Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01

DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

Cyber Law Violation in Digital Environment: An Overview

Dr. Ajai Veer

Assistant Professor, Faculty of Law, Shia P.G. College, Lucknow

Dr. Syed Nuzhat Husain

Assistant Professor, Faculty of Law, Shia P.G. College, Lucknow

Abstract

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

An Act or omission is punishable under the law inforce, is known as crime. The same explanation in also applicable to Cyber Crime. But there is not legal definition for Cyber Crime. The purpose of adding the word cyber, with crime is only to indicate that the computer has been used to commit and illegal act and to caution the users for safe guarding the electronic evidence, which is of fragile in nature. In short Cyber crime can be known as digital crime, cyber was a word coined by William & Gibson in his 1984 fictional novel 'Necromancer' cyber is the Prefix relating to the worldwide field of electronic communication crimes involving stealing fabricating, leaking or circulating forbidden digital information is collectively branched under the umbrella term cyber crime.

Cyber crime is the most recent type of crime that effect individual, institution and the nation internet has become a way of life for the people and the haven for the criminals. The growth of crime of internet is directly proportional to the growth of the internet itself.

The Police Team Investigating the e-mail threat on the lives of the President and the Prime Minister of India has prepared a sketch of the suspect who had sent them e-mail from a cyber cafe in the city.[1]

The world internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The internet is fast becoming a way of life

[1] The Hindu Newspaper, Sunday, 29 Aug., 2008.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

for million of people and also a way of living because of growing dependence and reliance of the mankind on these machines: Internet enable the use of Website, communication e-mail and lot of anything any where IT solutions for the betterment of human kind.[2]

Cyber crime is the most recent type of crime that effect individual, Institution and the Nation It challenges Police Prosecutions and Tame Makers enterer has become a way of life for people and the hayen for the criminals. Cyber and computer crimes are white collar crimes and are committed by the students non professional computer programmers business rivals individuals having vested internets and criminals.[3]

CYER SPACE AND CYBER CRIME

Before analysis cyber laws regarding, cyber crimes we must know the meaning of cyber crime and cyber space.

The term 'Cyber Crime' has not defined in any statute or Act The Oxford Reference online defines 'cyber crime as, crime committed over the internet. The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of Special knowledge or expert use of Computer Technology. So what exactly is cyber crime. Eeper prime could reasonably include a wide variety of criminal offences as activities.

CBI Manual defines Cyber Crime as:

i. Crimes committed by using computer as a means, including conventional crimes.
ii. Crimes in which computer are targets.

A generalized definition of cyber crime may be "unlawful acts wherein the computer either a tool or target or both". The information Technology Act 2000, does not define the term 'cyber crime' cyber crime can generally be defined as a criminal activity in which information technology system like computers and communication devices are the means used for the commission of the crime.[4]

[2] Criminal Investigating Department Review, Jan. 2008, Pg. 17
[3] Cyber Crime Journal, 2001, Pg. 185.
[4] FABIO GIACOMINLAND MD. HASANZAIDI, Electronic Evidence 2012, Pg, 378-380.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

The information and Technology Act 2000 for the first time brings the cyber crime punishment and procedure for proving it within legal frame work. It is said that "human beings are vulnerable so rule of law is required to protect them. Computer is also vulnerable so there must be law to safe guard it against cyber crime.

The Expression crime is defined as an act which subjects the does to legal punishment or any offences against morality. Social order or any injust or shameful act. The "offences" is defined in the code of criminal procedure to mean as an Act or omission made punishable by any law of the time being inforce.

Cyber crime is a termed used to broadly describes criminal activity in which computer or computer network are a tool, a target or a place of criminal activity and include everything from electronic cracking to denial of services attack. It is also used to enable to illicit activity.[5]

The Supreme Court of United States of America (U.S.) in ACLU v. Reno, explains the nature of cyber space as follows:

Anyone with access to the internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categories precisely but, as presently constituted that most relevant to this case are electronic mail (e-mail) automatic mailing list services ("mail exploders" some time referred to as "list services"') "News Groups", Chat Rooms" and the world wide web". All of these methods can be pictures, these tools constitute a unique medium particular geographical location but available to anyone, anywhere in the world with access to the internet.[6]

FACTORS CONTRIBUTING TO CYBER CRIME OR COMPUTER CRIMES

Computer systems are particularly vilnerable to cyber crime because of a number of factors. The most important contributors are analysed below:

- Quantum of data available in network
- Density of traffic in the networking systems

[5] Criminal Investigation Department Review Jan., 2008, Pg. 17
[6] ACLUVs. Reno 521 US 844 (26 June. 1997 decided) http:/www.epic.org/ed-decision.html

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

- Open and Easy connectivity
- Advancement of electronic technology
- Human involvement
- System accessibility

1. **Technology:** Hard Disk Capacity (space), memory capacity (RAM) and speed of new generation processors have considerably been increased due to technological advancement. These factors enable easy centralisation of large database other information and also their processing further it is easy to connect any system anywhere in the globe to any other system in the globe internet is the best example.
2. **Computer Viruses:** Viruses and Trojons may contain a "time-bomb" intended to destroy programs or data on a specific data or when some condition has been fulfilled.

   The damage caused by a virus may consist of the deletion of data or programmes, may be even reformating of the hard disk, but more subtle damage is also possible.
3. Easy Accessibility: The exposure provided through increasingly easy access to electronic data and system resources is an important contribution to the vulnerability of modern computer system. Two types of computer crime that exploit remote cases are:

a. These use of fraudulent identification and access codes to access the system resources.
b. The un authorised use to an unattended terminal, logged on by an authorized person.[7]

Accused in Rs. 400 millions SMS Scam Arrested in Mumbai: The alleged mastermind behind a Rs. 400 million SMS fraud that duped at least 50,000 people has been attested along with an associate more than two month after the scam was unearthed.[8]

4. **Impediments in Investigation:** The sophisticated nature of the crime makes detection and collection of evidence extremely difficult, placing the investigating authorities to great disadvantages. The lack of knowledge on the part of investigaling authorities with regard to the technical aspect involved in computer software, data processing, storage, networking, transmission etc, are also the contributing factors which embolden the computer criminals."[9]

[7] Rodney D. Ryder Guide, 2nd Ed. 2003 The Indian Cyber Law, Pg. 87,88.
[8] SMS Scam Case www.cyberindia.net
[9] Rodney D. Ryder Guide, 2nd Ed., 2003 The Indian Cyber law, Pg. 83-84,

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

TYPES OF OFFENCES UNDER CODE OF CRIMINAL PROCEDURE

Offences are cognizable or non -cognizable according to sec-2 and 2(1) of Cr.P.C: The Various oftences under information Technology Act 2000 are tribal in accordance with the Provision of Cr.P.C. The Information Technology has been made applicable to offences committed ouiside India and in sec. 76 Information Technology Act the Authorities can confiscate computer, computer system, floppy disc, compact disc, tape drives, communication device or other accessories:. The offences under the Information Technology Act, 2000 are:

1. Tampering with computer source document (Sec.-65).
2. Computer related offences (Section 66).
3. Publishing obscene information in electronic form (Sec. 67 to 67-B).
4. Decrypting information (Sec.-69 to 69-B).
5. Breach of Privacy and confidentiality (Sec.-72).
6. Publishing false statement in an electronic signature certificate (Sec. 73) and
7. Creation, Publication or making available an electronic signature certificate for fraudulent or unlawful purpose (Sec. 74).[10]

INDIAN CRIME SCENE

The Major Cyber Crime reported in India are denial of services, defacement of website, SPAM, computer virus and alarms pornography, cyber squatling cyber stalking and Pihsing, cyber crime is emerging as a serious threat worldwide government, police department and intelligence units have started to react. It is curve cross border cyber threat are taking shape.[11]

Phising: Pishing attacks were more popular among Indian users due to rising Internet Penetration and growing online transactions. India has now joined the dubious list of the world to 15 countries hosting "Phising" sites which aims at stealing confidential information such as passwords and credit cards details.[12]

In Case of Bank of India vs. maedi Shanker Rao where an account in her bank transactions misrepresented her and received money and it was proved that the signature on the reverse of the

[10] Electronic Evidence by FABIO GIACOMINI & MOHD HASAN ZAIDI, Pg. 401.
[11] Cyber Crime Scenario in India www.gcl.in.
[12] The Hindu Sunday, November. 26, 2006

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

form taken by the bank as a acknowledgement for the receipt of money to be that of the accused he was liable to be convicted under section 467 r/w Sec. 109 and Sec.471.[13]

In other case residential Malyal had an account in Nationalized Bank of Adoor costS 10,000 when the bank authorities heeded a fake e-mail request to transfer the amount to an account of ghana. In Mangalapuram a person transferred a large sum of money as "Processing Charge" to a foreign bank account after he received an e-mail which said he had won a lottery.[14]

CYBER CAFES E-MAIL

Cyber Cafe means any facility from where access to the internet is offered by any person in the ordinary course of Business to the member of public. (See Section 2(1) na of I.T.Act 2000). Cyber cafe has merged as a hot spot for cyber crime. Even terrorists with each otherprovide the secrecy through cabins constructed for users has also made the porn literature easily accessible to the People visiting them. [15]

23 years old person from Tiruchi was arrested by the city cyber crime Police on charge of sending an e-mail threat to the Chief Minister and his family. [16]

A 23 years old person from Tiruchi was arrested by the city cyber crime Police on charge of sending an e-mail threat to the Chief Minister and his fmaily.

STALKING

A 10th standard boy from Bangalore got into trouble when a girl much older than him started stalking him. She pasted "Love you slips on his gate and called his" on reviewing his orkut profile it was realized that he had accepted chat invites from more than 20 People only 2 of them who were his real life friends. [17]

HACKING

Website Dictionary defines the term 'hackers' as a computer enthusiast who enjoy learning everything about a computer system on network and through clever programming. Pushing the system to it highest possible level of performance.

[13] Bank of India vs. Maredi Shanker Rao AIR 1987 SC. 821: 1987 (i) Crimes 389: 1987 Cr. L.J. 722: 1987 (1) SCC 577
[14] Cyber Crime on the Risc. in St. Kerala. The Hindu Newspaper, Monday Oct 30, 2006.
[15] Chandigrah Tribune Monday, May 28, 2001
[16] The Hindu Friday, Aug, 10, 2007.
[17] The Hindu Tuesday, May 1, 2007.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

Essential of Hacking

The essential of hacking are:

a. Whoever

b. Intention or knowledge

c. Causing wrongful loss on damage to the Public or any person.

d. Destroying or altering any information residing in a computer resource or diminishes its value or utility or affects in injuriously by any means.[18]

A case of suspected Hacking of certain web portals and obtaining the residential address from the e-mail account of city residents had recently came to light after getting the addresses letters were sent through post mail and the recipients were lured in to participating in an international lottery that had Australian $ 23 Lakh at Staks.[19]

Effect of Cyber Terrorism

- Cyber terrorism can affect internet based business.
- Cyber terrorism can weaken and destroy countries Economy and even make it more vulnerable to military attack.
- Cyber terrorism can endanger the security of nation

Some Incidents of Cyber Attack

- Pro-Palestinian and Pro-Israel Cyber Group Cyber war.
- Pakistan terrorist target India's Internet Community.
- Massive website defacement and e-mail bombardment attack on USA by Pro-Chinese.
- Tamil and Estonia Cyber attach, Moonlight maze, Israel, Espionage Ring, Yugoslavia conflict, Titan Rainde.[20]

Anti-Terrorism legislation International Scenario

1. USA: After September 11, 2001 attack on Twin Towers of USA. The Patriot Act 2001 was enacted by the congress empowering federal officers to intercept communications both for law

[18] Electronic Evidence by FABIO GIACOMINI & MOHD. HASANZAIDI Pg. 423-424.
[19] Criminal Department Review Jan, 2008, Pg. 21.
[20] FABIOGIACOMINI & MOHD. HASAN ZAID, Electronic Evidence, 2012, Pg 193-494.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

enforcement and for foreign intelligence gathering. It also tries to combat corruption in US Financial institutions and for foreign money laundering. The Act also contains provisions for preventing alien terrorist especially from Canada entering United States and enables authorities to detain and deport them. New federal crimes, such biological weapons offences, harbouring terrorists affording material support to terrorist, misconduct associated with money laundering etc. have also been created. Further, for these offences, new Penalties have also been provided.[21]

2. Europe

Council of Europe convention on Cyber crime, 2001.

Council of Europe convention for protection of individuals with regard to automatic processing of personal data, 1981.

Council of Europe problems of criminal procedural law relating to information technology.

Council of Europe Additional protocol of the convention on cyber crime,
concerning the criminalisation of Äcts of a racist and xenophobic nature committed
through computer system 2002.[22]

In result the Internet had left almost every law in the statute book utterly toothless and ineffective as far as India is concerned e.g. The laws against obscenity and Pornography are unenforceable on the internet as in the Indian Penal Code. The ease of business transactions is also copled with a massive scope for fraud and cheating in the absence of clearly defined laws and a mechanism for dealing with offences, There were vitally no cheat in the statute book to deal with cyber and even assuming that the existing legislations where interapted in a manner as to adjust to the change in technology the law enforcement machinery would be utterly incapable of enforcing them.

The passage of the Information Technology Act 2000 is therefore an event of for reaching. Proportions and union government deserve, special and unqualified Praise, The Act recognize the release of computer viruses unauthorised access to secured computer system, stealing of confidential information from computer as criminal offences and also creates a fine limit of a whopping one croge papees.

Section 66 of the act makes the publication of absence material an offence punishable with

[21] Field Guidance on New Authorities (Redacted, 2001; American Civil Liberties Union vs National Security Agency, Case No. 01-2090/2 40 (US COurt of Appeals) (Decided on O' nuby, 2007).
[22] FABIOGIACOMINI& MOHD, FLASAN ZAIDA, Electronic Evidence, 2012, Pg. 503.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

imprisonment up to two years and a fine of upto Rs. One Lakh on a subsequent conviction, a term of 10 years imprisonment and fine upto Rs. 1 Lakh.

The Act also contains elaborate provisions for other offences such as disobedience of the controllers discretions, breaking into notified protected computer system of Network, misrepresentation, Breach of confidentiality false Publication of digital signatures, Publication for fraudulent purpose.[23]

The question of cyber jurisdiction in criminal case come to the forefront of attention in early 1996 in U.S. Vs. Thomas. When the sixth circuit upheld the highly, publicized conviction of a couple operating a pornographic bulletin board from their home. [24]

The time has clearly come for embarking on preventive measures in the field of computer /data security. Appropriate guidelines and legislations enactments have to put in place on a war footing. The IT Act 2000 has amended the following legislations, in order to meet the challenges posed by computer crime.

- The Indian Evidence Act, 1872
- The Indian Penal Code, 1860.
- Banker's Book Evidence Act, 1891.[25]

How to combat and check Cyber Crime

It is not easy and possible to eliminate cyber crime once for all in view of latest scientific department. However, it is quite possible to combat and check the cyber crime. To achieve that object, the first and for most requirement is the awareness among the public about the cyber crime and the precautions to prevent the same. A netizen should keep in mind the following things:

1. To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and update anti-viru software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination.

[23] The Information Technology Act 2000: By: Abhijit Sen. Advocate 205, Pg. 215-217.
[24] US Vs. Thomas, 74 F.Zd. 701, 6th Cir, 1996.
[25] Rodney D. Ryder, 2 Ed. 2003, The Indian Cyber Law, pg. 90.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

5. Never send your eredit card number to any site hat is no secured (o guard apainst frauds.

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

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

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

9. Use of firewalls may be beneficial.

10 Web servers running Public sites must be physically separate protected from internal corporate network [26]

In India to tackle cyber crime Police have taken the initiatives to keep on electronic eye on the users of the various cyber cafes spread over the city The Kerala State IT mission has launched a web portal and call center to tackle cyber crime.[27]

The (CBI) Central Bureau of Investigation and Mumbai Police have recommended issuance of Licenses to Cyber Cafe Owners.[28]

Guidelines for Cyber Cafe under Information Technology Rules, 2000 Rules 2011.

1. Agency for registration of cyber cafe.
2. Identification of users.
3. Log Register
4. Management of Physical Layout and Computer resource.
5. Inspection of cyber cafe by an officer.[29]

Short Commings

1. Over Mechanism does not show any seriousness in handling juvenile Criminals.

2. A misapplication of the law to specify hacking technique could allow a hacker to walk free due to lack of specific technical framing.

3 A unique features of hightech and computer related crimes is that often require immediate action to

[26] Elecironic Evidence by: FABIO GIACOMINI «& MOHD. HASAN ZAIDI.
[27] The Hindu Business line Tuesday, July 21, 2007.
[28] The Hindu Business Line Aug. 23, 2007.
[29] Vide Note No. CSR 315 (E) dated lindprit, 2011 Published in Gazette of India (Extra), Part ll Section 3 (I) dated 13" April, 2011.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

locate and identify criminals lack of information is due to the tact that there is no longer a revenue related to recording transmission information for individual connection because experts must receive regular and frequent framing in the investigation and prosecution of high tech cases.

4. The Indian criminal justice system not exactly technosavey.

5. Sophisticated nature of cyber crimes that lack of knowledge on the part of the investigating agency make it difficult for the proper detection and investigation of cyber crime.

Suggestion

1. Specific law's should be incorporated in the IT Act to make rendering of justice more gentle as far as Juveniles are concerned.

2. Successful criminal prosecution and litigation require that the legal community familiar themselves with the various hacking techniques to ensure that the perpetrators are tried and convicted under the relevant statutes.

3. In the internet era, cyber law awareness is essential to a Netizen with thriving opportunities in e-commerce throughout the world.

4. Considering the potential of net transactions world wide and also an account for the information revolution in India, cyber law shall not be allowed to bypass India. In this context the legal regime has to play its independent and legitimate role.

5. India should continue to work with countries, international groups to develop comprehensive and global plans for addressing the complex and challenging legal and policy issue surrounding jurisdiction raised by unlawful conduct on the internet.

Conclusion

No doubt IT Act 2000 being used against new age criminals. Indian legal system is equipped how all these offences and contraventions to be detected and investigated. The Indian criminal justice system and exactly technosavey and training of personal is essential to achieve and secure electronic environment. In this crimes examined so for there is the Problem of jurisdiction.

The Nature of Internet is such that Geographical and political boundaries are tendered irrelevant a person with access to computer and the Internet might be attempting or planning a criminal act anywhere in the world. The internet is analogous to the high seas. No one owns it yet people of all nationalities use it.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 04, Issue 01
DOI: 10.46523/jarssc.04.01.07
Multidisciplinary, Open Access

This makes the control of cyber crime an international issue to being cyber crime under international crimes similar to offences such as piracy under the law of the sea which may be tried in any country However the formation of international model law of cyber crime could be one of the practical approach steps have been underway among the countriesto have a set of a global standards for cyber crime. The success of this could go a long way in controlling cyber criminals from all over the world.

Received: 08.04.2021 **Accepted:** 27.04.2021 **Published**: 28.04.2021