*Available online at http://www.journalcra.com*

*International Journal of Current Research*
*Vol. 6, Issue, 03, pp.5403-5412, March, 2014*

**INTERNATIONAL JOURNAL OF CURRENT RESEARCH**

**ISSN: 0975-833X**

## RESEARCH ARTICLE

# CYBER SECURITY AND RELATED CRIMES IN INDIAN SCENARIO

***Shriram, S.**

Engineering Professional, Working at Cognizant Technology Solutions, Chennai, Tamilnadu, India

**ARTICLE INFO**

***Article History:***
Received 05th December, 2013
Received in revised form
10th January, 2014
Accepted 14th February, 2014
Published online 25th March, 2014

***Key words:***

Cyberterrorism,
Cyber Laws,
Defamation,
Webjacking

**ABSTRACT**

Computers, Mobile phones and the Internet have become part of our life. As most human activities are part of computer and mobile networks, many traditional crimes have also changed their modus operandi and certain new crimes have come into existence. Most of these instruments permit their users a high degree of privacy. The technology does not distinguish between use and misuse, cyber criminals enjoy privacy too. The internet is a global medium while laws are mostly local. This makes investigation agencies difficult to find jurisdiction when a cyber crime originated out from a different country.



## INTRODUCTION

Computer crime, or cyber crime, refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of a crime. Net crime refers, more precisely, to criminal exploitation of the Internet. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Computer crime encompasses a broad range of potentially illegal activities. Generally, however, it may be divided into one of two types of categories:

(1) Crimes that target computer networks or devices directly
(2) Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device

This paper deals with various types of Cyber crimes that can be encountered over the net are:

### *A. spam*

Spam, or the unsolicited sending out of junk e-mails for commercial purposes, which is unlawful. New anti-spam laws are being passed in various countries which will hopefully limit the use of unsolicited electronic communications.

****Corresponding author: Shriram, S.***
*Engineering Professional, Working at Cognizant Technology Solutions, Chennai, Tamilnadu, India.*

### *B. Fraud*

Computer fraud refers to the fallacious misrepresentation of fact conveyed with an intention of inducing another to do or refrain from doing something that will ultimately lead to some major kind of loss.

### *C. Obscene or Offensive Content*

The contents of some of the websites and other electronic communications over the net can be really distasteful, obscene or offensive for a variety of reasons. In many countries such communications are considered illegal. It can be very troubling if your children are exposed to adult content.

### *D. Harassment*

This cyber crime encompasses all the obscenities and derogatory comments directed towards a specific individual or individuals focusing for example on gender, race, religion, nationality, and sexual orientation. Harassment is the cyber crime most commonly encountered in chat rooms or through newsgroups.

### *E. Drug Trafficking*

Drug traffickers use the Internet as a medium for trading their illegal substances by sending out enciphered e-mail and other Internet Technology. Most of the drug traffickers can be found arranging their illegal deals at internet cafes, using courier websites for the delivery of illegal packages containing drugs,

and sharing formulas for amphetamines in restricted-access chat rooms.

### *F. Cyber Terrorism*

Due to the increase in cyber terrorism, the hacking into official websites or the crashing of official websites, government officials and Information Technology security specialists have recently begun a significant increase their mapping of potential security holes in critical systems in order to better protect information sensitive sites.

### *G. Common Sources of Cyber crime*

Researchers at Sophos Labs claim to have created a language software that can figure out the host country of malicious software by tracing the default language of the computer on which it was programmed. According to their analysis of the default language linked up with about 19,000 samples at the end of last year, Americans and other non-British English speakers, surprisingly, produced a large proportion of malware. China produced 30%, Brazil with 14.2% and Russia produced 4.1% of the world's malware.

### *H. Information Technology (Amendment) Act 2008*

Information Technology (Amendment) Act 2008 has been notified and enforced on 27th Oct,2009.This Act punishes various cyber crimes including Cyber Terrorism.Important Sections Related to Cyber Crimes Chapter XI 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.

**Explanation**

For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

**Sec 66. Computer Related Offences**

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

**Explanation: For the purpose of this section**

a) The word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
b) The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

66A Punishment for sending offensive messages through communication service, etc Any person who sends, by means of a computer resource or a communication device,-

a) Any information that is grossly offensive or has menacing character; or
b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,
c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66 B. Punishment for dishonestly receiving stolen computer resource or communication device
Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66C Punishment for identity theft
Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D Punishment for cheating by personation by using computer resource
Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66E Punishment for violation of privacy
Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

**Explanation.- For the purposes of this section**

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
(d) "publishes" means reproduction in the printed or electronic form and making it available for public;
(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that--
(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66F. Punishment for cyber terrorism

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-
(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or
(iii) introducing or causing to introduce any Computer Contaminant.
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or
(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

67. Punishment for publishing or transmitting obscene material in electronic form
Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science,literature,art,or learning or other objects of general concern; or
(ii) which is kept or used bona fide for religious purposes.

67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever,-
(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or
(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
(d) facilitates abusing children online or
(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:
Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67 C. Preservation and Retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

68. Power of Controller to give directions
(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.
(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

Sec 69. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.
(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed (3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -
(a) provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or (b) intercept or monitor or decrypt the information, as the case may be; or
(c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Sec 69 A Power to issue directions for blocking for public access of any information through any computer resource
(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.
(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
(3) The intermediary who fails to comply with the direction issued under subsection
(1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.
Sec 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information.
(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.
Explanation: For the purposes of this section,
(i) "Computer Contaminant" shall have the meaning assigned to it in section 43 (ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Sec 70 Protected system
(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the

incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety.
(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)
(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

Sec 71 Penalty for misrepresentation
Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, 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.

Sec 72 Breach of confidentiality and privacy
Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, 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 with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Sec 72 A. Punishment for Disclosure of information in breach of lawful contract
Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Sec 73. Penalty for publishing electronic Signature Certificate false in certain particulars
(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that
(a) the Certifying Authority listed in the certificate has not issued it; or
(b) the subscriber listed in the certificate has not accepted it; or
(c) 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.
(2) Any person who contravenes the provisions of sub-section (1) 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.

Sec 74 Publication for fraudulent purpose
Whoever knowingly creates, publishes or otherwise makes available a Electronic 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
Sec 75 Act to apply for offence or contraventions committed outside India

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Sec 77 Compensation, penalties or confiscation not to interfere with other punishment
No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

Sec 77 A Compounding of Offences
(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.
Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of of a different kind.
Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.
(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

Sec 77 B Offences with three years imprisonment to be cognizable
(1) Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

**Intermediaries not to be liable in certain cases**

Sec 79 Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2)

and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.
(2) The provisions of sub-section (1) shall apply if -
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
(b) the intermediary does not-
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission
(c) the intermediary observes due diligence while discharging his duties under this
Act and also observes such other guidelines as the Central Government may prescribe in this behalf
(3) The provisions of sub-section (1) shall not apply if-
(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act.
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

**Explanation**

For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

Sec 84 B Punishment for abetment of offences
Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.
Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

Sec 84 C Punishment for attempt to commit offences
Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

Sec 85 Offences by Companies.
(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

**Explanation**

For the purposes of this section
(i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
(ii) "Director", in relation to a firm, means a partner in the firm
Offenses covered under IPC and Special Laws

1. Sending threatening messages by email
Sec.503 IPC
Section 503. Criminal intimidation
Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.
Explanation-A threat to inure the reputation of any deceased person in whom the person threatened is interested, is within this section.

2. Sending defamatory messages by email
Sec. 499 IPC
Section 499. Defamation
Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, of defame that person.
Explanation 1-It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.
Explanation 2-It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.
Explanation 3-An imputation in the form of an alternative or expressed ironically, may amount to defamation.
Explanation 4-No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character

of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.

3. Forgery of electronic records , Email spoofing
Sec 463, 464, 468, 469 IPC
Section 463. Forgery.
1Whoever makes any false documents or electronic record part of a document or electronic record with, intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

Section 464. Making a false document
1[A person is said to make a false document or false electronic record-
First-Who dishonestly or fraudulently-
(a) Makes, signs, seals or executes a document or part of a document;
(b) Makes or transmits any electronic record or part of any electronic record;
(c) Affixes any digital signature on any electronic record;
(d) Makes any mark denoting the execution of a document or the authenticity of the digital signature,
With the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or
Secondly- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or
Thirdly- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alterations.]

Section 468. Forgery for purpose of cheating
Whoever commits forgery, intending that the 1[document or Electronic Record forged] shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 469. Forgery for purpose of harming reputation
Whoever commits forgery, 1[intending that the document or Electronic Record forged] shall harm the reputation of any party, or knowing that it is likely to used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

**Bogus websites, cyber frauds**

Sec 420 IPC
Section 420. Cheating and dishonestly inducing delivery of property
Whoever cheats and thereby dishonestly induces the person deceived any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

**Web-Jacking**

Sec. 383 IPC
Section 383. Extortion
Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits "extortion".

**E-Mail Abuse, Online Defamation**

Sec.500, 509 IPC
Section 500. Punishment for defamation
Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.
Section 509. Word, gesture or act intended to insult the modesty of a woman
Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, of that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

**Criminal Intimidation by E-mail or Chat**

Sec. 506, 507 IPC
Section 506. Punishment for criminal intimidation
Whoever commits, the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both;
If threat be to cause death or grievous hurt, etc.: -And if the threat be to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or 1[imprisonment for life], or with imprisonment for a term which may extend to seven years, or to impute, unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

Section 507. Criminal intimidation by an anonymous communication
Whoever commits the offence of criminal intimidation by an anonymous communication, or having taken precaution to conceal the name or abode of the person form whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in

addition to the punishment provided for the offence by the last preceding section.

**Online sale of Drugs**

-NDPS Act

**Online sale of Arms**

-Arms Act
10. Piracy
-Sec. 51, 63, 63 B Copyright act
51.When copyright infringed:- Copyright in a work shall be deemed to be infringed ---

(a) when any person, without a licence granted by the owner of the Copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a licence so granted or of any condition imposed by a competent authority under this Act
( i ) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright, or
( ii ) permits for profit any place to be used for the performance of the work in public where such performance constitutes an infringement of the copyright in the work unless he was not aware and had no reasonable ground for believing that such performance would be an infringement of copyright, or
(b) when any person ---
( i ) make for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or
( ii ) distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright, or
( iii ) by way of trade exhibits in public, or
( iv ) imports (except for the private and domestic use of the importer) into India, any infringing copies of the work.

**Explanation**

For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an "infringing copy".

63. Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of-
(a) the copyright in a work, or
(b) any other right conferred by this Act, 125[except the right conferred by section 53A] shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees :
Provided that where the infringement has not been made for gain in the course of trade or business the court may, for adequate and special reasons to be mentioned in the judgement, impose a sentence of imprisonment for a term of less than six months or a fine of less than fifty thousand rupees.
Explanation.-Construction of a building or other structure which infringes or which, if completed, would infringe the copyright in some other work shall not be an offence under this section.

63A. Enhanced penalty on second and subsequent covictions. - Whoever having already been convicted of an offence under section 63 is again convicted of any such offence shall be punishable for the second and for every subsequent offence, with imprisonment for a term which
shall not be less than one year but which may extend to three years and with fine which shall not be
less than one lakh rupees but which may extend to two lakh rupees :
Provided that where the infringement has not been made for gain in the course of trade or
business] the court may, for adequate and special reasons to be mentioned in the judgment impose a
sentence of imprisonment for a term of less than one year or a fine of less than one lakh rupees:
Provided further that for the purposes of this section, no cognizance shall be taken of any conviction
made before the commencement of the Copyright (Amendment) Act, 1984.

63B. Knowing use of infringing copy of computer programme to be an offence.
Any person who knowingly makes use on a computer of an infringing copy of a computer programme shall be punishable with imprisonment for a term which shall not be less than seven days but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees:
Provided that where the computer programme has not been used for gain or in the course of trade or business, the court may, for adequate and special reasons to be mentioned in the judgment, not impose any sentence of imprisonment and may impose a fine which may extend to fifty thousand rupees."

**Obscenity**

Sec. 292,293,294 IPC, Indecent Representation of Women Act
Section 292. Sale, etc., or obscene books, etc.

(1) For the purposes of sub-section
(2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.]
3(2) Whoever-
(a) Sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or
(b) Imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or
(c) Takes part in or receives profits from any business in the course of which he knows or has reason to believe that any

such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) Offers or attempts to do any act which is an offence under this section,

Shall be punished (4)[on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees].

(5) **Exception:** This section does not extend to-

(a) Any book, pamphlet, paper, writing, drawing, painting, representation or figure-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art of learning or other objects of general concern, or

(ii) Which is kept or used bona fide for religious purposes;

(b) Any representation sculptured, engraved, painted or otherwise represented on or in-

(i) Any ancient monument within the meaning or the Ancient Monuments and Archaeological Sites and Remains Act, 1958 (24 of 1958), or

(ii) Any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose.

Section 292A. Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail

Whoever, -

(a) Prints or causes to be printed in any newspaper, periodical or circular, or exhibits or causes to be exhibited, to public view or distributes or causes to be distributed or in any manner puts into circulation any picture or any printed or written document which is grossly indecent, or in scurrilous or intended for blackmail, or

(b) Sells or lets for hire, or for purposes of sale or hire makes, produces or has in his possession, any picture or any printed or written document which is grossly indecent or is scurrilous or intended for blackmail; or

(c) Conveys any picture or any printed or written document which is grossly indecent or is scurrilous or intended for blackmail knowing or having reason to believe that such picture or document will be printed, sold, let for hire distributed or publicly exhibited or in any manner put into circulation; or

(d) Takes part in, or receives profits from, any business in the course of which he knows or has reason to believe that any such newspaper, periodical, circular, picture or other printed or written document is printed, exhibited, distributed, circulated, sold, let for hire, made, produced, kept, conveyed or purchased; or

(e) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any Act which is an offence under this section, or that any such newspaper, periodical, circular, picture or other printed or written document which is grossly indecent or is scurrilous or intended for blackmail, can be procured from or through any person; or

(f) Offers or attempts to do any act which is an offence under this section *[shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Provided that for a second or any subsequent offence under this section, he shall be punished with imprisonment of either description for a term which shall not be less than six months and not more than two years.

Explanation I-For the purposes of this section, the word scurrilous shall be deemed to include any matter which is likely to be injurious to morality or is calculated to injure any person:

Provided that it is not scurrilous to express in good faith anything whatever respecting the conduct of-

(i) A public servant in the discharge of his public functions or respecting his character, so far as his character appears in that conduct and no further; or

(ii) Any person touching any public question, and respecting his character, so far as his character appears in that conduct and no further.

Explanation II-In deciding whether any person has committed an offence under this section, the Court shall have regard inter alia, to the following considerations-

(a) The general character of the person charged, and where relevant the nature of his business;

(b) The general character and dominant effect of the matter alleged to be grossly indecent or scurrilous or intended for blackmail;

(c) Any evidence offered or called by or on behalf of the accused person as to his intention in committing any of the acts specified in this section.

Section 293. Sale, etc., of obscene objects to young person

Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offers or attempts so to do, shall be punished 2[on first conviction with imprisonment of either description for a term which may extend to three years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees.

Section 294. Obscene acts and songs

Whoever, to the annoyance of others-

(a) Does any obscene act in any public place, or

(b) Sings, recites or utters any obscene song, balled or words, in or near any public place,

Shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both.

**Theft of Computer Hardware**

Sec. 378, 379 IPC

Section 378. Theft

Whoever intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.

Explanation1. -A thing so long as it is attached to the earth, not being movable property, is not the subject of theft; but it becomes capable of being the subject of theft as soon as it is severed from the earth.

Explanation 2. -A moving effected by the same act which affects the severance may be a theft.

Explanation3. -A person is said to cause a thing to move by removing an obstacle which prevented it from moving or by separating it from any other thing, as well as by actually moving it.

Explanation 4. -A person, who by any means causes an animal to move, is said to move that animal, and to move everything which, in consequence of the motion so caused, is moved by that animal.

Explanation 5. -The consent mentioned in the definition may be express or implied, and may be given either by the person in possession, or by any person having for the purpose authority either express or implied.

Section 379. Punishment for theft

Whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

**Conclusion**

The major socio economic reason for the above mentioned cyber crimes are due to greed for becoming rich and to make quick money. Each country has different laws and the enforcement of such laws to the other countries is difficult unless there is a common effective organization like Interpol. So, there is a need for common organization which exclusively deals with cyber related crimes. The author has made an attempt to give a glimpse on the types of cyber crimes and relevant laws available in India to deal with such crimes under IPC and IT act. There is a need for stringent enforcement of law by the enforcement officers who are dealing with cyber crimes. The author suggests here, the enforcement officer should have the knowledge of computer and its network and the law relating to cyber crimes and cyber activities to enable them to handle such hi tech crimes which normally an ordinary law officer finds it difficult.

## REFERENCES

Atul Jain, Cyber Crimes: Issues, Threats and managements 2005.

NASSCOM –DSCI-Cyber lab

The Information Technology (Amendment) Act, 2008.

The Information Technology Act, 2000.

Understanding cybercrimes A guide for developing countries by ITU

Vivek Sood, Cyber Crimes, Electronic Evidence and Investigation, legal issues 2010.

Website of Department of Information Technology under Ministry of Commerce and IT.

*******