Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages
17 March 2018
Peer Reviewed Refereed Research Journal

Cyber Crime and Cyber Terrorism

Dr. Vinod Patidar
Principal
Indore Institute of Law
Indore, Madhya Pradesh, India

Introduction

When Blaise Pascal built the first non-electronic computer in 1642, little did he know that centuries later the descendants of this innovation would change the way we live and would rewrite law lexicons. These electronic behemoths became a substitute for human brains. In 1969, the birth of the internet multiplied the power of this wonder machine and the world was never like before. New crimes appeared and old crimes disappeared, and what counts as a crime will vary across the societies. The creation of new crimes may be most evident in times of rapid social, political, economic, technological and cultural change and interaction has become possible, bringing with them challenges and threats to order and well being.

The rapid development of internet stands as an example of such change, just ten years ago it was in its infancy, yet it is now a fact of life for billions of people around the globe. It has brought in its wake significant changes in the ways we work, trade, study, learn, play, consume, communicate and interact. At the same time, a whole host of crime problems has emerged in tandem with life online. Politicians, police, businesspeople and citizens now have a new vocabulary with which to identify such dangers, hacking, spoofing, phishing. Viruses, Trojans, malware, piracy, downloading, spyware, chat room grooming, and so on. The internet has opened up a world of opportunities in e-commerce and information sharing, on the flip side the internet has its own threats and abuses which are perpetrated by a new breed of criminals known as cyber criminals. Just as you know that our world is unsafe and criminals lurk in dark alleys, in the cyber space too criminals lurk and the danger is all the more high with new and novel methods employed by cyber criminals. With the internet being touted as no one being in-charge and one can do whatever one wants, cyber criminals started having a field day with a range of crimes like cyber terrorism, cyber stalking, cyber warfare, invading your privacy, cyber pornography or obscenity etc. The world is indeed, undergoing a new information revolution today. It not only touches every aspect of life but also makes the way extensively to perform the industrial and economic function of the society. New communication system and digital technology have made dramatic changes in the way we live. A revolution has been occurred due to technological progress. Almost everybody is making substantial use of computers and the internet connections are becoming an essential part of our daily use. They are being used by individuals and societies to make their life easier. They use them for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and almost all aspects of life.

Computer crime or an e-crime

The computer crime or an e-crime can be simply defined as a crime where a computer is the target of a crime or it is the means adopted to commit a crime. While some of the crimes may be new, the others are simply different ways to commit conventional crimes such as frauds, theft, blackmailing, forgery, and embezzlement using the online medium often involving the use of internet. What accelerate the growth of such crimes are typical characteristics of cyber space inter alia anonymity, speed, access, dependency, borderless space and lack of awareness of laws. The information technology is a double edged sword, which can be used for destructive as well as constructive work. Thus, the fate of many ventures depends upon the benign or vice intentions, as the case may be, of the person dealing with and using die technology. For instance, a malicious intention forwarded in the form of hacking, data theft, virus attack, etc can bring only destructive results. These methods, however, may also be used for checking the authenticity, safety and security of one's technological device, which has been primarily relied upon and tested for providing the security to a particular organization. For instance, the creator of the 'Sassier worm' has been hired as a 'security software programmer' by a German firm, so that he can make firewalls, which will stop suspected files from entering computer systems. This exercise of hiring those persons who are responsible for causing havoc and nuisance is the recognition of the growing and inevitable need of 'self-protection', which is recognized in all the countries of the world. In fact, a society without protection in the form of 'self-help' cannot be visualized in the present electronic era. The content providers, all over the world, have favored proposed legislations in their respective countries, which allow them to disable copyright infringers. In some countries the software developers have vehemently supported the legislations which allows them to remotely disable the computer violating the terms and conditions of the license allowing the use of the software. This position has, however, given birth to a debate about the desirability, propriety and the legality of a law providing for a disabling effect to these 'malware'. The problem is further made complicate due to absence of a uniform law solving the 'jurisdictional problem'. The Internet recognizes no boundaries; hence the attacker or offender may belong to any part of the world, where the law of the offended country may not be effective. This has strengthened the need for a "techno-legal' solution rather than a pure legal recourse, which is not effective in the electronic era.' Almost everybody is making substantial use of computer. The giant companies, now small companies/firms also are investing millions of rupees in sophisticated information system. Railway, Banks, Judiciary etc. are the institutions which are computerized and there are many departments/institutions/ministries which are trying to achieve the goal of "fully computerized". In fact we are living in the "Information age" through automation and development in the field of communication.

Legal & Technological Measure's to Combat Cyber Crime

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet. The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represent the cyber crime as Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data. Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for governments because different domains are typically administered through respective ministries and departments. The task is made all the more difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators.

The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown a pace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and Stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by Politico-Military security actors at one end and economic-civil society actors at the other.

Need for an International Convention on Cyberspace

Cyber security is becoming an indispensable dimension of information security. The rapid growth of ICTs has contributed immensely to human welfare but has also created risks in cyberspace, which can destabilize international and national security. Global and national critical infrastructure is extremely vulnerable to threats emanating in cyberspace. Additionally, the growth of social media (Twitter, Face book, Orkut etc.) has created a new medium for strategic communication that bypasses national boundaries and national authorities. The global data transmission infrastructure also depends critically on the NW of undersea cables, which is highly vulnerable to accidents and motivated disruptions.

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's so that they can efficiently fight the cyber 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 cyber 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 Reserve 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 cyber 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. cyber 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. To understand cyber crime as a significantly new phenomenon, with potentially profoundly new consequences, it is necessary to recognize it as a constituent aspect of the wider political, social and economic reconstructing currently affecting countries worldwide. Free flow of uncensored information on electronic networks and web-sites is as attractive to insurgents and extremists groups as it is to dissidents proclaiming their human rights just as crimes have changed with the growth of information technology so have the categories of criminals who engage in such crime.

References

- *Srivastava, V.P, an Introduction to Cyber Crime Investigation. Delhi, Indian Publishers Distributers, 2003, p.2.*
- *Astt Narayan - LK Thakur,'Internet Marketing E-Commerce and Cyber Laws'Authors Press, Delhi, 2000.*
- *Bama, Yogesh,'Criminal Activities InCyberworld.'Dominent Pubhshers and Distributeis, New Delhi, 2005.*
- *Barua, Yogesh and P. Dayal Denzyl,'Cyber Crimes - Notorious Aspects of the Humans and the Net.'Dominent Publishers and Distributers, NewDelhi, 2001*
- *Dr. Gandhi; K.P.C,'Introduction to computer related crimes.'CBI Bulletin, Delhi.*
- *Dr. Ahmad Farroq,'Cyber Law in India (Law on Internet).'New Era Law Publications, Delhi, 2011*
- *Articles*
- *Anant D. Chinchure, 'Global Response to Secure Cyberspace: A Comparative Analysis of National Strategy of USA and India.'Karnataka LawJournal.Vol. 5, 2010.*
- *Anant D. Chinchure, 'Cyber (Computer) Crimes- A Conceptual Analysis.' Criminal Law Journal. Nov. 2010.*
- *Amn Kumar Gupta, 'Cyber Crime and Jurisdictional problem.' CBI Bulletin.*
- *June -December 2006.*