SEMINAR AND WORKSHOP ON

DETECTION OF CYBER CRIME

AND

INVESTIGATION

Presented by

Justice K.N.BASHA,
Judge, Madras High Court,
Chennai - 600 104.

28.06.2010 & 29.06.2010

SARDAR VALLABHBHAI PATEL
NATIONAL POLICE ACADEMY,
HYDERABAD - 500 052.

CYBER CRIME

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

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

3.0. The term 'cyber crime' has not been defined in any Statute or Act.

3.1. The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet.

3.2. The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of special knowledge or expert use of computer technology. So what exactly is Cyber Crime. Cyber Crime could reasonably include a wide variety of criminal offences and activities.

3.3. CBI Manual defines cyber crime as:

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

(ii)Crimes in which computers are targets.

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

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

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

5. However, the rapid increase in the use of Internet has led to a spate in crime like child pornography, cyber terrorism, publishing sexually explicit content in electronic form and video voyeurism. The need for a comprehensive amendment was consistently felt and after sufficient debate and much deliberation, the I.T. Amendment Act 2008 was passed. The ITAA 2008 got the President's assent in

February 2009 and was notified with effect from 27.10.2009. The new IT Amendment Act 2008 has brought a large number of cyber crimes under the ambit of the law. Some of the significant points in the Amendment Act include introduction of corporate responsibility for data protection with the concept of 'reasonable security practices' (Sec.43A), recognition of Computer Emergency Response Team – India (CERT-In) as the national nodal agency empowered to monitor and even block web-sites under specific circumstances, introduction of technological neutrality replacing digital signatures with electronic signatures etc. Besides, the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

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

7. Cyber Crimes – Three categories :

- Against Property – Financial crimes – cheating on-line – illegal funds transfer.
- Against Persons – On-line harassment, Cyber Stalking, Obscenity.
- Against Nations – Cyber Terrorism – Damaging critical information infrastructures.

8. MODUS OPERANDI IN CYBER CRIMES

NATURE	MODUS OPERANDI
I. <u>OFFENSIVE MESSAGES</u> (Messaging, annoying, intimidating, insulting, misleading, defaming)	
<u>i. SMS</u>	❖ SMS of above nature may be sent using mobile phone of one's own identity or by acquiring a fade identity. ❖ Such SMS may be forwarded amongst groups and communities (inter/intra) in which case the actual source could not be fixed. ❖ Few SMSs had been circulated affecting public tranquillity; Eg: False Tsunami warning, false alarm as target of explosion.
<u>ii. MMS</u>	❖ Multimedia messages often defaming or obscene are sent among small groups using mobile phones/bluetooth ❖ If there had been a sharing in many mobile equipments the first source couldn't be fixed. Eg., Arrest of the Managing Director of bazee.com in a school MMS scandal in Delhi. ❖ Often captured in private places unknowingly for future exploitation.
<u>iii. Web based SMS</u>	❖ SMS can be sent by logging onto sites like way2sms.com by becoming a member of the site typing the message of choice and choosing destination to be sent any where in the world by concealing one's identity ❖ Way2sms never share the IP logs with law enforcement agencies.
<u>iv. Chat room messages</u>	❖ Chat room messages in internet relay chats happens by direct connection between each others' machines in which the IP logs are stored neither by Yahoo nor Google and so information shared in Chat rooms may be saved but can never be traced retrospectively to its origin.

NATURE	MODUS OPERANDI
II OFFENSIVE CALLS (Offender calls either by his/her own name or by acquiring false identity- Landline calls/mobile calls, web based calls, VOIP calls, Skype, Yahoo messenger, Chat room calls, overseas calls etc.)	
i. Landline/mobile calls	❖ Many landlines still have no caller Ids ❖ Difficulty if the connection is in a non-existent fictitious address.
ii. Web based calls	❖ Calls can be made by spoofing the mobile number using the sites like http://www.phonetrick.net/ www.prankdial.com/
iii. Overseas calls Landline/mobile	❖ For overseas landline/mobiles the details of the subscribers are not available without the co-operation of international agencies.
iv. Chatroom calls – VOIP Calls – Skype	❖ In VOIP it is difficult to ascertain the source as it passes through various international gateways before it enters the country to get terminated in an Indian operator's subscriber
III Deceptive messages (Lottery, cheating, job racket) (*SMS of lottery cheating, emails of prize money, articles, false promise of jobs, false mail for admission to a reputed University)*	❖ Greed of the victim is the main reason why cyber frauds are successful. ❖ SMS/Email messages of winning a lottery of prize money or articles, alluring people to deposit money. ❖ Clues available are email IDs and sometimes few mobile phone numbers. ❖ Live.com, Yahoo.co.uk domains IP which are frequently used never share the login IPs and it provides a conducive climate for commission of crimes. ❖ To the extent it was made available, the IP logs invariably had shown some Nigerian, Mediterranean, Middle East and American countries. Hence users details are not available.

NATURE	MODUS OPERANDI
	❖ The mobile numbers are often fictitious and seasonal. ❖ The Bank accounts are invariably bogus and have transient life; some times an innocent gets allured for commission by stating false reasons for the source of money. ❖ The following awareness messages have been propagated: Do not believe emails or SMS that say that you have won a million dollar lottery. Be way of strangers who promise to transfer Crores of rupees to your bank account. ❖ Similar cheating can be for prize of cars, for an employment to a job fetching high income, admission to a course in a reputed university abroad. ❖ Sometimes Nigerians use the tool of threat of an insider staying inside star hotels waiting for instructions to ignite an explosive if not parted with the ransom money by negotiations. ❖ Occasionally criminals hide behind proxy servers by concealing their real location of log-ins. ❖ (Threat to critical infrastructures and vital installations and public places) E-mails of threatening nature often with an intention to mislead or to deceive or to implicate another person by wielding threat to critical infrastructures.
<u>IV. DATA THEFT</u> *(Theft of proprietory information causing breach of confidentiality and integrity and thereby altering its utility value. More due to disharmony in employee/employer situations by disgruntled employees.)*	❖ Sensitive information belonging to business organizations is targeted by rivals, criminals and sometimes even by disgruntled employees. ❖ Disharmony in work place often makes the ex-employees to take away the valuable data or design or client information. ❖ Sometimes they damage it; delete it; or sell it to a competitor. ❖ Many a times the employers become suspicious about their ex-employees and attribute instances of data theft which the ex-employee was holding in his possession to carryout his official duties at the time of his employment. ❖ Frequently breach of Non Disclosure of Agreement (NDA) and Memorandum of terms of employment are often attributed to criminal activity by employers which in truth may be a civil violation.

NATURE	MODUS OPERANDI
V. IDENTITY THEFT	❖ Identity theft involves fraudulent or dishonest use of someone's electronic signature, password or other unique identification feature. ❖ It is the first step towards credit card fraud, online share trading scams and e-banking crimes.
VI. INTERNET VIOLATIONS OF COPY RIGHTS *(Internet violation of copyrighted informations like feature films, songs, music etc. IPR theft)*	❖ Posting of features films, part of the films, causing loss to the revenue and criminal violations of Copy Right Act, 1957 often challenges the film industries and law enforcement. ❖ Uploading happening in Indian servers can be deleted. ❖ If it is an International server, deletion happens by request. Despite that if persisting, deletion becomes a task of chance and persons behind the activity may not surface at all.
VII. FINANCIAL CRIMES – SPOOFING/PHISHIHG/ INTERNET BANKING *(Offender creates/Spoofs, the webpage of a bank or any organization in the guise of enhancing their security or updating the services, collects personal confidential information at various stages and abuses the information for causing wrongful loss, fraudulent transfer of funds in Internet banking)*	This is a wide term that includes credit card fraud, online share trading scams and e-banking crimes. ❖ In today's highly digitalized world, almost everyone is affected by financial crimes. ❖ Phishing usually involves spoofed emails that contain links to fake websites. ❖ Spoofing becomes a pre-requisite for causing deceptive belief and it follows phishing of vital information. ❖ Spoofing of the sites normally happens in bank pages if the intention is for a financial fraud. Other sites get spoofed for misleading the viewer or for causing embarrassment. ❖ A spoofed page becomes difficult to be distinguished by normal viewers. ❖ Phishing normally happens for credit card related information or for password details of internet banking. ❖ Internet Banking requires unique authentication. Forgotten PIN or password option generates new ones if answers to the questions match. New PIN or Passwords reach as mobile SMS, mobile phone security if compromised, criminals then know the precious PIN or Password. ❖ Fund transfer normally goes to bogus fictitious accounts within the country but far apart in Geography. ❖ Quick withdrawal happens through short living accounts and the offender manages to open further bogus accounts as a preparation for his future crimes.

NATURE	MODUS OPERANDI
	❖ Withdrawal happens mostly in ATMs by concealing the identity. ❖ Banking systems and mobile phone systems provide facilities without proportionate security breeding vulnerabilities. ❖ The system now is not immune for account opening or for activating a new SIM card by producing forged ID cards and non-existence characters or by impersonation. ❖ Sheer non-compliance of the KYC norms of RBI and verification norms of TRAI opens wide scope for criminal activities ranging from a disturbance call to a fraudulent fund transfer culminating even as a mean for anti-national activities. ❖ The following awareness message have been Propagated: Never respond to unsolicited emails asking for financial information
VIII. WEB PAGE HACKING *(The page gets defaced by altering the content of the file and appearance causing embarrassment and denial of service)*	❖ The primary objective in web page hacking is to deface and embarrass an organization or an institute. ❖ The intention may extend from causing a denial of service to bringing down a business competitor. ❖ Government sites get hacked and hackers sometimes claim responsibility for hacking; the intention being to cause defamation and damage to the dignity of the institution.
IX. SPAM/MALWARE/ ESPIONAGE	❖ Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. ❖ E-mail spam, known as junk mail, is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. ❖ Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. ❖ Malware is a wide term that includes viruses, worms, Trojans, rootkits, backdoors, spyware, botnets, keystroke loggers and dialers. ❖ Cyber espionage is the act of obtaining personal, sensitive proprietary or classified information without permission.

NATURE	MODUS OPERANDI
	❖ Also known as cyber spying, it involves the use of cracking techniques and malicious software including Trojans and spyware.
X. MOBILE DEVICE ATTACKS	❖ Threats to the security of mobile devices include unauthorized access, stolen, handsets, data theft, malware, phishing etc. ❖ Mobile devices are getting more computing power and are becoming increasingly feature rich. This increases the likelihood of attacks against potential vulnerabilities.
XI. DENIAL OF SERVICE	❖ This involves flooding a computer with more requests than it can handle, causing it to crash. ❖ In a Distributed Denial of Service (DDoS) attack, the perpetrators are many and are geographically widespread.
XII. SOCIAL ENGINEERING	❖ A social engineering attack tricks people into revealing passwords or other confidential information by making people believe an unanticipated situation. ❖ Training the personnel for handling such situations and effectively ensuring the "need to know basis" may be a viable solution.
XIII. VIOLATION OF PRIVACY *(Capturing and publishing the images, pictures and videos of individuals often without the knowledge and concurrence and thereby passing humiliation and embarrassment)*	❖ Normally females victimized in this way by the posting of pictures with an attachment of an unwanted message, often with the phone number to cause incessant disturbance by calls from international strangers. ❖ Social networking sites like Orkut have fairly responded to Police requests by furnishing the IP addresses and log details. ❖ Face book has proved to be a non-responsive, despite requests not withstanding even if addressed to any of the International organizations like Child Exploitation On-line Protection forums. ❖ Social networking sites like face book have maintained its unbroken silence if requests for deletion of posted pictures were addressed.
XIV. CYBER TERRORISM	❖ Cyber terrorism involves the use or threat of disruptive cyber activities for ideological, religious or political objectives.

NATURE	MODUS OPERANDI
	❖ Cyber terrorism can weaken a country's economy and even make it more vulnerable to military attack.
XV. OBSCENITY & PORNOGRAPHY *(Uploading obscene and lascivious materials in Internet and causing propagation and transmission: abusing children and uploading of images of such abuse)*	❖ International online sharing sites like Rapidshare, megaupload and various sites have provided a nurturing platform for the cultivation, propagation and transmission of the menace of pornography including children. ❖ Surprisingly sites like Paypal and other online payment sites have been hand in glove with such sites prompting one to infer that there might be a sharing of the proceeds of income by the propagation of pornography. ❖ Blocking of porno-sites had been a challenge both in technical and legal means because the content can be hosted in a different domain names or in different IP addresses from different geographies of the world.

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

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

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

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

13. Information Technology Act, 2000 & Indian Penal Code

- All cyber crimes do not come under the IT Act.
- Many cyber crimes come under the Indian Penal Code.

Sending threatening message by email	Section 506 IPC
Sending defamatory message by email	Section 499 IPC
Sending a mail outraging the modesty	Section 509 IPC
Forgery of electronic records	Section 465 IPC
Bogus websites, cyber frauds, phishing	Section 420 IPC
Email spoofing	Sections 465, 419 IPC
Web-jacking	Section 383 IPC
Criminal breach of trust	Sections 406, 409 IPC
Online sale of Narcotics	NDPS Act
Online sale of Weapons	Arms Act
Hacking	Section 66 of IT Act
Pornography	Section 67 of IT Act
Email bombing	Section 66 of IT Act
Denial of Service Attack	Section 43 of IT Act
Virus Attack	Sections 43, 66 of IT Act

14. PENALTIES AND ADJUDICATION :

The Information Technology (Amendment) Act, 2008, adds 8 offences, 5 of which are added to the Information Technology Act, 2000 and 3 to IPC.

15. The new offences are as follow :

Sl.No.	***Section***	***Description***
1	66	As proposed in ITAA, 2008, this Section combines contraventions indicated in Section 43 with penal effect and reduces the punishment from 3 years to 2 years. It also introduces the pre-conditions of "Dishonesty" and "Fraud" to the current Section 66.
2	66 A	Punishment for sending offensive messages through communication service, etc.
3	66 B	Punishment for dishonestly receiving stolen computer resource or communication device.
4	66 C	Punishment for identity theft.
5	66 D	Punishment for cheating by personation by using computer resource.
6	66 E	Punishment for violation of privacy
7	66 F	Punishment for cyber terrorism.
8	67	Punishment for publishing or transmitting obscene material in electronic form.
9	67 A	Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
10	67 B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
11	67 C	Preservation and retention of information by intermediaries.
12	71	Misrepresentation to the Controller or the Certifying Authority. Making any misrepresentation to or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be.
13	72	Any person who, in pursuance of any of the powers conferred under IT Act, has secured access to any electronic record, book, register, correspondence, information or document without the consen of the person concerned discloses such electronic record, book, register, correspondence, information, document to any other person.
14	73	Publishing Digital Signature Certificate false in certain particulars. Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge that the certifying Authority listed in the certificate has not issued to other subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
15	74	Creation, publication or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose.

16.0. IMPORTANT SECTIONS OF IT ACT 2000 :

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

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

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

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

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

16.3.0. **Section 46 (Power to adjudicate – Adjudicating Officer)** empowers the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a Stale Government to be an adjudicating officer for holding an inquiry regarding the commission of the offences laid out in Chapter IX in the manner prescribed by the Central Government. The persons appointed shall possess such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government. Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction. This is also discussed in ***S.Sekar v. The Principal General Manager (Telecom), (BSNL),*** **MANU/TN/9663/2007.**

16.3.1. Every adjudicating officer appointed as above shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under Section 58(2). Further all proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code, 1860 and it shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973.

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

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

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

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

(c) the repetitive nature of the default.

16.5. **Section 65 – Tampering with computer source documents** – Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Tampering with computer source documents was discussed in ***Syed Asifuddin and Ors. v. The State of Andhra Pradesh and Anr.*****, 2005 Cri L J 4314,** ***Jigar Mayurbhai Shah v. State of Gujarat,*** **(2008)2GLR1134,** ***Pootholi Damodaran Nair v. Babu*****, 2005(2)KLT707, and** ***Ravi Shankar Srivastava v. State of Rajasthan,*** **2005(2)WLC612.**

16.6. **Section 66 (Computer related offences)**– This Section deals with hacking the Computer System and states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource

or diminishes its value or utility or affects it injuriously by any means, commits hacking. It further states that whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both. The case of ***Nirav Navinbhai Shah v. State of Gujarat and Anr.*****, MANU/GJ/8458/2006 involved Section 66.**

16.7. **Section 67 – Punishment for publishing or transmitting obscene material in electronic form :** This Section was in question in ***Dr. Prakash v. State of Tamil Nadu and Ors.,*** **AIR 2002 SC 3533,** ***Fatima Riswana v. State Rep. by A.C.P., Chennai and Ors.,*** **(2005) 1 SCC 582**, ***Assistant Commissioner of Police, Crime Record Bureau, Inspector of Police v. Saravanan and others,*** **MANU/TN/1776/2003,** ***Avnish Bajaj v. State (N.C.T.) of Delhi,*** **(2005) 3 Comp L J 364(Del),** ***M.Saravanan v. State of Tamilnadu,*** **MANU/TN/8296/2006, and** ***Maqbool Fida Husain v. Raj Kumar Pandey*****, MANU/DE/0757/2008**

16.8. Sections 76, 68(2), 69 and 70 have been amended by the Information Technology Amendment Act 2008, Also See ***Firos v. State of Kerala*****, AIR 2006 Ker 279.**

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

16.10. **Section 72 (Penalty for breach of confidentiality and privacy)** Again if any person who, in pursuance of any of the powers conferred under the Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished under **Section 72** with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

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

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

which may extend to one lakh rupees, or with both.

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

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

16.15. **Section 79 (Exemption from liability of intermediary in certain cases)-** This Section declares that no person providing any service as a network service provider shall be liable under the Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the

offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. This issue was also discussed in the case of ***Sanjay Kumar Kedia v. Narcotics Control Bureau and Anr.*, (2008)2 SCC 294**.

16.16. The Amendments brought about by the Information technology Act in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 came up for consideration in ***State of Punjab and Ors. v. Amritsar Beverages Ltd. and Ors.,* (2006) (7) SCC 7, *In Re: Sr. Abaya* 2006 Cri.L.J. 3843, *SICOM Ltd v. Harjindersingh and Ors.,* AIR 2004 Bom 337, *Vishal Paper Tech India Ltd. and Ors. v. State of A.P. and Anr.,* 2005Cri L J 1838, *Sri. P. Padmanabh v. Syndicate Bank Limited*, AIR 2008 Kant 42, *Steel Tubes of India v. Steel Authority of India*, 2006 Cri L J 1988, *V.K. Soman Achari v.: Sabu Jacob and Anr.*, 2007 Cri L J 1042, *Indira Priyadarshini Forum v. State of Kerala*, 2001 Cri L J 2652.**

17.0. Cyber crimes in India :

17.1. Cyber Crimes have emerged as a serious global threat, forcing governments, police departments and intelligence units to adopt counter measures.

17.2. The CERT (Computer Emergency Response Team), the apex cyber security division under the ministry of information technology of India, found that cyber crime in the country has accelerated about 50 times since 2004.

17.3. The agency recorded just 23 cyber crime incidents in 2004 in contrast to a huge 1,237 in 2007. These primarily included phishing attacks,

distribution of viruses/malicious code and illegal infiltration to computer networks.

17.4. A high ranking official from the IT ministry told DNA on April 8, 2008 that phishing is a kind of fraud in which an online criminal tricks the user and grabs his/her secret online banking details such as account number, or security codes like password to access those accounts.

17.5. Further, according to annual report for 2007 of CERT, there were 392 incidents of phishing, 358 cases of virus proliferation and 223 cases of network infiltration recorded in 2007. Compared to this, there were only 3 phishing attacks, 5 cases of virus proliferation and 11 incidents of network infiltration reported in 2004.

17.6. These statistics from CERT are, however, only indicative without giving the actual picture of cyber crime in India. The agency merely maintains records of cases that are notified to it.

17.7. Furthermore, a data of the government revealed that in January 2008, 87 security related incidents were recorded in contrast to 45 in December 2007. Of these, 47% involved phishing, 25% related to worm/virus under the malware category, 21% to unauthorized scanning, and 7% to technical help under separate categories.

18.0. **Tamil Nadu State :**

18.1. As far as Tamil Nadu State is concerned, Tamil Nadu Police formed two Cyber Crime Cells in the year 2002 – one in the Central Crime Branch, Egmore

for Chennai City and the another in the CBCID Headquarters, Chennai, for the entire state of Tamilnadu. Recently another Cyber Crime cell has been sanctioned for Coimbatore city.

It is learnt that Dr.M.Sudhakar, Additional Deputy Commissioner of Police, Central Crime Branch, Chennai, is rendering commendable service in respect of registration of cases in cyber crime as well as its investigation.

18.2. **Year wise reported cases**

Reporting of cases to Cyber Crime Cell has increased due to awareness spread among the Net users regarding the existence of separate investigation agency and a special Act. In particular, cases of Identity theft and cheating through Internet have increased.

19.0. Investigation and Computer Forensics :

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

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

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

19.3. The stages in computer forensic investigation are usually as follows:

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

Chain-of-custody is one of the controls used by courts to satisfy admissibility standards. Chain-of-custody is a process consisting of methodical checklists and procedures during the collection, preservation and analysis of evidence for the purpose of establishing authenticity and reliability of evidence. In other words, the evidence offeror tries to prove the chain-of-custody in order to rebut or minimize charges that evidence may be tainted or altered.

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

19.5. The Cyber Crime Investigating Officers are enhancing their technical knowledge by undergoing periodical training organized by Central Bureau of

Investigation Academy (CBI), Chaziabad, Tamil Nadu Police Academy (TNPA), Chennai, (Tamil Nadu Police Officers), Government Examiner of Questioned Documents (GEQD), Hyderabad, Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram, National Association of Software and Services Companies (NASSCOM), Chennai, Anna University, Chennai and Computer Emergency Response Team-India (CERT-IN), New Delhi.

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

20.1. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advises the five "P" mantras for online security, viz., **P***recaution,* ***P****revention,* ***P****rotection,* ***P****reservation and* ***P****erseverance.* A netizen should keep in mind the following things :-

1.to prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.

2.always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

3.always use latest and up date anti virus software to guard against virus attacks.

4.always keep back up volumes so that one may not suffer data loss in case of virus contamination

5.never send your credit card number to any site that is not secured, to guard against frauds.

6.always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

7.it is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

8.web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

9.use of firewalls may be beneficial.

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

20.2. In respect of using mobile phones, the public should not be carried away by S.M.S. messages offering attractive gifts and thereby inducing to part with huge amounts. Recently in a case at Chennai, a woman having been attracted by a S.M.S. message incurred a loss of Rs.57/- lakh as she was promised a huge sum of money. It is better to record the following news item:

"Woman falls for SMS offer, loses Rs. 57 lakh

S. Vijay Kumar

She was promised a huge prize money

Gang operated from India and abroad

CHENNAI: A woman who responded to an SMS was relieved of Rs.57 lakh by a gang that operated from India and abroad.

The 52-year-old graduate of Mylapore, who was promised a huge prize money as part of the 'World Cup Promotion Draw,' deposited the money in different bank accounts over a period of one month, starting third week of May. After realising the fraud, she lodged a complaint with the police.

According to police sources, the woman received an SMS in May second week, stating that she had won a cash prize worth a few crores of Indian currency. She responded to the email account that was mentioned in the SMS.

Days later, the complainant received an email in which the accused persons said the money would be delivered in India after obtaining necessary clearance from different agencies, including the United Nations and the Reserve Bank of India. They communicated the movement of the person bringing the cash box and asked her to deposit her money in various bank accounts for obtaining clearance from the immigration and customs authorities. A majority of the accounts into which the woman deposited money, ranging between Rs. 87,000 to Rs. 7.5 lakh, were opened in ICICI Bank. When there was no trace of the prize money even after depositing Rs.57 lakh, the victim lodged a complaint with Commissioner of Police T. Rajendran last week who directed the Central Crime Branch to form a special team and investigate the case.

"A major portion of the money was deposited in the accounts of Zulfikar Zariar, Javed Khan and Imran Zari. We have written to ICICI Bank to share the details of these account holders. The money was drawn from ATMs across the country,

including New Delhi and Mumbai. Video footage recorded by cameras in ATM machines could provide a clue to the identity of the suspects," an investigator told The Hindu.

"One of the accounts from which emails were sent was ukembassyact@yahoo.com. When contacted, Yahoo asked us to get in touch with law-enforcing agencies in the United States to get the user details," he said. Police suspect that the accused used fictitious names and documents to open bank accounts."

(Source : The Hindu dated : 23.06.2010)

20.3. The above case is only a tip of the iceberg. Therefore, the public should not only be aware about the effective functioning of the cyber crime cells, but they should also be vigilant in preventing such cases.

* * *