy India. As Dr. C knew that this researcher was studying about Cyber Crimes, he contacted the researcher. The researcher in turn contacted a Detective Inspector attached to the Cyber Crime Police Station, Bangalore. He and the then Head of the Station, an officer of the rank of Deputy Superintendent of Police sent tracker mails and located the e-mail-hacker to be somewhere in Pakistan. Due to the trans-national nature, the Police
could not prosecute the culprit. The only remedy they could offer was to correspond with yahoo!, the e-mail service provider and block the e-mail account.

Case: 2. Dr. X, (Names Withheld on request) a prominent surgeon in Belgaum, receives a call from his wife, Dr.(Mrs.) X, asking him as to when did he go to Egypt. She informed him of the e-mail which she had received from him, stating that he had lost his passport, money and credit cards, while on a holiday at Egypt. The mail requested the reader to remit money, in a bank account at Cairo. As Dr. (Mrs.) X had seen Dr. X the very same morning, the joke became suspicious and they started mailing all friends who may have received the so called “request” mail. When money failed to turn up, the mail-hackers started sending out obscene and defamatory mail, based on the content of the folder. As the victim knew about this researcher studying Cyber Crimes, the victim contacted the researcher, who in turn assisted them in contacting the Cyber Crime Police Station, Bangalore. A Detective Inspector registered the case and tracked the e-mails. The mails had originated from Nigeria. Due to the trans-national nature, the Police could not prosecute the culprit. The only remedy they could offer was to correspond with g-mail, the e-mail service provider and block the e-mail account.

Thus, the findings and the news features provide proof that the Third Hypothesis is positive.

Fourth Hypothesis:

The Information Technology Act 2000 is casually enforced unlike other penal legislations; The Act requires amendments with the changes in the technology and types of usage of cyber space;
The following Tables are used as proof of this hypothesis:

The findings of Table 4.6 indicate that a very large number (81%) of the respondents opine that penal provisions for Tampering with computer source Document as laid down under S.65 is inadequate. The Information Technology Act-2000 provides for punishment as imprisonment for a period up to three years, or with fine which may extend up to one lakh rupees, or with both. The framers of the Act have not recognised the vitality of tampering with the Computer Source Codes, which may be the reason for the lenient punishment.

The findings of Table 4.7 indicate that a simple majority of the respondents have opined that punishment for ‘Hacking’, as laid down under S.66 is inadequate. The punishment for hacking is imprisonment up to three years, or with fine which may extend up to one lakh rupees, or with both.

Table 4.8 indicates that the respondent’s opinion to the adequacy of punishments as laid down under S.67 for publishing of information which is obscene, in electronic form. A sizeable number (43%) of the respondents have opined that the punishment of imprisonment of either description for a period up to five years and with fine of one lakh rupees for the first conviction; in the event of a second conviction, the punishment may extend with imprisonment of either description for a period which may extend to ten years and with a fine which may extend up to two lakh rupees. On the other hand, half the numbers (50%) of the respondents have opined as adequate.
The findings of Table 4.11 indicate that majority of the respondents (66%) disagree with the provision of S.79 that a Network Service Provider not to be liable in certain cases. This is with the popular belief that the network service provider should know the content of the information posted in his Network Service, or should have exercised 'due diligence' in this regard.

Table 4.12 indicates that an overwhelming majority (95%) of the respondents have opined that the Information Technology Act-2000 is not capable of preventing Cyber Crime. This is due to the fact that the Act is of Dual Nature and incorporates Civil Provisions. The Act has chiefly aimed at Techno-Legal Compliance in the conduct of E-Commerce.

To support the contentions, the following articles and opinions from stalwarts in the field of Cyber law have been used.

**Parthasarathi Pati in Legalservices.com**\(^38\) has commented about the Information Technology Act-2000 as:

"'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislate the laws & by-laws also are neither perfect; the laws therefore enacted by them nor can be perfect. This law has emerged from the womb of globalization. It is at the threshold of development. In due course of exposure through varied & complicated issues it will grow to be a piece of its time legislation."

**NBO Article on Information Technology Act of India**\(^39\)

**CYBERLAW IN INDIA: THE INFORMATION TECHNOLOGY ACT, 2000 -SOME PERSPECTIVES**

---

\(^{38}\) Partasarathipati_legalservices.com

\(^{39}\) Cyberlaws.net
The Parliament of India has passed its first Cyber law, the Information Technology Act, 2000 which provides the legal infrastructure for E-commerce in India.

Looking from an overall perspective, the Information Technology Act, 2000 is a laudable effort by the Government to create the necessary legal infrastructure for promotion and growth of electronic commerce. As on date, the judiciary in India is reluctant to accept electronic records and communications as evidence. Even email has not been defined in the prevailing statutes of India and is not an accepted legal form of communication as evidence in a court of law as of today. The said IT Act, 2000 indeed is a step forward in that direction also.

As Cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defines in the IT Act are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act make it appear as if the offences detailed in the said IT Act are the only Cyber offences possible and existing. For example, cyber offences like cyber theft, cyber stalking, cyber harassment and cyber defamation are not covered under the Act.

Further IT Act talks of any agency of the government intercepting any information transmitted through any computer resource if the same is necessary in the interest of the sovereignty or integrity of India, the security of the State,
friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence. This is one provision, which is likely to be misused by future governments to suit their political motives as also for the purpose of victimization. No standards or provisions have been laid down by the IT Act, which define any conditions detailed above. The supporters of the cause of individual privacy and freedom see this provision as a gross violation of individual freedom and that aforesaid conditions are unreasonable restrictions, which are not permissible in the context of the rapid growth of Internet.

The biggest concern about the Information Technology Act-2000 relates to its implementation. The said Act does not lay down parameters for its implementation. Also when Internet penetration in India is extremely low and government and police officials, in general are not at all, computer literate, the Information Technology Act-2000 raises more questions than it answers them. It seems that the Parliament would be required to amend the IT Act, 2000 to remove the gray areas mentioned above.

All said and done, The Information Technology Act, 2000 is a great achievement and a remarkable step ahead in the right direction. The Information Technology Act-2000 is a first step taken by the Government of India towards promoting the growth of electronic commerce so that E-Commerce in India can leap frog to success. Despite all its failings, it is a first historical step. The other steps have to follow.
India calls for tough cyber laws after ‘The Sun’ alleged it was sold data by an Indian IT worker

India's Prime Minister Manmohan Singh has asked his officials and IT experts to consider changes in existing cyber security laws in the country.

He was speaking after recent allegations in a British tabloid of an Indian call centre fraud. The Sun claimed that bank details of 1,000 British customers were sold to an undercover reporter by a Delhi-based Indian IT worker. The worker named by the newspaper has denied the allegations. On Wednesday, Mr Singh chaired a meeting of top government officials and representatives of India's National Association of Software and Service Companies to review steps taken to curb cyber crime. He asked them to suggest changes in existing laws if necessary to "ensure that any break of secrecy, any illegal transfer of commercial or other privileged information and any other form of cyber crime is made a punishable offence", a statement released by his office says.

The findings and supporting articles prove that Fourth Hypothesis is positive.
FIFTH HYPOTHESIS

The Cyber Crime Police Station, Bangalore though well equipped and staffed is unknown to the victims of Cyber Crime; Corporate Bodies have their own internal Cyber Security mechanisms to handle cyber crimes.

The following Tables are used as proof of this hypothesis:

The finding of Table 4.25 reveal that a vast number (74%) of respondents have opined that the Cyber Crime Police Station, Bangalore, is not capable of investigating and detecting cyber crimes. A significant number (13%) of the respondents have not responded to this question, as they are not aware of the competencies of the personnel of the Cyber Crime Police Station, hence cannot opine either way.

This is reinforced by the findings of Table 4.19, where in, an overwhelming number (96%) of the respondents have opined that the Government or the law Enforcement agencies alone should not be worried about Cyber Crimes. In other words, they have mooted at a Private-Public Partnership (P P P) approach. This is due to the fact that cyber Crimes directly erode the E-Commerce base, which is essential for the I T sector’s growth in India.

The findings of Table 4.16 reveal that a very large number (97%) of the respondents have replied that their organisation have a specific Cyber Security protocol to handle cyber crimes.

The findings of Table 4.18 show that a overwhelming majority (98%) of the respondents have indicated that every organisation should have its own Cyber Security System for the prevention of Cyber Crimes.
To substantiate these findings, the following news articles are:

1. Computer crime Research center

**Tremendous growth of cybercrime, report says**

*Date: September 20, 2005*

*Source: Washington Post*

*By: Brian Krebs*

Online criminal activity of nearly every variety surged in the first half of 2005, fueled in large part by an increase in software security flaws and in the number of home computers being used against their owners' wishes to distribute spam, spyware and viruses, according to a new report.

The six-month period saw the discovery of a record 1,862 new software vulnerabilities, according to the survey from Cupertino, Calif.-based Symantec Corp., a computer security firm. The report classified nearly all of those flaws as moderate to high security threats and found that about 60 percent of them were in programs that run over the Internet.

Security holes in Web-based programs are especially serious threats for businesses because attackers can use them to bypass a company's outer security measures -- such as Internet firewalls -- or to access confidential information.

Some of the most common and dangerous vulnerabilities are found in Internet browsers. While Mozilla's Firefox browser gained

[^41]: http://www.computercrimeresearchcenter.com
popularity this year after being touted as a more secure alternative to Microsoft's ubiquitous Internet Explorer, security researchers uncovered 25 security holes in Firefox during the first half of 2005, nearly twice the number found in Explorer.

2. Sifynews quoting P T I has the following article:

India ranks fifth in reporting cyber crime cases

2009-03-31 19:22:01
Last Updated: 2009-03-31 19:36:32

New Delhi: India ranks fifth among countries reporting the maximum number of cyber crimes, the latest report released by Internet Crime Complaint Centre of the United States has said.

The US report analysing internet crime in 2008 compiled by experts from FBI, Internet Crime Complaint Centre (IC3) and other agencies shows the number of complaints from victims shot up by almost a third since 2007 with the total touching 275,284 cases in which about USD 265 million were lost globally. Cyber crimes record 50 percent rise in India.

http://sifynews.com
The United States led the tally of victims' complaints, while India remained at fifth by reporting 0.36 per cent of the global complaints received at IC3 which was about 1,000 complaints, the data said.

Majority of the fraudsters on the information highway, this year, resorted to the trick of selling products online but not delivering it to buyers who had already made payments.

It remained the most adopted method to cheat during the year with 33 per cent of internet crimes of this nature being reported, according to the report.

3. A news article by Soumya Menon in DNA News has the following:

"The conviction rate for cyber crime is zilch in Bangalore"

Soumya Menon / DNA

Tuesday, December 8, 2009 9:01 IST

Bangalore: The cyber crime cell in Bangalore receives at least 200 complaints every year, most of which pertain to Internet banking fraud. However, only 10% of the cases have been solved and a majority of them haven't even reached the trial stage yet.

http://www.DNAnews.com
Speaking on the matter, an officer with the cyber crime cell said, "It's very difficult to get evidence in some cases, as they involve scamsters from other countries. Extradition is not an easy task."

There have also been instances of victims backing out of the case because they don't want to be involved in lengthy judicial procedures. However, the most recent reason cited for the low detection rate is the increase in neo-cyber crimes such as phishing and illegal money transfer.

According to Director General of Police (Crime Investigating Department) Dr. D.V. Guruprasad, this has been the case since the cyber crime police station was set up in 2001. "Of 100 cyber crime cases that are reported, only 25 get detected. Not a single one results in a trial or conviction. But the conviction rate in this regard is abysmally low across the country," he said, adding that they are trying to find the cause for this phenomenon.

"The courts that conduct these trials are also clueless. With new kinds of cyber crime cases coming up everyday, the judiciary is finding it difficult to keep up. Considering the changing trends in cyber crime, everybody in the investigation process and the judiciary should constantly update their knowledge" Dr.D.V. Guruprasad said. He said that though the IT Act-2008 has been amended to cover all kinds of cyber offences, the process of prosecuting the offender is still very slow.

There have also been cases where the cyber cell has not been able to arrest offenders for crimes like online lottery scams and phishing because the offenders operate from countries such as Nigeria and UAE, where the rules of extradition are rather complex.

When asked to comment on the measures undertaken to tackle the changing face of cyber offences, Dr.D.V. Guruprasad said that the cyber
crime cell constantly upgrades its equipment and software to catch up with changing trends.

"Unless we upgrade cyber forensics, it becomes very difficult to crack cases. And this includes not just software and equipment, but also training of staffers. Taking note of this, the CID set up a training school, initiated by NASSCOM and the Data Security Council of India, several years ago. Through the training school, information on various aspects of cyber crime is given to police officers, bank officers, prosecutors, defence council, children and parents," Dr. D.V. Guruprasad said.

He said that the only way to tackle this spurt in cyber crimes is to evolve with the times.

4. An article in The Hindu E-Paper by Raghava M is as following:

Cyber crime police lose way in bureaucratic maze

By Raghava M.

BANGALORE: Nine years since the cyber crime police station was set up in Bangalore — the first in the country — not much ground has been covered in uncovering Internet misdemeanor.

While there are innumerable complaints related to use of computers for frauds and threats, the cyber crime police station has restricted itself to cracking cases of hacking, source code tampering and tracing generation of obscene content, all of which are punishable under the Information Technology Act 2000. Internet frauds and threatening mails come under the jurisdiction of the local police station.

44 http://www.thehindu-paper_bangalore
Poor record

“The enforcement agencies have failed to effectively deal with cyber crimes. They are lacking in knowledge and are ignorant of the advances made in the field of information technology,” said Venkatesh D. Pastey, an advocate who dealing with cases related to Information Technology Act 2000. The Corps of Detectives (COD) created its own cyber crime cell in 1999. This cell became the cyber crime police station in September 2001, a year after the IT Act came into force.

This police station was tasked not only with investigating cyber crimes but also to prevent them.

“When we set up the police station it was ahead of its time. Now perhaps we are way behind,” said the former Director-General and Inspector-General of Police R. Sri Kumar. “Like other police departments, this too has been affected because of irrational transfers,” he added.

The cyber crime police station was allocated four Deputy Superintendents of Police who are empowered to look into violations under the IT Act.

Officers interested in information technology were to have been posted here as they needed to be constantly updated to keep abreast of the fast moving technology.

“Unfortunately, officers have been posted in and out of this station. Officers who honed their skills in this field have been moved out, while those not having any interest are being posted here,” Mr. Kumar lamented.

The State Government is yet to constitute a mentor board comprising experts from the field of network security, systems, finance, cyber laws and prosecution to oversee the working of the cyber crime
police station. As such a board has not been set up; the cyber police have been taking help of experts on an ad hoc basis.

The above findings and articles indicate that the Fifth Hypothesis is positive.

SIXTH HYPOTHESIS

Cyber Crimes are preventable to a great extent by creation of awareness of it; involvement of experts in the field of Information Technology and by increasing the awareness levels of the users of the Cyberspace.

The following tables are used to prove this hypothesis:

The findings of Table 4.24 indicates that an overwhelming (90%) of the respondents are of the opinion that India should have a campaign on similar lines of The Department of Justice and Information Technology Association of America (ITAA), which endeavors to create awareness in the prevention of Cyber Crimes.

Table 4.23 on the contrary indicates that a significant number (37%) of the respondents have opined that Cyber Crimes of an obscene nature can be prevented by proper education in safety while using the net by women and children. A majority (63%) did not feel so. This may be
due to the fact that crime avoidance of any type will have a limited effect only.

News articles to support that education in the responsible use of the Cyberspace are necessary, which are as following:

I. The Hindu E-Paper:

“On the Internet, how much is too much?”

By Deepa Kurup

The web affords unlimited space but that does not mean it should translate into unlimited freedom; using the web to defame an individual is offensive; it is difficult to accurately trace the author of a post Misused: Thousands of bloggers continue to air their opinions, often extreme and offensive, oblivious to the repercussions.

BANGALORE: As many as 9,740 website links are thrown up when running a search with a phrase ridiculing the Indian President on the popular search engine Google. Of these, at least a few hundred websites host content that criticise the first citizen, often in harsh terms; one even hosts a game on flash player where you can fling virtual tomatoes on the President’s portrait. The Internet is inundated with such attacks, arguably offensive and hurtful, on several public personalities.

Last week a Bangalore-based engineering student ‘Y’ was arrested for allegedly posting “obscene content” about the President on the Internet under Section 469 of the Indian Penal Code (forgery for purpose of harming reputation). Later, he was released on bail. Police sources said the

http://www.thehindue-paper_bangalore
message was objectionable and not “obscene or pornographic”, as reported in some sections of the media. Two unsubstantiated versions did the rounds: the student had hacked into an official government website, and posted on her behalf: “I am a rubber stamp”. The second story is that ‘Y’ created an online profile under her name and posted the same.

**SC refusal**

Using the web to rant, make unwarrantable allegations or defame an individual is offensive, to say the least. However, those who campaign for a non-invasive Internet argue that laws are often misused to target individuals and stifle dissenting voices. Recently, the Supreme Court refused to quash criminal proceedings against a student, ‘A’. He had been prosecuted for creating an anti-Shiv Sena community on Orkut. ‘A’ had argued that he merely started the community, and also pleaded that his life would be under threat if he had to appear in a Maharashtra court. “Anything that is posted on the Internet goes to the public... you are a computer student and you know how many people access Internet portals,” the court said, adding that he will have to explain his conduct in a court of law.

**Debate**

This observation has triggered a debate among net users and academics who differ on the private — and public — nature of web space. Those who advocate boundless Internet freedom point to incidents in 2007 and 2008 where a political party consistently clamped down on individuals that criticised it, often resorting to violence and vandalism. But were these isolated cases? Or can a Right Wing Organisation — seen beating up women in a pub in Mangalore — use defamation laws against the retaliatory and witty Pink Chaddi campaign that spread though a social-networking site?
The Internet, unlike traditional media, is complicated for various reasons, one of them being that it is difficult to accurately trace the author of a particular posting. Gurumurthy of the IT for Change, a non-profit organisation, feels that Internet norms have to be evolved. "The Internet is global, and the laws also must be. The real solution can be a global public policy process, which is being considered at the Internet Governance Forum (a UN body)," he says.

The Indian IT Act, as it stands today, is being criticised as restrictive. Sunil Abraham of the Centre for Internet and Society says the law is "unclear and over-expansive". "If you are an individual blogger, a law like this could have a killing effect on creativity and free speech. You could call this a scare tactic: by making examples of a few people and scaring people from doing what could be normal web activities like forwarding a joke," Mr. Abraham explains.

The other argument is that technology and email gateways are seldom fool-proof. Mr. 'L', a software professional arrested in August 2007 for allegedly defaming Maratha king Shivaji by uploading an "offensive picture" on a social networking site, says "better clarity and awareness on laws is critical today".

For no fault of his, he spent 50 days in jail because the Internet Service Provider made a mistake in tracking his IP (Internet Protocol) address. "I later decided to go public though this meant prolonging the agony for my family, because there is no awareness and accountability in the net space," he says.

"I will never condone offending someone on the Internet — but if authorities want to keep the laws strict, then they must create awareness among users. Perhaps, websites can be asked to moderated content," Mr. 'L' says.
Laws of the land

Google and such websites act in accordance with the laws of the land. Moreover, these IP addressed can be manipulated and a random cruise through websites or social networks reveal that the next offensive message is just a few clicks away.

As Mr. ‘L’ points out, thousands of bloggers continue to air their opinions, often extreme and offensive, oblivious to the repercussions. It is time they pause to think about the possible consequences, before going ahead with their blogging.

2. The Hindu E-Paper:

“Cyber cafe, a security headache? “46

By Chitra V. Ramani

Contrary to rules, hardly anyone asks for user’s photo identity; 37 p.c. of Internet access in India is through cyber cafes; Cyber cafe owners have to maintain a log of users

Bangalore: Internet parlours a.k.a cyber cafés in recent times have become security headaches as suspected terrorists and fraudsters have resorted to using them for their activities. Several cases of hacking and threat emails have been traced to cyber cafés.

What is worrying is that this is happening even after the State Government issued a notification way back in August 2004 directing cyber café owners to compulsorily check the identities of customers and maintain a log of users. Cyber café owners are also required to have web cameras in place to photograph the customer in case he/she does not have a photo identity card.

http://www.thehindue-paper_bangalore
According to the findings of a survey conducted by the Indian Market Research Bureau (IMRB) International and the Internet and Mobile Association of India, 37 per cent of Internet access in India is through cyber cafés. This makes it all the more important for authorities to ensure that the guidelines as specified in the notification are implemented.

No ID sought

*The Hindu* visited a few cyber cafés in the city to find that the owners/attendants do not follow these regulations. At one café, the reporter found that there was in place a system for regular customers. However, none of the parlours asked for a photo identity card to check the user’s identity.

Mr. ‘B’ (19), who visits cyber cafés regularly, said that the customers in a few cafés are required to enter their names, addresses and contact numbers in the register. “However, many of us do not enter our names. We enter fictitious names, addresses and false numbers. This, so that even if our accounts are hacked into, we are not affected or tracked,” he said.

Restricted access

A cyber café owner said that he has in place a system for his regular customers. “We have an online register which is updated every day. Though we do not ask for photo identity, we request customers to give us their address and phone number which is fed into our online register. We also have a special software — one that restricts access to porn sites and another that logs off the Internet session after the time expires,” he said.

The police, on their part, have to visit the parlours and ensure that the owners follow the rules. Since this is not the case, the police themselves find it difficult to trace users while investigating cyber crimes. Mr. Alok Kumar, Joint Commissioner of Police (Crime), said that the police only visit cyber cafés if they receive information that the owners are not following rules.
"We cannot really check on a routine basis as owners may feel we are interfering with their business. But if someone complains or we receive information our officials will inspect the parlours," he said.

4. the Cyber Crime Police Station, Bangalore City has posted the following in its website:

**E - SECURITY TIPS for CHILDREN:**

Do not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. Do not send your photograph to anyone on the Net without first checking with your parents or guardians. Do not respond to messages or bulletin board items that are suggestive, obscene, belligerent or threatening. Never arrange a face-to-face meeting without telling parents or guardians. Remember that people online may not be who they seem to be.

**PARENTS:**

Use content filtering software on your PC to protect children from pornography, gambling, hate speech, drugs and alcohol.

There is also software to establish time controls for individual users (for example blocking usage after a particular time at night) and log surfing activities allowing parents to see which site the
child has visited. Use this software to keep track of the activities of your children.

GENERAL INFORMATION:

Don't delete harmful communications (emails, chat logs, posts etc). These may help provide vital information about the identity of the person behind these.

Try not to panic.

If you feel any immediate physical danger of bodily harm, call your local Police.

Avoid getting into huge arguments online during chat or discussions with other users.

Remember that all other internet users are strangers. You do not know who you are chatting with. So be careful and polite.

Be extremely careful about how you share personal information about yourself online.

Choose your chatting nickname carefully so as not to offend others.
Do not share personal information in public spaces anywhere online, do not give it to strangers, including in e-mail or chat rooms. Do not use your real name or nickname as your screen name or user ID. Pick a name that is gender and age neutral. And do not post personal information as part of any user profile.

Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.

Make sure that your ISP and Internet Relay Chart (IRC) network have an acceptable use policy that prohibits cyber-stalking. And if your network fails to respond to your complaints, consider switching to a provider that is more responsive to user complaints.

If a situation online becomes hostile, log off or surf elsewhere.

If a situation places you in fear, contact a local law enforcement agency.

Save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with Internet System Administrators or Law Enforcement Officials.
Suggestions for better security:

Use strong passwords. Choose passwords that are difficult or impossible to guess. Give different passwords to all other accounts.

Make regular back-up of critical data. Back-up must be made atleast once in each day. Larger organizations should perform a full back-up weekly and incremental back-up every day. At least once in a month the back-up media should be verified.

Use virus protection software. That means three things: having it on your computer in the first place, checking daily for new virus signature updates, and then actually scanning all the files on your computer periodically.

Use a firewall as a gatekeeper between your computer and the Internet. Firewalls are usually software products. They are essential for those who keep their computers online through the popular DSL and cable modem connections but they are also valuable for those who still dial in.

Do not keep computers online when not in use. Either shut them off or physically disconnect them from Internet connection.

Do not open e-mail attachments from strangers, regardless of how enticing the subject line or attachment may be. Be suspicious of
any unexpected e-mail attachment from someone you do know because it may have been sent without that person's knowledge from an infected machine.

Regularly download security patches from your software vendors.

The above findings and articles indicate that the Sixth Hypothesis is positive.

5.2 SUGGESTIONS

1. Definitions of crimes and penalties pertaining to Internet Time Theft, Cyber Stalking and on-line Fraud (internet fraud) are to be incorporated into the Information Technology Act-2000.

2. Provisions of law relating to credit card misuse are to be comprehensively addressed within the Act. The current application of the law pertains to the misuse of credit cards in the internet. This will have a wider ramification of the entire credit/payment/debit card related offences.

3. As with the conventional Law, where law of crimes and civil laws are separated, it may be necessary to evolve separate enactments for cyber crimes as cyber criminal law and cyber civil law.

4. Banks and financial institutions issuing the credit/debit cards must enclose a comprehensive brochure in instructing the customer of the likely chances of the card being misused and steps to avoid them. These instructions must be in simple
language and preferably in the local language along with English, for greater understanding of its safe use.

5. Many crimes relating to documents such as counterfeiting, forgeries etc are with the use of computer systems. While they amount to an offence under the Indian Penal Code-1861, relevant provisions to this effect are to be incorporated in the Information Technology Act.

6. Piracy is yet another type of computer facilitated crime that needs to be addressed in the Information Technology Act. The use of pirated software, audio/video products, copyright infringements are addressed in other enactments relating to Intellectual Property are to be incorporated within the Information technology Act.

7. Cyber cafés must be registered with the Cyber Crime Police Station and Identities of the users must be stringently checked. This has been seen as one of the single largest cyber security loophole.

8. Wider publicity to the crime avoidance is needed. Every cyber café must be made to publicise the dos and don’ts in the cyber space must be made.

9. Public education is a very vital aspect in the prevention of cyber crime. The proper use of cyber space and the cyber laws must be incorporated in the syllabus of computer education. This may be at the school and college levels.

10. Effective use of personal cyber security measures such as anti virus software, firewalls etc., must be publicised and encouraged to avoid victimization to cyber crime.

11. Effective training for the Police, Advocates and Judiciary, dealing with cyber crimes are needed.
12. Investigative methods, the effective use of Cyber Forensics must be imparted to a larger number of Police personnel. Regular Police Stations are usually the first responders to the crime or the crime scene.

13. Non Governmental Agencies and IT Companies must be encouraged to contribute their knowledge in the prevention, investigation and detection of cyber crimes.

14. While the Government of Karnataka and Karnataka State Police are to be lauded in their effort in establishing the Nation's first ever Cyber Crime Police Station in Bangalore City, further publicity of its functions, charter of duties, types of cases dealt with is necessary.

15. As the Cyber Crime Police Station is having the jurisdiction of the entire State of Karnataka, there is a need to have several more Police stations, one for each Police Range, at the least.

16. The Officers and Staff must be dedicatedly posted to these Police Stations.

17. The frequent transfers and rotation of the officers are seen as a hindrance by many senior level officers, retired officers and experts in this field.

18. As handling cyber crime cases are quite different from investigating and collection of evidence of conventional crimes, a separate Cadre and Recruitment for these posts are to be made. They may be in the 'Special' posts and enjoy status of an 'Expert', on similar lines of the Fingerprint Bureau.

19. The use of Access control devices such as biometric identification system should be used by all, as a precautionary security measure.
5.3: CONCLUSION

The findings of this research supported by various literatures, theories and cases reveal that Cyber Crimes are a universal phenomenon. They are global or trans-national in nature. Constant innovations and upgradation of technology makes several aspects of our lives simpler, e-commerce and business faster, crimes have also become more anonymous and losses due to cyber crimes are on the increase day by day. Technology and law are incorporated here to prevent, investigate and detect such crimes. While the world has sought uniformity in e-commerce, to facilitate uniformity in its business transactions, penal laws are always a contentious issue. Sovereignty, geographic territory and jurisdiction to police have drastically altered. The cyberspace has a different version of domain altogether.

While there is a universal agreement that crimes occur due to many social factors, economic situation and psychological state of the offender, cyber crimes differ in its nature. This study identifies the following issues relating to the Criminological Study of Cyber Crime:

1. Cyber crimes are mostly anonymous; so are the cyber criminals. Persons with repressed criminal behaviour in the physical space will not hesitate to commit crimes in cyberspace.

2. There is no loss of status or position for a cyber criminal. Hackers gain notoriety in cyber space, while a physical intruder is apprehended and incarcerated. If a hacker is detected, he will use a different identity and persist with his hacking, rather than being apprehended and incarcerated.
3. Cyber Crimes are intellectual crimes. A person with high levels of technological knowledge alone is successful in Cyber Crimes. He/she can escape detection by various means available in the cyber space.

4. Cyber laws are rarely a deterrent to a cyber criminal. The quantum of punishment is of no deterrence even in conventional crimes. Effective deterrence can be only by the certainty of the crime being investigated, detected and the Judicial process finding his/her guilt.

5. Cyber crimes are not only economic gain. They are for the vicarious pleasure. A cyber criminal may hack into a highly protected computer network or system, just as an adventurer seeks the thrill; a person may photograph a nude picture of a woman by invading her privacy and distribute it to his friends; a person may ‘morph’ a known females face over a nude body of another women and circulate it in cyber space. Obscenity in electronic form is a serious form of cyber crime.

6. Jealousy, hatred and wantonness find greater avenues of expression in cyber space. A jealous person can spread Malware such as Trojan Horse in the intended victim and gain information; hatred can lead to malicious programme or a e-mail bombing spree or simply defamation; a reckless person can create a logic bomb or alter the data or simply spread a virus in the network or system.

7. Just as internet is addictive, internet crime is addictive; A person visits a porn site unwittingly, but keeps repeating the visits and seeks more. A person who gambles on the net easily is addicted and so on.

8. Plagiarism, data theft, Piracy and other crimes facilitated by the use of computers or computer systems is one of the significant threats which fall both in the physical
space as well as cyber space. The erosion of Intellectual Property Rights issues is likely to cause losses beyond the scope of that of the conventional crimes.

9. The cause for concern of all is the phenomenon of cyber terrorism, which can destroy the e-governance base or destruct the e-commerce mechanism. In addition to this, the use of cyber space for covert terrorist communication has shown the world the vulnerability in which it exists.

However, public awareness is very essential through mass media regarding the vulnerability and avoidance of cyber crime. The use of Access control mechanisms such as biometric identification devices is needed in addition to the passwords, which must be confidential. The need to train the law enforcement agencies and the Justice system is re-emphasised here. Cyber surveillance in India is a must, to prevent and pre-empt cyber terrorism or the terrorists use of cyber space. Cyber Frauds are another area of concern. Techniques of detection are a grey area, as it involves multiple agencies. The losses are of the magnitude that there must be a coordinated effort.

In light of the valuable suggestions in my research, the Information Technology Act-2000 needs to be amended suitably in defining and punishing the offender with stringent penalty along with enhanced period of imprisonment, rather than fine only as is the case, without any further delay.

In conclusion, this is one of the few Criminological studies on Cyber Crimes. Though it has unraveled certain aspects of the problem phenomenon, more
studies are to be made. The issues relating to behaviour in cyber space, techno-legal compliance, cyber ethics and adherence to norms are quiet distinct from that of the physical space. While it is hoped that advancements in technology can provide solutions to the problems of cyber crimes, it is also hoped that the same advanced technologies do not give rise to newer challenges to the law in the cyberspace.