ISSN NO. 2456-3129

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

Indescribable Examination of Virtual Crime

Navneet Gupta[1], Bala Buksh[2]

Research Scholar, Career Point University, Rajasthan[1]
Career Point University, Rajasthan[2]
Email: mail2navneetgupta@gmail.com[1], balabuksh@gmail.com[2]

Abstract- The review of literatures that provide a bird's eye view of the research conducted in the field of virtual crime and virtual terrorism. It also explain the statement of the problem, hypothesis formulated for the purpose as well the objectives of the study and methodology adopted to conduct the research work and deals with conceptual analysis of virtual crime. In this chapter history and evolution of virtual crime has been discussed in detail. Categories of sub crime and their sub categories also explained with the help of case laws.

Keywords- virtual crime, virtual terrorism, bird's eye, scientific research, internet

1. INTRODUCTION

Presently in India as well as in the world the computers have become an integral part of the fast developing society. The computers are being used in various aspects such as in Banking, Manufacturing, health care, defense, insurance, scientific research, strategic policy making, law enforcement etc' If we think presently about the society without the computer everything seems to be impossible for example Railway Ticketing system. Airline ticketing as well as traffic control. Electricity bill, Telephone Bill office works etc, all are seems to be impossible without the computer. Computers with the aid of the Internet have today become the most dominant medium of communication, information, commerce and entertainment. The internet is like life in the real world being extended and carried on in another medium that cuts across boundaries space, time, nationality, citizenship, jurisdiction, sex, sexual orientation and age. Every coin has two side likewise, internet having all benefits of anonymity, a liability, and convenience has become as appropriate place for pensions interested in making are of the net for illegal gainful purpose, either monetary or otherwise. Internet has transformed the world into a Global Information Village. Internet has also made this world a virtual sleeper's global market place. History is a witness to the most fact that all the technological inventions have been put to as much destructive use as constructive one. Innovation technologies are no different, while good people are using Information technology for finding better alternatives which can improve the quality of human life while bad elements are using it for harming individuals, cheating others of their hard earned money, subverting and defrauding the business and to hide their crimes.

2. HISTORY AND DEVELOPMENT OF INTERNET

Internet has transformed the world into a Global Information Village. Internet made this world a virtual sleepless global market place. Internet is a global network of computer."Internet and online services, sometimes called as "new media" services as in many respects similar to the traditional media as it also includes production oriented material such as music, audio, video, graphics, text and games. It works in communication from is also likewise messaging, chatting, video conferencing etc. The internet's roots can be traced from 1950's. In 1957 the Soviet Union launched tile first Satellite, Sputnik I, triggering US president Dwight Eisenhower to creating the ARPA agency to arms race. So, the evolution of internet can be said to be started with the use of ARPANET sponsored by US military, which was set up in 1969. The first communication touch place between research Center at the University of California at Los Angles and the Stanford research Institute. The ARPANET was as joint venture of Massachusetts Institute of Technology and the American Department of Defense Advance Research Project Administration as a source to establish continued communication between remote computer resources in the event of war. The communication links were confined to military, defense contractors and university laboratories involved in defense related research. In early 1970's further innovations took place, such as electronic mail possibilities have grown. During this period other network equivalent to ARPANET being established such as the United Kingdom's Joint Academic Network (JANET) and the United States National Science foundation Network (NSENET). In the year 1990 the US authorities released ARPANET and transferred it to National Science Foundation (NSFNET). In the year 1993 Time Bemers-Lec's he is the person who developed the World Wide Web (www) in the European Laboratory for particle physics (CERN). The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet explorer the preceding year. So, there browsers made Internet access possible from personal computers. From the year mid 1990's

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

various commercial Internet Services Providers (ISP) entered the market and offered the Internet connection through conventional telephone line. On 24 October, 1955 Federal Networking Council (NFNC) unanimously passed a resolution defining the term Internet. This definition was developed in consolation with members of the Internet and Intellectual property Rights communities. The term internet defined as: "Internet" refers to the global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extension or follow-ons (ii) is able to support communications using the transmission control protocol/internet protocol (TCP/IP) suit or its subsequent extensions/follow ons, and or other IP compatible protocols and (iii) provides, uses or makes accessible either publicly or privately, high level ser\"ice layered on the communications and related infrastructure described herein.

3. EVOLUTION NATURE AND SCOPE OF VIRTUAL CRIME

Virtual crime is the deadliest epidemic confronting our planet in this millennium. At present when everything from microwave ovens and refrigerators to nuclear power plants are being run or computers virtual crime has assumed rather sister implication.^ It has raised its head as multi headed hydra. Where if one is being cut other and newer kinds of crimes are appear or develop suddenly virtual crime can involve criminal activities that are traditional in nature, such as theft, fraud forgery, defamation and mischief. The above of computer has also providing an scope of new age crime such as hacking, web defacement virtual stalking, web jading etc. Virtual crime is a twentieth century foetus of technological development, now which grown up like as epidemic and has become uncontrollable in the twenty-first century.'° The first virtual crime took place in the year 1820. Joseph-Marie Jacquai'd, a textile unmanufactured in France produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquardi employed that their traditional employment and livelihood were being threatened. They committed the acts of sabotage to discharge Jacquard from further use of the new technology. So, this is the first recorded virtual crime. Broadly speaking, the virtual crimes refer to all activities done with criminal intent in virtual space. They can be divided into three categories:

3.1. Virtual Crime against person

The first category of virtual crimes committed against person include various like transmission of child-pornography, sexual harassment of any one with the use of a computer, such and e-mail and virtual stalking. Any unwanted contact between two people that directly or indirectly communicates a thi'eat or place the victim in fear can be considered stalking. The Trafficking, distribution, posfing and dissemination of absence material including pornography, indecent exposure and child pornography constitutes one of the most important virtual crimes know today. The potential harm of such a crime to humanity can hardly be over stated

3.2. Virtual Crime against property

The second category of virtual crime is that of virtual crimes against all types of property. These crimes includes Hacking is unauthorized use of computer and network resources and cracking some breaks into someone else computer system often on a network or intentionally breaches computer security, Vims is a computer programme that can reproduce itself and causing destruction of data contamination, copy-right protects creative or artistic works. You should only copy or copyrighted work with the copyright owner's peraiission infringement, potent is a set of exclusive rights granted by a state to an inventor or his assign for a fixed period of time in exchange for a disclosure of an invention. Infringement, impersonation or virtual fraud, virtual squatting is registering, trafficking in or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else etc. In these Hacking and cracking are among the gravest virtual crimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent has tampered with precious confidential data and information. Coupled with this, the reality is that no computer system in the world is hacking proof. So, it is unanimously agreed that any and every system in the world can be hacked.

3.3. Virtual Crime against Government.

Virtual terrorism could be defined as the premeditated. Politically attack against information system, computer programs, and data to deny service or acquire information with the intent to disrupt the political, social or physical infrastructure of a target resulting in violence against public.

3.4. Virtual Crime and Organized Crime

The internet revolution has transformed the society in general and the commercial world in particular. While commercial dealing is rampant on the internet due to its reach worldwide in low cost. So organized crime also found the new opportunities and benefits on internet that are very useful for furthering the criminal activities organized criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in virtual space. Some traditional criminal groups are seeking the co-operation of criminals with the necessary technical

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

skills; newer types of criminal networks operating in the area of e-crime have already emerged. Criminal organizations are constantly on the lookout for new opportunities as well as new ways of keeping themselves safe and away from the law enforcing authorities. Internet offers a number of services for the common man and criminals could abuse many of those services to their advantage. Internet is most in expansible and realizable Id. These attributes attract the criminals as well as also help them in speeding up their activities. The structure of this criminal organization is different from traditional organized crime organization. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centered on online meetings. These networks are structured on "Stand alone" basis, as members rarely meet each other is person and sometimes do not even have a virtual contact with other colleagues

3.5. Virtual Crime and Legislation of Nations

To meet the challenges posed by new kinds of crime made possible by computer technology including telecommunication, many of the countries largely industrialized and some of those which are moving towards industrialization have in part few years reviews their respective domestic criminal laws from the point of adaptation, further development and supplementation so as to prevent computer related crime. A number of countries have already introduced more or less extensive amendments by adding new statutes in their substantive criminal law.

4. VIRTUAL CRIMES OTHER THAN THOSE MENTIONED UNDER THE IT ACT

4.1. Virtual Stalking

Although there is no universally accepted definition of virtual Stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the virtual criminal towards the victim by using Internet services. Stalking in General terais can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical hamis to the victim. It all depends on the course of conduct of the stalker.

4.2. Virtual squatting

Virtual squatting is the obtaining of a domain name in order to seek payment irom the owner of the trademark, (including business name, trade name, or brand name), and may include type squatting (where one letter is different).
A trademark owner can prevail in a virtual squatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiffs distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of –pocket expenses.

4.3. Virtual Defamation

Any derogatory statement, which is designed to injure a person's business or reputation, constitutes virtual defamation. Defamation can be accomplished as libel or slander. Virtual defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

4.4. Virus/worm attack

Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

4.5. Salami attack

This is basically related to finance and therefore the main victims of this crime are the financial institutions. This attack has a unique quality that the alteration is so insignificant that in a single case it would go completely uniotiсed. E.g. a bank employee inserts a programme whereby a meager sum of Rs 3 is deducted from customers account. Such a small amount will not be noticeable at all.

4.6. Virtual terrorists

There are many forms of virtual terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of likeminded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent. Earlier when IT Act enacted in

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

2000 the punishment was silent but after amendment in 2008 the punishment has been prescribed.
The following is a table in brief showing the various offences under the Information Technology Act, 2000 together with their respective punishments:

5. Challenges posed by virtual crime

As the virtual law is growing, so are the new forms and manifestations of virtual crimes. Russia, China and Brazil are world leaders in virtual crime and India is fast emerging as a major hub of virtual crime in spite of enacting IT Act, 2000 to regulate and control virtual crimes. This situation raises apprehensions and concerns about the efficacy of our virtual law in dealing with virtual crimes. It can't be disputed that Information Technology Act, 2000 though provides certain kinds of protections but doesn't cover all the spheres of the I.T where the protection must be provided. The offences 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 virtual offences possible and existing.

Table1: various offences under the Information Technology

S. No.	Offence	Punishment	After amendment
1.	Tampering with computer source document	Imprisonment up to 3 years, Fine up to 2 lakh rupees.	
2.	Hacking with computer system	- DO –	
3.	Failure to comply with direction of the controller	- DO -	
4.	Breach of confidentiality or privacy	Imprisonment up to 2 years, Fine up to one lakh rupees.	
5.	Publishing false digital certificate	- DO –	
6.	Publishing digital certificate for fraudulent purposes	- DO -	
7.	Misrepresentation or suppression of material facts	- DO -	
8.	Failure to assist to decrypt information	Imprisonment up to 7 years	
9.	Securing access to protected systems	Imprisonment up to 10 years and fine	
10.	Publishing information which is obscene	1st conviction – imprisonment up to 5 years and fine up to one lakh rupees. 2nd conviction – imprisonment up to 10 years and fine up to two lakh rupees.	1st conviction – imprisonment up to 3 years and fine up to five lakh rupees. 2nd or subsequent conviction – imprisonment up to 05 years and fine up to ten lakh rupees.

6. Conclusion

Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided. The truth is that the criminals have changed their methods and have started relying on the advanced technology, and in order to deal with them the society, the legal, and the law enforcement authorities, the private corporations and organizations will also have to change their mechanism to combat it. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardware's and software so that they can efficiently fight the virtual criminals. Thus, necessary facilities must be established in various parts of the country so that crime in the virtual world can be controlled'. Another aspect which needs to be highlighted is that a culture of continuous virtual education and learning needs to be inculcated amongst the legal and the law enforcement authorities because the Information Technology field is very dynamic as the knowledge of today becomes obsolete in a very short time. Lastly the preamble of the Information Technology Act, 2000 provides that the Act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce, further the Act has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserx'e Bank of India Act, 1934 for facilitating legal recognition and regulation of the commercial activities. Though this objective of the Act is not to suppress the criminal activity, but this act has defined certain offences and penalties to overpower such omissions, which is understood to come within the characterization of virtual crimes. From this, it can be inferred that the law cannot afford to be static; it has to be change with the changing times and viz. virtual space. This is all the more required, that many applications of the technology can be used for the battement of the mankind, similarly it equally true that such application can also be used for the detriment of the mankind as has been demonstrated by the Spy-cam case. The bottom-line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development.

7. References

[1] Anant D. Chinchure, 'Global Response to Secure Virtualspace: A Comparative Analysis of National Strategy of USA and India.' Karnataka Law Journal. Vol. 5, 2010.
[2] Anant D. Chinchure, 'Virtual (Computer) Crimes- A Conceptual Analysis.' Criminal Law Journal. Nov. 2010. Amn Kumar Gupta, 'Virtual Crime and Jurisdictional problem.' CBI Bulletin. June-December 2006..

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 3, No. 1, March- 2018

[3] Benjamin R. Jones, 'Comment virtual Neighbourhood watch: open source software & community policing against Virtual crime.' The Journal of Criminal Law & Criminology. Vol.97, No. 2, winter 2007. 'Virtual crime in India.' Criminal Law Journal. June 2007.
[4] Dawson Cherie, 'Creating Borders on the Internet- Free Speech, the United States and International Jurisdiction." Virginia Journal of International Law. Vol. 44, No-2 (Winter, 2004). Delvin Jacob Mathews, 'Virtual Crimes Ahead.' Kerala Law Times. Vol. 3, 2002.
[5] Dr Anita Verma, 'Virtual Pornography.' Army Institute of Law Journal Vol.-1,2007. Dr. G.I.S. Sandhu, 'Virtual Crimes and IT Act- Penology and Jurisdictional Issues.' Army Institute of Law. Vol. I, 2007.
[6] Dr. Gurbax Singh Karkara & Dr. S.K. Shanna, 'Law of Virtual Crime in India.' Journal of The Legal Studies. Vol. 29, 1998-1999.
[7] Dr. M. Ponnaian, 'Virtual Crimes, Modem Crimes and Human Rights.' The PRP Journal of Human Rights. July-Sept. 2000.
[8] Dr. Umsa Mohsin & Shashank Shekhar, 'Pornography at the Age of Electronic Revolution.' Criminal Law Journal. Sept. 2011..