ESSENCE - International Journal for Environmental Rehabilitation and Conservation

Volume VII: No. 1 2016 [88 – 100] [ISSN 0975 - 6272]

[www.essence-journal.com]

Effect of Cyber Crime on Environment and Role of Enforcement Agencies in India: An Analysis

Chadha, Sanjeev Kumar

Received: January 31, 2016 | **Accepted**: February 19, 2016 | **Online**: June 30, 2016

Abstract

With the development of technology it can be easily seen in the society that the various offences is being done with the use of these technologies and therefore it is compulsion for the investigation agencies that they use these latest technology in their investigation and in collection of evidences. At one side advent of communication technologies benefitted the society while other side it has greatly affected the environment also. Now the problem arise for police department how they can nurture greater accountability towards society. Further many other researches shows that the police department and other concern department facing lots of problem regarding know how of the cyber crimes. With the fast growing technologies the number of cyber offender is increasing day by day while other side society including the environment is being affected and cyber crimes have become headache for all. Therefore it is required that the government should take initiative to prevent hidden effect of cyber crime on society especially on environment. Considering various effect of cyber crime over environment ultimately on society the researcher has discussed in present article various issues which is creating problem for our environment which need to be taken under serious consideration. In this article it has been discussed what can be role of the police and other concerned authorities to check the peril of cyber crime in this regard.

Keywords: Cyber Crime | Environmental Law | Enforcement Agencies | Indian constitution |

For correspondence:

Deptt. of Law, HNB Garhwal Central University, SRT Campus, Tehri Garhwal, U.K.
Email: **sk.chadha123@gmail.com**

Introduction

The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the information society. This development of the information society offers great opportunities. Unhindered access

to information can support democracy, as the flow of information is taken out of the control of state authorities. Technical developments have improved daily life – for example, online banking and shopping, the use of mobile data services and voice over Internet protocol (VoIP) telephony are just some examples of how far the integration of ICTs into our daily lives has advanced. However, the growth of the information society is accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICTs. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. Attacks against information infrastructure and Internet services have already taken place. Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. Most of the attacks against computer infrastructure are not necessarily targeting critical infrastructure.

On the basis of above statement it can be said that in present time the whole world is more interconnected through internet than earlier. At one side its advantage is that we can share information from one place to another while other side this fast growing connectivity brings increased risk of theft, fraud and abuse. Now a day as government is promoting modern technology the Indians become more reliant on these technologies resultant at one side we are being developed while other side we become more vulnerable to cyber attacks such as corporate security breaches, spear phishing, hacking and cyber terrorism etc which adversely doing effect our environment.

In this regard various law enforcement agencies performing an essential role in achieving our Nation's cyber security objectives by investigating a wide range of cyber crimes, from theft and fraud to effect on environment and apprehending and prosecuting those responsible. The environment is the integral part of nature and no one can live without environment therefore the role of police has become more important and they are proactively expected to provide multi-dimensional service to the people. The police can effectively work if they are equipped with the latest technology then only it can establish a people friendly police system. The researches show that in providing best services to the society police system still following the traditional trend and most of the officers remain unpractical and uncomfortable towards modern technological developments. At this juncture the modern technological development are providing comprehensive range of tasks to the people at one side while other side the police department is facing problem with this new technological development.

The abuse of technological developments which challenged the police and other enforcement governmental agencies is a new form of crime and is known as cyber crime. The article is an attempt to explore the possible changes needed in a system and suggest methods and technical skills that the law enforcement agencies should use to combat

with cyber crime so that the environment of this earth could be saved.

Cyber Crime

The term "cyber crime" has not been statutorily defined till now in any statute. Even the Information Technology Act, 2000 which deals with the cyber transactions not contain the definition of cybercrime. It is an umbrella term under which many illegal activities may be grouped together.

In this regard Pawan Duggal in his book titled "Cybercrime" has written that, *cybercrimes may precisely be said to be those species of crime in which computer is either an object or a subject of the conduct constituting the crime or it may be even both*. It means any activity that uses the computer as instrument, target or a means for perpetrating further crime, can be falls under the ambit of cyber crime. Here also because of anonymous nature of internet, there are many illegal activities occurring in the cyberspace which may enable the criminal minded people to indulge in various kinds of crimes which is known as cybercrimes. In this way cybercrimes is an offence which takes place on or using the internet through computer or other communication devices.

The medium of this cybercrime is technology and therefore, most of the cybercriminals are technically skilled who have thorough understanding of computer and internet. Therefore the *sine qua non* for cybercrime is that there should be an involvement of computer or internet at any stage.

At international level cybercrime defined by the U.N. Congress on Prevention of Cybercrime and Treatment of Offenders, which comprises two categories as follows:

> In narrow sense cybercrime connotes a computer crime and includes any illegal behavior directed by means of electronic operations that targets the security of the computer system and the data processed by them.
>
> In broader sense cybercrime includes all computer related crimes and consists of any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

In the Indian context, cybercrime may be defined as a voluntary and willful act or omission that adversely affects a person or property or a person's computer systems and made punishable under Information Technology Act, 2000 or liable under Indian Penal Code such as for e-mail spoofing, sending threatening mail, cyber defamation etc.

Classification Of Cyber Crime

In this regard R. Nagpal has clearly written in his book that, In general cyber crimes can be divided into following categories:

1. Cyber crime against person or individual: The cybercrime committed against persons disturbing him physically or mentally can be put in this category.

(A) Harassment via e-mail: It is similar like harassing through phone or letter. Sending

sexual, racial or religious mail which is concern for victim comes in this category.

(B) E-mail spoofing: Spoof mails are those which misrepresent its origin and it appears to originate from one source but actually emerged from some other source. In e-mail spoofing, the attacker creates a false context in order to mislead the victim and makes him believe it to be real with intention to retrieve victim's secret information.

(C) Defamation: There is no deference in traditional form of defamation and cyber defamation except medium which is being used by the criminal to defame. A person may be defamed through the help of computer and or the internet. For example if a person publishes defamatory statement over website or sends defamatory e-mails to someone's friends then it is called cyber defamation.

(D) Dissemination of obscene material: Here both the term 'dissemination' and 'obscene' are required to elaborate to understand the concept. The term dissemination is very broad term and it includes sale, distribution, promotion and exhibition and a material is obscene, if it predominantly draws an average person in the contemporary community to a shameful or morbid interest in nudity, sex or erection, such material if taken as whole lacks serious literary, artistic, political or scientific value. In this sense dissemination of obscene material through internet is a cyber crime.

(E) Indecent exposure: It means displaying of body parts specially genital parts of male or female inappropriately in public with obscene interest.

(F) Pornography or polluting through indecent exposure: Pornography can be put in the previous category of cyber crime i.e. dissemination of obscene material. In this regard as per the Oxford Dictionary the term 'pornography' means "*representation of the sexual activity virtually or descriptively to stimulate erotic rather than aesthetic feelings"*. As per the section 67 of the I.T. Act, 2000 if a person publishes or transmits or cause to be published in the electronic form, any material which is lascivious, or its effect is such as to tend to deprave and corrupt person who are likely to read, see or hear the matter contained or embodied in it, is punishable under this section and pornography always corrupt the mind of people so cover under this section.

(G) Pornography (specially child): Child pornography is a distinct kind of cyber crime and it is offence when committed without right. The conduct undertaken with artistic, medical, scientific purposes would not be considered as "without right"; instead, it will be rightful conduct. It includes offering, making available, distributing, transmitting, producing and even possession of child pornographic material.

(H) Cyber Stalking: Simple meaning of stalking is "to follow". When following is done through internet like posting messages or entering the chat-rooms or constantly bombarding the victim with e-mails etc. comes in this category.

(I) Unauthorised control/access over computer system: Any kind of access over computer system without the permission of the owner of the computer is popularly known as hacking. Section 2(1)(a) of the Information Technology Act, 2000 says 'access' means gaining 'entry' into or instructing or communicating with the logical, arithmetical, or memory function resources of a computer system or computer network. Section 66 of the I.T. Act, 2000 particularly provides for hacking and says that "whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damage to any person, destroys or deletes or alter any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, is said to commit hacking through unauthorized access"

2. Cyber Crime against Property

(A) Internet time theft: When someone who is not authorized to use the paid service of internet uses the internet without permission of the owner, it is known as internet time theft. This is done by gaining access to login ID and the password. Dewang Mehta in his book illustrated a good case in this regard. In that case Colonel Baweja had bought 100 hours which had been installed in his computer by a café owner. After one week Mr. Baweja found 94 hours had been used but actually he had not used those hours. He reported to police but police had not entertained him so he get it published as news in Times of India. When police commissioner read this news he ordered to reopen this case. Subsequently police filed a complaint for theft as at that time I T Act, 200 was not there.

(B) Denial of service attack (DoS): Denial of service attacks is a malicious act which denies to the user, legitimate access to a computer system. These attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. This can be launched by single computer or series of computers across the world. They are to very difficult to trace therefore it cause problem for enforcement agencies.

(C) Computer vandalism: It means physical damage to anyone's computer; it includes theft of a computer, some part of a computer or a peripheral attached to the computer or physically damaging a computer or its peripherals. Causing hindrance in the normal function of computer system through introduction of viruses, worms or logic bomb with the intention to gain economic advantage over a rival competitor or stealing data for extraction of money are some common form of computer vandalism.

(D) Intellectual property crime: Intellectual property is a bundle of rights which includes copyright, trademark, patent, GIs and industrial designs. The common forms which are vulnerable to cybercrimes are copyright, trademark and service mark. The Intellectual Property holder has certain rights to use his property alone but if some use that rights without permission with the help of internet, it is known as violation of

intellectual property right in form of cybercrime. In this regards software piracy, copyright and service mark violation are general.

(E) Virus transmission: The term 'virus' used first time by Fred Cohen in his thesis published in 1984 wherein he explained virus as program which propagate by attaching themselves directly to the computer programs.

3. Cyber Crime against State or Society

(A) Online illegal trafficking: Online trafficking is another kind of cybercrime. Online trafficking may be in drugs, human beings, arms, ammunitions, weapons and wild life etc.

(B) Online gambling: Online gambling involves huge volumes of transactions and cash flows that can obscure and disguise money laundering. Here players do not deal with a tangible, physical product and even physical currency does not change hands. As a result, illegal proceeds can be laundering by wagering them on one end of a transaction and receiving the payouts as gambling wins on the other end. Resultants as gambling winnings are tax free in many jurisdictions governments and authorities often incapable of monitoring these transactions and in this way government bear tax loss.

(C) Cyber terrorism: "Cyber terrorism is an unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives". It is a matter of global concern having both, domestic as well as international implications. The common form of terrorist attacks through internet is denial of service, hate websites, hate e-mails, attack on sensitive computer networks etc.. It may not be false to quote here that terrorist attack of September 11, on WTC in United States of America and of November 26, 2008 in India is an live example of cyber terrorism. Now a day world most technically advanced country are waging war against cyber terrorism.

(D) Sale of illegal articles: Now a day many websites providing platform to buy illegal articles like wild animals skins, narcotics, weapons, drugs and antiques etc. these are also distinguished branch of cyber crime.

(E) Financial scams and frauds: Cyber financial crimes include cheating, credit-frauds, money laundering etc. Money laundering is a very traditional crime of converting black into white money which involves physical cash transfer from one place to another place. When physical transfer of money laundering became unsafe and not feasible, the use of electronic transfer of money with the popularisation of internet gained momentum. There are many co-ordinated effort are being made at the international level to money laundering but the menace still persists in one form or the other due to lack of desired cyber forensic expertise.

Effect Of Cyber Crimes On Environment

If we analyses various kinds of cyber crime then it can be said that there is no any direct

impact of cyber crime on environment but indirectly it's affecting the environment at very large scale. There are some issues which can be linked up with the environment these are as follows:

1) Virus Attack And Environment:

The first issue which can be co-related with the environment is virus attack. As we know after virus attack the effected computer becomes dead or un-operational and therefore it becomes necessary to dismantle that computer or other effected electronic devices. Now as and when it becomes un-operational the problem regarding environment comes into picture because now a day the whole world facing the problem regarding destruction of dead electronic devices which are serious threat to environment.

2) Cyber Terrorism and Environment

Cyber terrorism also can be a serious threat to our environment. As we know now a days many terrorism activity is being done through internet which is known as cyber terrorism in which various terrorist group can explode bomb and other biological weapon without going to concerned place. Therefore in this way with the use of cyber terrorism any hazardous substance can be spread in the air, bomb can be exploded and various other activity can be done which is ultimately effect the environment.

3) Hacking and Environment

The other issue can be discussed here is hacking in this regard. As we know in present days most of the atomic power stations are controlled by the fully automatic electronic signals which run through internet. Therefore, there can be a possibility of hacking of this system by hackers and they can harm to the power station resultant nuclear substance can go into open atmosphere and cause serious damage to environment as well as to the human health.

Cyber Law In India

Prior to Information Technology Act, 2000 there was no separate and independent law in India to deal with the problem of cybercrime and all other computer related crimes which were tried under Indian Penal Code, 1860. The objectives of the Information Technology Act, 2000 as contained in the statement of the objects as follows:-

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with Government agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

From this statement of objects it clearly appears that the Information Technology Act was primarily introduced to facilitate and promote e-commerce but in subsequent year it brought to light certain lacunae and

shortcomings inherent therein which obstructed its smooth operation and therefore, it was amended in 2002 and again proposed to be amended by the Information Technology (Amendment) Bill, 2006 which was cleared by the Parliament on December 24, 2008 and received the assent of the President of India on February 5, 2009 and now it has been enforced as the Information Technology (Amendment) Act, 2008. The Amendment Act seeks to plug the loopholes in the existing Information Technology law so as to make it more effective.

The Grey Areas Of The It Act, 2000

1. The IT Act, 2000 is likely to cause a conflict of jurisdiction. This is the major problem for the enforcement agencies.

2. The IT Act, 2000 does not deal with any issues concerning the protection of environment in the context of the harmful effect on human. Contentious yet very important issues concerning environment have been left untouched by the law, thereby leaving many loopholes.

3. 4. As the cyber law is growing, so the new forms of crimes and manifestations of cyber crimes defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing.

5. The IT Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.

6. Another grey area of the IT Act is that the same does not touch upon any anti- trust issues.

7. The most serious concern about the Indian Cyber law relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. Also, when internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers.

Information Technologies, Cyber Crime And The Police

At this juncture in the era of the information technology most of the countries following the technologies which has already been used by the developed countries like United States, China, Germany, European Nations and Japan. In these countries most of the people working in the sector of IT as compare to other sector service men, industrial workers and farmers also it is obvious result of the lucrative salary package which are being given in this sector. IT personnel are those who gather, produce or distribute IT technologies from one place to other. These millions of IT personnel are mostly highly educated and living the same lifestyle irrespective of place. It can be easily seen in Indian context also where the new communication technologies such as internet, computers, telephone, satellites and cable television are bringing noticeable changes in the society. But irrespective of these noticeable changes there is a chance of being misguided of these IT Personnel by the various notorious groups and they become cyber criminals. These cyber criminal do work only for money

and for them there is no importance of society or environment because they operate various criminal activity from such place which can be very far from the affected area.

Therefore, in this regard it can be said that on one hand, the introduction of information technologies has generally facilitated services in public administration and has benefited the quality of life for citizens in almost all sectors like education, medicine, health, agriculture and industry. While another hand it has entailed a major area of challenges for the law enforcing agencies in form of cyber crimes.

Investigations And Search Procedures Under It Act, 2000

Section 75 of Information Technology Act, 2000 talks on jurisdictional matter in case of cyber crimes, and one would be punished irrespective of his nationality and place of commission of offence. Power of investigation is been given to police officer not below the rank of Deputy Superintendent of police or any officer of the Central Government or a State Government authorised by Central Government. He may enter any public place, conduct a search and arrest without warrant person who is reasonably expected to have committed an offence or about to commit computer related crime. Accused has to be produced before magistrate within 24 hours of arrest. Provisions of Criminal Procedure Code, 1973 regulate the procedure of entry, search and arrest of the accused.

Problems Underlying Tracking Of Offence

Most of the times the offenders commit crime and their identity is hard to be identified. Tracking cyber criminals requires a proper law enforcing agency through cyber border co-operation of governments, businesses and institutions of other countries. Most of the countries lack skilled law enforcement personnel to deal with computer and even broader Information technology related crimes. Usually law enforcement agencies also don't take crimes serious, they have no importance of enforcement of cyber crimes, and even if they undertake to investigate they are posed with limitation of extra-territorial nature of crimes.

Lecuna In Law Enforcement Regarding Cyber Crime

In present decade the new technological development has attracted attention of various law enforcement agencies to establish new institutions to supervise police and enable them to combat with the problem of cybercrime. In this regard the aim of police should be prevention or pre-emption of cybercrime rather than prosecution because in cases of cybercrime it is very difficult to punish cybercriminals because of jurisdictional issue and also as we are discussing here cyber crime as serious threat to environment, hence if any cyber activity already have done which affect the environment then it will be difficult to protect the environment. Therefore it is better to prevent such activities. Today law enforcement agencies facing a number of challenges in its combat against cybercrime, which can be identified as follows:

First: Laws defining computer offences and the legal apparatus needed to probe criminals

using the internet cannot match up with the fast scientific and societal developments.

Second: Procedural problem: it is very difficult for enforcement agencies to find out and summons the cybercriminal who operating online.

Third: last but not least that there is scarcity of well trained, well equipped investigators and prosecutors to detect high tech crime.

To counteract these emergent cyber threats, the role of the police in India must be redefined and the police force should be professionalized to perform its tasks in cyber space through various organizational and structural changes in order to re-institutionalise the existing occupational culture, which is the main obstruction for the police in combating cybercrimes.

In context of cybercrime it is very difficult for the police to maintain their jurisdiction over cyberspace and to exercise cyber patrolling. The success of combat against cybercrimes depends on the support that enforcement agencies gets from the legal systems and the support of community and the users of new technologies in cyberspace.

Steps To Be Taken To Prevent Cyber Crime

Though by passage of time and improvement in technology to provide easier and user friendly methods to the consumer for make up their daily activities, it has lead to harsh world of security threats at the same time by agencies like hackers and crackers etc. various Information technology methods have been introduced to curb such destructive activities to achieve the main objects of the technology to provide some sense of security to the users. Few basic prominent measures used to curb cyber crimes are as follows:

A) **Firewalls**: It creates wall between the system and possible intruders to protect the classified documents from being leaked or accessed. It would only let the data to flow in computer which is recognized and verified by one's system. It only permits access to the system to ones already registered with the computer.

B) **Encryption**: This is considered as an important tool for protecting data in transit. Plain text (readable) can be converted to cipher text (coded language) by this method and the recipient of the data can decrypt it by converting it into plain text again by using private key. This way except for the recipient whose possessor of private key to decrypt the data, no one can gain access to the sensitive information.

Not only the information in transit but also the information stored on computer can be protected by using Conventional cryptography method. Usual problem lies during the distribution of keys as anyone if overhears it or intercept it can make the whole object of encryption to standstill. Public key encryptograpy was one solution to this where the public key could be known to the whole world but the private key was only known to receiver, its very difficult to derive private key from public key.

C) **Digital Signature**: Are created by using means of cryptography by applying algorithms. This has its prominent use in the business of banking where customer's signature is

identified by using this method before banks enter into huge transactions.

D) Syncronised Passwords: These passwords are schemes used to change the password at user's and host token. The password on synchronized card changes every 30-60 seconds which only makes it valid for one time log-on session. Other useful methods introduced are signature, voice, fingerprint identification or retinal and biometric recognition etc. to impute passwords.

Conclusion and Suggestion:

After analyzing various issues regarding the effect of cyber crime on environment and role of enforcement agencies it can be conclude that there must be some major Insinuations would be developed by the Police department or other enforcement agencies to curb the cybercrime and in this regard following things needed to be considered:

1. The police department must take initiative to gather the information about the new technologies that are being used by the special cyber police of foreign countries like U.K. and America for investigation of cyber crimes. In this way they can develop itself as a high tech cyber cops.
2. In each district there must be a group of trained officers in form of special cyber cell to deal with cases of cyber offence which can be more serious to environment specially in cases of hacking and cyber terrorism. And also these offences should be taken very seriously because may be it would not directly create loss to anyone but it can have great impact on environment which indirectly affect the society. These specially trained officers should be efficient in detecting cybercrimes and be skilled in collection of digital evidence. These specially trained officers can be called as 'cyber cops'
3. The government should make mandatory provision regarding cyber cafes that they would ensure the identity of internet users who use their café for any purpose. In this regard there must be clear cut guidelines that the café owner will keep the records of internet user uses their café. Apart from this cyber café should maintain a record of visitors and also prohibit surfing of porn website or website containing obscenity, terrorism and other objectionable materials. Further also the local police stations should keep a vigil on the cyber cafes of their respective localities and they should ensure that no one could use the cyber café without valid ID proof.
4. For analyzing the cyber evidences there must be a cyber forensic laboratory at appropriate level so that the investigation process could become easy and fast..
5. There must be some awareness program organized by police or other enforcement agencies for the general public so that they could aware about cyber crime. In this regard awareness program or seminar can be conducted by the police or other enforcement agencies through website or by advertisement in educational institutions and at other public places. The contact information of cyber police should be properly advertised.

6. The police must maintain a separate data regarding cyber crime that should not be merged with the other traditional forms of crime because it is very technical matter. In this regard it is also that irrespective of rank all police officer must be provided wireless handset, computers, mobile telephones and internet to make them proficient in handling technology.
7. The cyber police must be trained in handling of latest technology to investigate cyber crime so that they could carry forward the legacy of the police department successfully. It is also that the training should be in such a way that they could realize the seriousness of cybercrime and give importance to complaints of cyber crimes. For this purpose special direction must be given to police officers that they should properly guide the people who come with complaint of cyber crime.
8. After 9/11 incidence in America and 26/11 incidence in India it is clear that various investigation agencies are not as proficient as they must be because both attack was although not directly cyber terrorism but the full blue print of the attacks was prepared through internet and also instruction were given through internet. Resultant our environment also got polluted; hence it is need of time that the police should be extra vigilant and sensible towards youth. In such cases of cyber crime police should not be lenient and they must take some hard step for the protection of nation as well as for the environment which is indirectly being affected in such incidence.

In this way considering all the issues discussed above in this regard the problem of cyber crime and its effect on environment can be prevented up to some extent and also police and various enforcement agencies can become more efficient.

References

Prof. Dr. Marco Gercke, Understanding Cybercrime: Phenomena , Challenges and Legal Response, ITU publication, 2012 available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (visited on 22-04-2015)

Ibid.

Pawan Duggal : Cybercrime (2003), p. 17.

Tenth U.N. Congress on Prevention of Crime and Treatment of Offenders was held in Vienna on April 10-17, 2000

R.K. Suri & T.N. Chabra : Cybercrime (Reprint, 2003) p.45.

R. Nagpal : What is Cyber Crime ? (2004), p.109, See also Dr. V. N. Paranjape, Cyber Crimes and Law, ed. 2010

p. 25-66

R.C. Mishra, Cybercrime: Impact in the New Millenium (2002) p.218

Vinod Kumar, Winning the Battle Against Cybercrime; p.83, see also Dr. V. N. Panajape, Cyber Crimes and law, Ed. 2010, Central Law Agency, Allahabad, p. 36

Bobby Art International vs Om Pal Singh, AIR 1996 SC 1846; see also Samaresh Bose vs Amal Mitra, AIR, 1986

SC 967

Oxford English Dictionary, 2000

Section 67 of the Information Technology Act, 200 as amended vide Information Technology(Amendment) Act, 2008

Dr. V. N. Paranjape, Cyber Crimes and law, Ed. 2010, p. 34

Dewang Mehta: Role of Police in Tracking Internet Crimes(2000) p. 179

Supra n. 15

Dr. V. N. Paranjape, Cyber Crimes and law, Ed. 2010 p. 57

R.K. Suri & T.N. Chhabra: Cybercrime (2003; Reprint) p.572

Dr. V. N. Paranjape, Cyber Crimes and law, Ed. 2010, Chapter IV p. 85

Dr. Fred Cohen in his doctoral research has defined “computer virus” as program that can infect to other programs by modifying them to include replicate version of itself.

McAfee Annual Reports 2014, Article : Cyber Pays: The Hidden Truth About Online Gambling Sites available on http://www.informationsecuritybuzz.com /cybercrime-pays-hidden-truth-online-gambling-sites/ (visited on February 26, 2015)

Dorothy E. Denning. "CYBERTERRORISM" Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University May 23, 2000 http://www.cs.georgetown.edu/~denning/ infosec/cyberterror.html , http://www.crime-research.org/library/Cyber-terrorism.htm (visited on March 3, 2015)

James R. Richards : Transnational Criminal Organisations, Cyber Crime and Money Laundering (1999) p.44

US Money Laundering Control Act, 1886 as amended in 1998; Vienna Convention organized by US in 1988 declared money laundering as a cybercrime. India enacted Money Laundering Act, 2002 which was amended in 2005.