Vol 3 Issue 5 June 2013

Impact Factor : 0.2105

ISSN No : 2230-7850

Monthly Multidisciplinary Research Journal

Indian Streams Research Journal

IMPACT FACTOR : 0.2105

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Indian Streams Research Journal
Volume 3, Issue. 5, June. 2013
ISSN:-2230-7850
Available online at www.isrj.net
ORIGINAL ARTICLE

CYBER CRIMES AND ITS JURISDICTION

B.K. TIWARI

Cyber Law Expert , Advocate , Bhopal, District Court.

Abstract:

The Computer technology has expanded the scope for criminal Activities in the form of cyber crimes which are different from conventional crimes in their nature and scope. The origin of cyber crimes is be found in growing dependence on computers in modern life in 21 century when everything from microwave ovens and refrigerators to nuclear plats being run by computers, cyber crime has assured semester application . The introduction of new digital information and communications technologies has given birth to new types of crimes; these crimes are commonly known as cyber crimes. A set of legal domain has to develop to deal with this type of crime called information and communication technology law or more fashionable cyber law. In this article I tried to explore various cyber crimes and their classification.

KEYWORDS:

Net Crime, Hacking, crime-harassment, E-mail frauds (spam), service provider.

INTRODUCTION:

The computer may be used as a tool in these kinds of actively financial crimes, sale of illegal article, pornography, online gambling, intellectual property Crime, email spoofing, forgery, cyber defamation, cyber stalking, 'Computer Crime' or 'Cyber Crime' stated 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 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. These are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Today cyber crimes agent women are increasing day by day with the advert of the technology and it is causing a great threat to the security of a person. All over the world, the women are victims of such type of crime.

Cyber Crime contains all criminal offences which are broadly be classified in two categories. (1)

(A)Cyber crime where computer as a target of the crime,
(B)Cyber crime where computer as an instrument of the crime,

The term of cyber crime to usually restricted to describing criminal Activity in which the computer or network is an essential part of the crime, this term is also used to include traditional crimes in which computers or network are used to enable the illicit Activity.

(1) Parthasarthy pati :- Cyber Crimes (2003) P. 70

Title :CYBER CRIMES AND ITS JURISDICTION
Source:Indian Streams Research Journal [2230-7850] B.K. TIWARI yr:2013 vol:3 iss:5

Essential elemeants of the cyber crimes are as follows:-

(I) In cyber crime where the computer or network as target of criminal Activity include unauthorized access to information systems.
(ii) Cyber crime where the computer or network as a tool of the criminal Activity include spamming and copyright crimes,
(iii) In cyber crime where the computer or network is a place of criminal Activity include theft of service and certain E-mail frauds (spam),
(iv) The traditional crimes facilitated although use of computer or network. Cyber stalking is an example of traditional crime-harassment that has taken a new from when facilitated through computer network.

FREQUENCY USED IN CYBER CRIME

(a) Unauthorized access to computer system or Network as 'Hacking' is gaining unauthorized access to a computer or network of computer. Information Technology IT Act, 2000 Section 66 defines the offence of Hacking. The 'Act' has taken a unique approach to define the term “Hacking”. Hacking is usually understood to be unauthorized access of computer systems and networks. Indian law has chosen to define hacking in relation to information.

The Text of The Section 66 is as under:-

Hacking with computer system2

(1) Whoever with the intent 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 diminished its value or utility or affects it injuriously by any means, commits hacking.
(2) Whoever commits hacking shall be punished with imprisonment up to three years or with fine which may extend up to two lack rupees, or with both.

Such an Act of hacking case also includes 'Disruption of information systems'.

(B) Theft of information contained in electronic form: This includes information stored in computer hard disk removable storage media etc.

Internet time theft is an offence when same unauthorized person steals the hours of internet to be used by a person generally, the logic is that internet as a pay off service i.e. to avail the service person has to pay money to the “service provider” for a particular duration.

Email bombing: Email bombing refers to sending a large number of e-mails to the victim Resulting en the victim's email account (in case of an individual) or mail servers in case of a company or a mail service provider crashing. A simple way of achieving this would be to subscribe the victim's e-mail address to a large number of mailing lists. Mailing lists are very popular and it can generate a lot of daily email traffic depending upon the mailing list some generate only a few messages per day while other generate hundreds of such messages. It a person has been unknowingly subscribed to hundred of mailing list his incoming email traffic will two large and his service provider well probably deletes his all own.

Data diddling : This kind of attack involves altering raw data just before it is processed by a computer and then changing it back alter the processing when it is completed.

Data is a formalized representation of information knowledge, fActs, concepts or instruction that is intended to be processed is being processed or has been processed in a computer. Data may be in any form including computer printouts, magnetic or optical storage media, and punched cards or punched tapes. Data may also be stored internally in the memory of the computer.

Computer database means a representation of information, knowledge, pads, concepts or instruction in text, image, audio, video that are being prepared or have been prepared in a faradized manner or have been produced by a computer and are intended for use in a computer.

Of an person without permission of the owner or any other person who is in charge of computer, computer system or computer network he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so altered.

Solami attack: These attacks are used for the commission of financial crimes. The key here it's to make the alternation so insignificant that in a single case it would go completely unnoticed.

Internet financial crimes include cheating, credit cads frauds, money laundering etc. online fraud and cheating are the most lucrative illegal business that are being carried on with impunity in the cyber space to day some of the cases of online fraud and cheating that have come to the light are those pertaining to contractual deceit, take offering of jobs, credit cards crimes, mark sheet scandals and stamps scandals etc.

Logic boms : This programmer are Activated on the occurrence of a particular predefined event.

A logic bomb as a computer instruction hat codes for a malious Act when certain criteria are met such as a specific time in a computer's internal clock or a particular Action such as deletion of a program or a file in a computer program, a logic bomb also called stag code, is programming code inserted superstitiously or intentionally, that is designed to execute under certain circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to programs command. A logic bomb when exploded may be designated to display or print a spurious massage, delete or corrupt data or have other undesirable effects.

Denial of service attack: This involves flooding a computer resource with more requests than it can handle under the denial of service-attack; the computer of the sultrier is swamped with more requests than at can handle thereby causing the resource (e.g. a web server) to crash, denying authorized users, the service altered by such resource. These attacks are usually launched to make a particular service unavailable to someone who is authorized to use it this can be launched either by using one single computer or computers across the world. Where there are many computers in the source for launching, it is known as distributed denial service attack.

Virus/warm attacks: Viruses are programs that attach themselves to a compute or a file and then circulate themselves to other files and to other computers and of Network. A computer worm is a self contained set of programs that is able to spread functional copies of itself, or its segments to other computer systems, usually via Network connection unlike viruses, warm do not need to attach themselves to a host program. A program that propagates itself over a Network reproducing itself as it goes. The world's most famous warms was the internet warm “Let loose” on the internet by Robert Morris in the year 1988.

A warm may be designed to do any number of things such as delete files and a host system or send docs via e-mail worms may be multi-headed and carry other executables as a pay- load. However, even it the absence I such a pay-load, a warm can wrack havoc just with the Network traffic generated by its reproduction. My doom, for example, causes a noticeable world-wide internet slow down at the peak of its spread.

There are two types of warms:

(A) Host computer warms
(B) Network warms

Host computer warms are contained in the computer they run and use Network connection only to copy them selves to other computers. They are also called “rabbits”

Network warms consist of multiple parts called 'segments', each running an different machines and using the Network for several communication purposes. Network warms that have one main segment which coordinates the work of the other segments are sometimes called “octopuses”

Jurisdiction and sovereignty

The question of jurisdiction and sovereignty have quickly come the force in the era of the internet. The Internet does not tend to make geographical and jurisdictional boundaries dear, but internet users remain in physical jurisdictions and are subject to laws independent of their presence an the internet. As such a single transition may involve the laws are three jurisdictions.

(1) The jurisdiction of the laws of the state nation that apply where the server hosting the trans Action is located.
(2) The jurisdiction of the laws of the state or nation which apply to the person or business with who me the transaction happened so a user in one of United States conducting a transaction with another user in China through a server in Canada Would be theoretically be subject to the laws all above countries as they relate to the transaction at how.
(3) Issues related the medium of the internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international Jurisdiction norm of universal application.

(4) Issues related to jurisdiction major problem of cyber law lies in whether to treat the internet as it were physical space (means subject to a given jurisdiction's law) or to Act as in the internet is a world unto itself.
(5) The main jurisdiction the law of all states/nations in which the user resides.

CYBER LAW IN INDIA

The issue of cyber crime and digital evidence in India is primarily dealt with by the Information Technology Act, 2000, The Indian Penal Code, the Code of Criminal Procedure, 1973, Indian evidence Act and the Indian Evidence Act 1872.

The I.T. Act and amended I.P.C. prescribe various penalties and ingredient of offences. A large number of cyber crimes are actually dealt with by all I.P.C. The investigation and adjudication of cyber crimes are dealt with by the I.T. Act and the Cr.P.C. The Questions of digital evidence and its admissibility in court are dealt in Indian Evidence Act and the Banker's Books evidence.

Section 43 of the I.T. prescribes the various Acts for which a person will be liable to pay damages up to rupee one crore Section 44 provided penalties for failure to furnish any information or document required under the Information Technology Act. Section 45 provides for residuary penalty in the form of compensation up to Rs. 25 thousand to the attached person.

The Act specifically stipulates that any subscriber may authenticate and electronic record by affixing has digital signature. It further states that any person can verify and electronic record by use off a public key of the subscriber. The Act provides that electronic governance and inter alia amongst other that, where any law provides that information or any other matter shall be in writing or in the lybe written or printed form. The 'Act' also states the legal recognition of digital signatures for authentication of any electronic document.

The Act states a scheme for regulation of certifying authorities. The Act envisages controller of certifying authorizes who shall perform the function of exercising supervision new the Activities of the certifying authorities as also laying down standards and condition governing the certifying authorities as also specifying the various forms and content of digital signature certifying. The Act recognizes the need for identity foreign opportunity certifying authorities and it, further details the various provisions for the issue of license to issue digital signature certificate.

The Act States the establishment of cyber Regulation apple tribunal, which shall be an appellate body where appeals against the order paneled by the judicial officers, shall be performed. The Act describes about penalties and adjudication for various offence. The penalty for damage to computer, computer systems has been fixed as damages by way of compensation up to one crore affected person. The Act provided about various offence and the said offences shall be investigated by police officer not below the rank of the deeply superintend of police. These offences include tempering with computer source documents, publishing of information, which is obscene in electronic form and hacking.

The I.T. Act also provides for the constitution of the Cyber Regulation Advisory Committee, which shall advice the government as regards any rules or for any other purpose connected with the said Act.

Cyber stalking is an example of fractional crime harassment that has taken a new form when facilitated through computer Network.

(1) Jurisdiction
(2) Frequently used cyber CrimeConclusion

The aforesaid article of cyber crimes highlights the enormity and magnitude of these offence and their damaging effect on individual person, government, commercial or business organization, banks and financial institution, industrial enterprises and human society as a whole, cyber law in India in its infancy and is struggling hard to meet the contemporary information communication technology requirement Information Technology trends in India 2006, I.C.T. Trends in India 2007, Cyber security trends by PTLB-2007, etc have proved that India has not paid enough attention to the legal frame work for the information society and legal enablement of LCT system in India to worsen the situation we have a weak cyber and LCT securely in India cyber and LCT securely in India is a “Ignored world” and same is not going to improve due to the foully cyber securely strategy in India.

Govt. and the internet service provider must help the user to educate them and also to provide them necessary information an how best to protect them by developing the culture of cyber securities.

The need of time, therefore, is to enact a uniform cyber law for the preventing and control of cyber crime which would be universally acceptable to all countries around the world effective steps must be taken by all the state holders. Cyber eco system would flourish to effect maximum damage to the public

which are now becoming more and more dependent an Information Technology in the upcoming digital world.

SUGGESTION:

"Prevention is always better than cure" it is always better to take certain precaution while operating or use the Internet. A citizen should keep in mind of the following few precautions:

1.Citizen should avoid sending any photograph online particularly to third or unknown person and chat friends as there have been incidents of misuse of the photographs.
2.Website owners should watch traffic and check any irregularity on the site pulling host-bases instruction detection devices on servers may do this. Web server running public sites must be physically separately provided from internal corporate Network.
3.Citizen should avoid send credit card number to any site that is not secured, to guard against frauds.
4.Citizen should always use latest and update anti virus software to protect against virus attacks.
5.It is also advisable to prevent cyber stalking, avoid discloser any information pertaining to one self. This is as good as disclosing your identity ton third person in public place.

NOTES AND REFERENCE

I.Parthasarthi Pati :- Cyber Crimes (2003) P. 70
II.Information Technology Act 2000
III.Section 43 and 44 I.T.A. 2000