Anurag Rawal et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue 4, Dec 2017, pp. 83-84

Cyber Crime: Nature and Types

Anurag Rawal

Master of Law, Kurukshetra university kurukshetra

Abstract: **Cyber space is fast emerging as an alternate way of living for the growing generation today. Civilization has seen the development of many technologies in the past but the emergence of cyberspace is the most revolutionary since it has enabled an explosion in social communications between ordinary people across geographical and political boundaries. William Gibson had used the term cyber space for the first time in 1984, in his novel named 'Neuromancer'. He had described cyber space as the 'virtual world of computers'. Now-a-days, cyberspace has become synonymous with the internet. Law cannot afford to remain oblivious of these developments and lose relevance. Law has to cope up with the new challenges and in the changing scenario, redefined the rule of individuals and groups. The situation demands that there should be a concerted effort on the part of the lawyers, judges and legislature to resolve the legal issues raised by the introduction of Information Technology. There is a genuine feeling that the new world of digits demands training not only to the Bench and Bar but also to the law enforcement agencies as new language has been introduced which has given new meaning to old words.**

Keywords: **Cybercrime, laws**

I. NATURE OF CYBER CRIME

Although we may get general consensus among criminal defense lawyers that cyber crime has been the most recent radical change in criminal behavior, it is unlikely we will receive the same consensus when it came to defining what cyber crime actually was. Nevertheless, broad consensus would most probably agree that cybercrime is a term of language used to describe "criminal activity that utilizes an element of a computer or computer network"[1].
Thus, essentially there are two separate and distinct elements to cyber crime. On the one hand we have an element of exploiting weaknesses in the computer operating system or computer network, On the other hand we have an element of exploiting social fabric of a computer network, whereby a criminal makes use of the computer network to infiltrate the trust of other users of that computer network for profit or gain. Although these different elements of what constitute cyber crime may not seem overly important, they do have an impact when we look at the evolution and development of cyber crime.

II. TYPES OF CYBER CRIME

Unauthorized access to computer system or networks means any person who secures access to attempts to secure access to protected system. It is complete when or secures access to any computer, computer system or computer network without permission of the owner or any other person who is in charge of such computer system or computer network. A person who engages in this activity is known as a compute hacker. A hacker may gain access remotely, using a computer in his own house or office connected to a telecommunication network. Computer means any electronic magnetically, optical or other high speed data processing device or system which performs logical, arithmetic and memory function by manipulations of electronic magnetic or optical impulses and all input, output processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer work.[2]

In the case of **DPP Vs/ Bignell**[3] a police officer obtain access of data held on the police national computer in order to identify the owner of a motor vehicle. The information was sought for the owner's personal interest and was connected with his duties as a police officer. The conduct was an offence under section 1 of computer misuses Act although it was not contended that the use for which the data was taken was unauthorized used by the Authorized user. The I.T. Act makes unauthorised access punishable regardless of intention and purpose. The complainant has to prove that the opposite accessed or secured access to a computer system or network without the permission of the owner or the in charge of such computer, computer system or computer network. He needs to prove that by such access he has suffered any loss. When a person access or secures access to a computer system, computer network with the permission of owner or its in charge but down loads copies or extracts any data, computer database or information from such computer, compute system or computer network including information or data held or stored in any removable storage medium, without the permission of owner or in charge network he shall be liable in play compensation not exceeding rupee one crore to person so offended.

---

1 http://home.indy.net/-Sabronet/secure/remote.html

2 Section 2 (1)

3 DPP V/s Bignell (1997) Time 6 June, 21 May, Independent (Loyed information technology law 1997 page 1991

© 2017 IJRRA All Rights Reserved

III. INTELLECTUAL PROPERTY CRIME:

Another major category of cyber crime consists of crimes against intellectual property crime. Hacking and cracking of the computer system internet and websites, secret codes, Trade names, domain names, etc. is done almost regularly by highly trained professionals in order to make unlawful economic gains at the expense of intellectual property rights or others. Inspite of technical protection system evolved no computer system can be completely immune from hacking and cracking. The highly complicated cyber technology tools have generated cyber crime of the new kind which go beyond the classical concept of trade marks and patents domain name may be the new electronic version of the traditional trade mark and the area of conflict. On internet the registration of Domain name is done on the first come, first served, basis without any direct government control. Mostly registration of domain names is done by the private organization without any territorial limits and without any prior check of earlier trade marks registered under Municipal laws of different countries. A company carrying on business of communication and providing services through the Internet carried a domain "Rediff". It was found that only object of adopting this domain name was to trade upon the reputation of the plaintiff domain name[4]. An injunction was ordered against the defendant in use of the said name. Just like in the case of **YAHOO INC V/s Ashok Arora and other**[5]**.** In this the defendant installed a website Yahoo India.com and provided similar services as those of the plaintiff. The plaintiff alleged passing off. The plaintiff was thus granted an interim injunction restraining the defendant from the domain name Yahoo.com. So the crime rate relating to intellectual property on the internet remains a gray area with the I.T.Act 2000 because the law is not addressing the issue on internet.

IV. VIRUS

If a person without permission of the owner or any person who is in charge of computer, computer system or computer network introduces causes to introduce any computer containment or computer virus into any 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 affected Computer contaminant means any set of computer instructions that are designed or to modify, destroy, record, transmit data or programme raiding within a computer, computer system or computer network or (2) by any means to disturb the normal operation of the computer, computer system or computer network[6]. Computer viruses means any computer instruction, information, data or Programme that destroys, damages or adversely affects the performance of a computer resource or attaches itself to another computer sources and operate when a programme, data or instruction is executed or some other event takes place in that computer resource[7]. Damage does not mean physical damages caused to a computer or computer system but means to destroy, alter, delete, add, modify or rearrange any computer resource by any means[8]. A Virus is a programme that infect a computer by inserting a copy of itself into the computer and harm the computer in same manner, generally without the computer users awareness. Not all viruses cause damages to its host virus that "benign" but not harmful are still consider viruses. For example a virus could display an innocuous message on a certain data.

V. CONCLUSION

Although it might be annoying and react a sense of anxiousness, the virus does not cause any measurable harm. The current antivirus and anti hacking statues do not distinguish between harmful and benign viruses. The IT envisages that damage may be caused to any computer, computer system or computer network by means other than malicious code and to prevent that the above provision has been made. Various types of computer viruses and computer contaminants are placed under a single head malicious code. The Primary object of writing a computer code is to charge damage to any computer resource or to run away with valuable information. There are different types of viruses and contaminants, some of them share similar techniques or objectives. These are however, important difference in various forms various types of malicious codes are discusses here.

4 AIR 2000 Bombay 27
5 1999 DTC (19) 201 Delhi
6 Explanation (i) to See 43
7 Explanation (ii) to See 43
8 Explanation (iii) to See 43

© 2017 IJRRA All Rights Reserved