"Managing cyber crimes in India – issues and challenges"

***Mrs.Vineetha.P.K**

***Principal, Sarada Vilas Law College, Mysore**

Abstract

The use of internet has become the part and parcel of every educated person in this world. It has opened the gates to the information superhighway connecting the rest of the world to whole a lot of information and to all corners of the world at once. It connects the person sitting in the remote corner of the home or office to the entire world thorough the information highway called passionately web, cyber, etc. It connects everyone to his office, bank, electricity dept, water works, travel service, bazaar, bookshop, friend in other country and also dangerously and unknowingly to cyber criminals waiting to hit the gullible internet user. So comes to web of national and international laws with it's enforcing agencies and intelligence to curb this menace of cyber crimes and protect the society from high-end, sophisticated, high-tech criminals. The effectiveness of the implementation of the cyber laws in India is a utmost important to protect our society new generation of crimes and criminals and whether it has been successful in India or not is the present research question.

A preliminary pilot survey was conducted by the researcher to have deeper understanding of the internet and cyber scenario in the selected cyber cafes by way of questionnaire survey on the users of internet and center/café owners to understand the level of awareness about the cyber crimes and the preventive measures taken by the centers and the internet users to protect themselves from the cyber crimes. The research findings, suggestions and heartening facts about the susceptible children using internet in cyber cafes is detailed in the end of this research paper. This pilot study has opened the gate way showing the broad and clear direction for the researcher to go on with the main research journey.

Key words: **cyber laws, Information technology act, cyber crimes, internet providers.**

1. Introduction to research:

The research is go into the study and investigation of implementation of cyber laws in India. The Implementation of cyber laws has following research parameters –and ***the identification, investigation, prosecution, punishment and prevention of cyber crimes*** *by the enforcement* authorities which include special police force properly trained to handle such sophisticated crimes passionately called as ***cyber police*** (supported by technical wing for the

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

identification and detection of cyber crimes) and the ***Indian law courts*** with specially trained judicial authorities trained in the technicalities of internet crimes. The research would also study among the police and judicial authorities - the level of awareness of cyber crimes, their abilities (level) to identify the crimes, their knowledge level to understand the technicalities of the subject and process of crime and damage it has and it might in future cause and technical ability level to take up proper steps to stop the further damages to general public. The research would study also the enforcement personnel's social concern and ability to involve other stake holders from society like internet cafes, internet providers, education and other institutions (where in particular internet suave youths use the facility extensively for their official as well as past time) and national and international website launchers and maintaining super computer based web companies in the process of judicial administration and prevention of cyber crimes in India.

The research would not only be done on the primary sample survey of investigating officers from cyber police stations, the top-police officials involved in the cyber crime investigations, the judicial officers administering justice in cyber cases but also include cyber café owners and the general public especially who use internet for all their day to day activities like sending e-mails to friends and relatives, online shopping, paying bills using internet, online banking, money transfers and all their office works either from their home or office or from internet centers.

The research would also conduct excusive and exhaustive secondary survey besides traditional literature survey - the police records to know the nature and number of cases reported, number of cases investigated, tried, punished and also to understand the type of cyber crimes which are very common in India (to create awareness campaign to stop and prevent the menace) and to successfully prevent the reoccurrence of the same.

2. Introduction to main research Study:

The main aim research is to address the issues of prevention, investigation, prosecution and punishment of cyber crimes by Indian law enforcing authorities in the first level and in the second level about creating awareness, technical knowhow about the cyber crimes for detection, prevention and investigation purposes through suitable training and development programmes to a) investigating officers b) judicial officers c) internet centers d) educational institutions and e) general public (internet users) and in the third level the research would try to devise suitable "enforcement and technical" models to prevent and free the whole society from such sophisticated and dangerous crimes.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

2.1 Introduction to Pilot study: As a preamble to the main research whose objective of the phd research is to find the level of implementation of cyber laws in India associated pilot study is conducted to frame the main objectives of research which will go on last for next three years. The aim of pilot study was to understand the internet scenario in India and to have firsthand information about the users of internet at cyber centers and their level of understanding about cyber crimes.

3. Research objectives:

The main objective of the research is to find the level of implementation of cyber laws in India. The research would investigate and try to find the level of prevention of cyber crimes in India with research objectives addressing the issues starting from ***the stage of identification cyber crimes, investigation, prosecution and punishment stage.*** The research would also try to find the ways and means and the type of special internet based training required by all the wings of enforcement agency like police officers and their staff, judicial officers and their subordinates and others involved in the process of investigation and judicial delivery systems.

The pilot study conducted at the internet centers revealed several issues on the internet scenario of internet users and it has helped to frame the following main research objectives.

For the purpose of research the above deliberated broad main objective is further divided into following specific objectives and associated hypothesis for the purpose of research.

The specific objectives of the research are to find:

1. The nature and number of cyber crimes intimated to the cyber police in India.
2. The nature and number of cyber cases investigated (and charge sheeted) by cyber police.
3. The nature and number of cyber cases brought before the court and the effectiveness of the process of administration of justice in these courts.
4. The nature and number of cyber criminals prosecuted by court and the nature and number of cyber cases left untried for technical defects and problems.
5. whether the general public i.e internet users are aware of different types of cyber crimes and what is the level of their understanding and whether they are equipped to protect themselves from cyber crimes (while in internet use).
6. whether the Indian cyber police are properly trained to handle cyber crimes effectively.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

7. whether the Indian cyber police are properly equipped (technology and equipments) to handle cyber crimes effectively.
8. whether the Indian law courts (and it's officials) are properly trained to handle cyber crimes effectively.
9. whether the Indian law courts (and it's officials) are properly equipped (technology and equipments) to handle cyber crimes effectively.
10. whether the Indian government has been able to effectively handle and control cyber crimes (Prevention, prosecution and awareness and technical training) through their laws and enforcement wing in national as well as at state level.
11. whether the Indian government is able to foresee the future technology and the cyber crimes that could strike in future to shake the integrity, sovernity and social and national security, psychosocial health and well being of the entire nation.

The **pilot study** conducted helped the researcher to frame the following research null hypothesis based on the main objectives of the research.

The following are the null hypothesis framed for research:

1. **H_{01}** All the cyber crimes are NOT intimated to the cyber police in India.
2. **H_{02}** All cyber crimes are NOT properly investigated (and charge sheeted) by cyber police.
3. **$H_{03\ All}$** cyber cases brought before the court are NOT properly handled by court.
4. **$H_{04\ All}$** cyber criminals are NOT prosecuted by court because of technical problems.
5. **H_{05}** The general public i.e internet users are NOT aware of different types of cyber crimes and how to protect themselves from cyber crimes.
6. **H_{06}** The Indian cyber police are NOT trained to handle cyber crimes effectively.
7. **H_{07}** The Indian cyber police are NOT equipped to handle cyber crimes effectively.
8. **H_{08}** The Indian law courts (and its officials) are NOT trained to handle cyber crimes effectively.
9. **H_{09}**The Indian law courts (and it's officials) are NOT equipped to handle cyber crimes effectively.
10. **H_{010}** The Indian government has NOT been able to effectively handle and control cyber crimes (Prevention, prosecution and awareness and technical training)

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

This empirical study would survey would be conducted on the respondents drawn from general public, internet users at college and cyber centers , cyber police officials and judicial officers the cyber café personnel to understand the subject matter of research to lead to suggestions and conclusions useful for society and nation as a whole.

3.2 Pilot study objectives:

The pilot study conducted in the beginning of the research to frame the above broad lined objectives and hypothesis of research had the following specific objectives which were investigated and findings were arrived at. The objectives of pilot study was to

a) find the awareness level about the cyber crimes among the cyber cafe owners, the measures taken by them to prevent the cyber crimes happening in their centers, the level of prevention and the cyber environment created in the society and to guard against and decrease the susceptibility level and
b) find the level of awareness about the cyber crimes among the internet users in cyber cafes.
c) Find any other issues important observed and noticed in the cyber centers useful for the further main PhD research.

4. Literature survey:

4.1.1 Introduction to cyber crimes:

In simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. [1]Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.[1]

4.1.2 Cyber crime[1] can be recognized in two ways :

I. The Computer as a Target:-using a computer to attack other computers.

Ex:. Hacking, Virus/Worm attacks, DOS attack etc.

II. The computer as a weapon:-using a computer to commit real world crimes.

Ex:. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

4.1.3 Cyber Crime regulated by Cyber Laws or Internet Laws.

Technical Aspects[1]: Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

a) Unauthorized access & Hacking:-

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. By hacking web server taking control on another persons website called as web hijacking

b) Trojan Attack:-

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans.

c) Virus and Worm attack:-

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms.

d) E-mail & IRC related crimes:-

1. Email spoofing: Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

2. Email Spamming: Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3 Sending malicious codes through email: E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

4. Email bombing**: E**-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

5. Sending threatening emails, 6. Defamatory emails. 7. Email frauds, 8. IRC related

Three main ways to attack IRC are: attacks, clone attacks, and flood attacks.

e) Denial of Service attacks:-

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users..[1]

To summarize the computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber-terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

4.1.3 The statistics of Cyber Crimes[1] in world:

The statistics that have been obtained and reported about demonstrate the seriousness Internet crimes in the world. In a FBI survey in early 2004, 90 percent of the 500 companies surveyed reported a security breach and 80 percent of those suffered a financial loss (Fisher 22). A national statistic in 2003 stated that four billion dollars in credit card fraud are lost each year. Only two percent of credit card transactions take place over the Internet but fifty percent of the four billion, mentioned before, are from the transaction online (Burden and Palmer 5). All these finding are just an illustration of the misuse of the Internet and a reason why Internet crime has to be slowed down. [1]

4.2 The Information technology acts [2]and it's salient features:

The Information Technology ACT, 2008 was drafted by Ministry of Law, Justice and Company Affairs (Legislative Department) and passed on New Delhi, the 9th June 2000 The following Act of Parliament received the assent of the President on the 9th June 2000 and is available in government web site. The present form of the act includes as Amended by Information Technology Amendment Bill 2006 passed in Loksabha on Dec 22nd and in Rajyasbha on dec-23rd of 2008. the salient features of the act include in it's 1st to 13th chapters the preliminary, digital and electronic signature, electronic governance, attribution, acknowledgement and dispatch of electronic records, secure electronic records and secure digital signatures, regulation of certifying authorities, electronic signature certificates, duties of subscribers, penalties and adjudication, the cyber regulations appellate tribunal, offences, network service providers not to be liable in certain cases, examiner of electronic evidence and miscellaneous chapter. These chapter are exhaustive and detailed and really would need a quite along time for any law enforcement officials to digest and implement in their day to day process of administering justice and enforcing cyber on Indian soil.

4.3 The Advantages of Information technology acts[3]:

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

a) From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

b) Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

c) Digital signatures have been given legal validity and sanction in the Act.

d) The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

e) The Act now allows Government to issue notification on the web thus heralding e-governance.

f) The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

g) The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

h) Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and cause loss. The damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

5. Research methodology :

The research methodology focuses on the cyber law enforcement systems in Karnataka, it's officials and executives wing which include the top-police officers, sub-inspectors and other intelligence officials (respondents of the research survey) involved in the investigation of cyber crimes in Karnataka and the judicial officers who administer justice and have administered justice in the cyber related cases in Mysore and Bangalore. The research would also like to hold discussions and interviews with the information technology training wing at High court (in charge IT training of judicial officers) and in the Karnataka police head quarters which is in charge of training the investigating officers and other supporting regular and technical staff. This would be done to understand and research into the level and sufficiency of the training modules and to understand if any lacunas are there in training delivery and if any improvement and updation is required for the internet technology training given to these officials. The last but not the least the personnel operating in cyber cafes and internet centers and educational institutions using exhaustive internet to know about the types of internet crimes that could happen and the precaution they have taken in this regard and the know what improvements in prevention systems are required to prevent further internet crimes in India.

The research would design separate sets of questionnaires for the randomly selected respondents drawn from general cyber users, cyber café owners, officials of cyber police stations, judicial officers, IT training wing officers of high court and police head quarters and the other stake holders.

A suitable sample size would be selected on the basis of need of the research and time limitation of research. An initial pilot survey was conducted to design the detailed and specific objectives and research hypothesis on the subject matter of research whose findings and suggestions are detailed next. The research has designed the null hypothesis with regard to the objectives of the research and the same would be tested under statistical study using, random sampling methods, stratification techniques and suitable statistical tests.

5.1 Methodology of pilot survey:

The initial pilot survey is conducted to understand the awareness level on cyber crimes among general users and cyber café/centre owners and about preventive measures. The survey has selected ten cyber centers in Mysore and interviewed them with specific questions. A sample of fifty respondents among the internet users were selected and surveyed with questionnaire addressing the pilot study objectives. The data collected out of the survey

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

was averaged, stratified and suggestions and conclusions of pilot survey are drawn and detailed below.

5.2 Pilot survey results, observations and Outcomes:

The pilot survey has revealed that

a) The general public has only a partial awareness on the cyber crimes and different types of cyber crimes for which they are susceptible. They know about compute virus and not on email address hacking. They don't take much attention to the protection of their password particularly younger children. They forget to "put-off" the option of "remember the password for future use" and end up in giving away their password for unscrupulous hands. The use of face-book, twitter and similar social sites are commonly observed. There is gross lack of knowledge on e-commerce and e-banking cyber crimes among most of the internet users.

b) The cyber police has not visited these centers even once in the present year.

c) Most of cyber centers have put internet virus protection packages

d) Except one centre all other nine centers out of sample of ten have login system adopted where the user has register his name, email address and personal details to use the internet, but some time they are bypassed to browse the internet only by entering name.

e) Most of the centers (eight out of ten) insist on personal identity to be entered into the register. Two centers don't allow any user without their identity card/ driving license /etc. for their address proof (original – not Xerox copy) and they keep the scanned copy for future use.

f) Most of the centers on general holidays, Saturday's, Sunday's and vacation holidays mostly adolescent children browsing and playing video games without any sort of control on them. They are sitting in congested cubicles, not monitored by the supervisors of centers may get into addiction to these games and driven away from their studies. There is always a chance that they may put their eyes into to objectionable and psychologically unhealthy sites are a very heartening fact observed by the researcher.

g) Adolescent children also seen using social sites and there is chance of they share the information not conducive for their age and healthy social upbringing. They give wrong date of births and register themselves into these sites and social networks.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

h) The social sites are creating problems of publicizing personal information, photos and videos to all by some unscrupulous elements.

5.3 Inferences and Suggestions:

The pilot Survey revealed that

a) There is only a partial awareness among the general users about the cyber crimes and government agency should take care of creating more awareness on this type of crimes to general public which as dangerous or even more dangerous than gold chain snatching.

b) The cyber café/center owners have done appreciable work by adopting the system of asking for address proofs and identity of the cyber users. This system has been adopted after the enforcement agency made it compulsory from the year 2010 to have the login time and logout time of every user with their identity to identify incase of cyber crime takes place. But the enforcement agency should have a follow-up action to see whether their records are maintained properly or not by each internet centers in city for preventing the city users from cyber crimes.

c) The children may become addict to games and visiting unscrupulous and objectionable sites not suited to their age. Parents, teachers, responsible citizens, cyber café owners and enforcement officers should take some action in this regard to protect the psychological health of future generation of India.

d) The social networking is being visited by youth and also by adolescent children and they are used to share all sort of information and mostly about films and film personalities. This is grossly wasting the time and energy of our youth for this type of most uncreative browsing. This all is the area of attention and concern for all in the society.

e) The internet users should be taught to protect their password and importance of protecting the password. This should be done by the internet café/ center's (owners) supervisors and teachers of school and colleges.

f) There is total lack of awareness of how the e-commerce and e-banking crimes are penetrated and most are susceptible for this type of crimes when give away their personal details like name, address, email and email address and other passwords to the sites while making purchases or e-money transfers on internet without taking proper precaution.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1

g) The survey reveal a need of educating all users about the types of cyber crimes and their consequences and importance of protecting one's password/ bank pin number and email address while using internet.

5.4 Final conclusion of pilot survey:

The pilot study conclude that though there is a partial awareness about the cyber crimes, there is a need of "plan of action" from government to educate the public completely about it and the onus rests on the government and enforcement agency to protect the public from such specialized crimes. The study conclude with an appreciation of the preventive measures and systems adopted by cyber centers but they need to continuously monitor that system adopted is unscrupulously followed round the clock in their center to protect the society and his customers. The study concludes that children – the future of our country should be protected becoming victim to any type cyber addiction. They need to be monitored and guided so that their energy and precious age of learning is spent on education and career development rather than wasting time on games, social network and objectionable sites. They have to be guided to take the advantage of internet for their mental, intellectual and psychological growth and how to be away from the rest of the cyber ocean filled with crimes, terrorism, wild games and useless information and to learn to know the difference between good and bad.

6 Final word:

The researcher is confident after the preliminary pilot survey and will be heading towards a longer research journey and would sincerely try to find the present level of the implementation of cyber laws in India and also try to find suitable models for enforcement of cyber laws, prevention of cyber crimes and training requirement of enforcement authorities - through years of research which would be of help for government and all other stake holders in the process and especially to the benefit of the society in creating fearless environment where they will have happy surfing, e-banking, e-shopping and e-mailing internet experiences for their lifetime.

This page was created using **BCL ALLPDF Converter** trial software.
To purchase, go to http://store.bcltechnologies.com/productcart/pc/instPrd.asp?idproduct=1