Legal Dimensions of Dreaded Cyber Terrorism in India

By Maneela Bansal
Research Scholar, Department of Law D.A.V. College, Muzaffarnagar C.C.S. University, Merrut INDIA

***Maneela Bansal** is a postgraduate Indian student at the Department of Law, D.A.V.College, Muzaffarnagar, of C.C.S. University, in Merrut, India,*

Maneela is the winner of the Computers and Law Journal 2009 Student Prize.

Introduction

We are witnessing varied cyber crimes such as internet fraud and financial crimes, online sale of illegal articles, online gambling, digital forgery, cyber defamation, cyber stalking, phishing, cyber conspiracy, cyber pornography, web defacement and cyber-terrorism. Among all these cyber crimes, cyber-terrorism has hit mankind with unbelievable severity. In the present article an attempt has been made to analyse the ambit of cyber-terrorism in India. Remedies are also mentioned in this article for tackling the grave issue of cyber-terrorism.

For a warrior, nothing is higher than a war against evil. The warrior confronted with such a war should be pleased. Arjuna, for it comes as an open gate to heaven. But if You do not participate in this battle against evil, you will incur sin, violating your Dharma and your honour.

BhagavadGita 2.31.

The traditional concepts and methods of terrorism have taken new dimensions which are more destructive and deadly in nature. Just as terrorism is a stigma in the real world, it is also a bane in cyber-space. The growth of the internet has shown that the medium of cyber-space is being used by individuals and groups alike to threaten the governments worldwide and to terrorise citizens.

Cyber-terrorism is the convergence of terrorism and cyber-space. Cyber-terrorism is generally understood to mean unlawful attacks and threats of attack against computer networks and the information stored therein when done to intimidate or coerce a government or its people in the furtherance of political or social objectives.[1] The Federal Bureau of Investigation in the United States has defined cyber-terrorism as:

"The unlawful use of force or violence against persons or **property** to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives through the exploitation of systems deployed by the target".[2]

It must be noted that the definition of **property** is not restricted to moveables or immoveables alone.

In *R K Dalmia v Delhi Administration* [1962] INSC 124; [1962] AIR 1821; 1963 SCR (1) 253 (5 April 1962), a decision concerning a misappropriation of funds held in a financial institution, the Supreme Court of India held that the word **"property"** is used in the Indian Penal Code[3] in a much wider sense than the expression "movable property".

There is no good reason to restrict the meaning of the word **"property"** to moveable property only, when it is used without any qualification. Whether an offence defined in any particular section of Indian Penal Code can be committed in respect of any particular kind of property, will depend not on the interpretation of the word **"property"** but on the fact whether that particular kind of **property** can be subject to the acts covered by that section.

Another definition of cyber-terrorism is that "[I]t is the premeditated, politically-motivated attack against information, computer systems, computer programmes, and the data which result in violence against non-combatant targets by sub-national groups or clandestine agents.[4]

Cyber-terrorism is the use of computers and information technology, particularly the internet, to cause harm or severe disruption with the aim of advancing the attacker's own political or religious goals. As the internet becomes more pervasive in all areas of human endeavour, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups[5] (i.e. members of an ethnic group or belief), communities and entire countries. The definition of "cyber-terrorism" cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature.

From the above definitions it can easily concluded that "cyber- terrorism" refers to two elements:

(i) Cyber Space; and

(ii) Terrorism.

This means that the term necessarily refers to any dangerous, damaging, and destructive activity that takes place in cyber-space. There have been reports of Osama Bin Laden and others hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other websites[6].

Major cases relating to cyber terrorism:

It has been rightly said that:

"Just as a modern thief can steal more with a computer than with a bag, tomorrow's terrorist may be able to cause more damage with a computer mouse than with a bullet or a bomb."

Case 1. The website of the Bhabha Atomic Research Centre (BARC) at Trombay was hacked in 1998. The hacker's gained access to the BARC's computer system and pulled out virtual data[7].

Case 2. In 2002, numerous prominent Indian web sites, notably that of the Cyber Crime Investigation Cell of Mumbai were defaced. Messages relating to the Kashmir issue were left on the home pages of these web sites[8].

Case 3. In the Purulia arms drop case, the main players used the internet extensively for international communication, planning and logistics.[9]

Case 4. In 2007, the two Indian doctors involved in the Glasgow airport attack used Computers for terrorists activities.

Case 5. Former Indian President, Dr. A.P.J. Abdul Kalam has expressed concern over the free availability of sensitive spatial pictures of nations on the internet. He pointed out that the internet could be utilised effectively for gathering information about the groupings of terrorists. According to him,Earth observation by "Google Earth" was a security risk to the nation. www.fas.org and "Google Earth" provide free availability of such high resolutions pictures[10].

On 26 November 2008, the Bombay bomb blasts militants examined the layout and landscape of the city using only images from "Google Earth".

Comparative scanning of the data:

Recently Federal Bureau of Investigation has warned the United States of cyber-attacks. It said that the destruction caused by such cyber-attacks can be compared to disastrous weapons causing mass destruction of life and property. The internet is used not only for spreading the message of Jihad but explaining new techniques of making bombs, recruiting new members for terrorist activities and raising funds for terrorist attacks. Arizona University's "Dark Web Project" claims that on the internet 500 million pages, 1 million pictures, 15 thousand videos and 300 forums related to terrorist activities and more than 30,000 terrorist members exist.

In India alone, every month 300 websites are hacked. The majority of hacked websites are that of government organisations, V.I.P.'s and celebrities. Recent data confirms this truth[11].

Hacking attacks on Indian websites

Year	*No. of websites attacked*
2005	4715
2006	5211
2007	5863
2008	4474

The data speaks for itself that the situation is becoming quite alarming and it requires timely measures to curb cyber-crimes at this juncture.

The latest case of hacking into computers is that of "Ghostnet"[12]. This was a vast electronic spying operation from China which infiltrated computers and stole documents from hundreds of government and private offices around the world, including those of the Indian embassy in the United States, the Dalai Lama's offices and Tibetan exile centres.

New forms and manifestations of cyber-terrorism are emerging every day. Therefore to control cyber-terrorism new legislative mechanisms are required. It is important that cyber-laws in India are legislated in such a manner as to provide for a sound legal and technical framework which, in turn, could help in the growth and success of the internet revolution in India.

The *Information Technology Act* 2000[13] completely missed any provisions regarding the prevention of cyber-terrorism but the latest (27 October 2009) *Information Technology (Amendment) Act* 2008[14] has put the provisions in right frame. The law has severely dealt with cyber terrorism (S/66F). The punishment for cyber-terrorism is imprisonment for life. Perhaps the provision can be considered as the silver lining of the *Information Technology (Amendment) Act* 2008.

The biggest challenge to the law is to keep pace with technology. The march of technology demands the enactment of new legislation both to regulate the technology and also to facilitate its growth. Giving birth to new technologies is the work of the inventors. Making use of those technologies for more advanced and drastic crimes is the craftwork of the criminals. Controlling such crimes is the result of the interplay of the functions of legislature, executive and judiciary. The old adage of 'an eye for an eye' would be equally applicable to cyber-terrorism. It should be 'technology for technology'. High technology crime must be prevented using high technology. If one is committing a crime by using technology, one will be blocked from doing so by employing technology.

The government has to be quick in responding to the challenges raised by the constantly changing technologies. The government must create a stimulus package which may work as a catalytic agent to check the internet for the safety of the citizens and to ensure the smooth working of government.

Law enactment and its implementation go together. Simply the government can enact the law by way of legislation but its implementation is the challenge.

Enactment of law is an essential part of law but its implementation also plays a significant role in dealing with issues like cyber-terrorism. Enactment of law and its implementation are two sides of the same coin, but each side has its own separate significance in the present scenario.

In future, to avoid disastrous crimes like the Bombay blasts (26 November 2008), the laws are required to be more stringent, so that the misuse of the internet (Google earth and satellite phones) may not be done in any way. The laws must be hardened as such, so that nobody dares to commit such heinous crime.

Conclusion

From the above discussion it can be concluded that cyber-terrorism can be curbed by suitable technology if it is supported by apt legislation. Popular public support and a vigilant judiciary to back this up are also required. To widen the thinking of the new generation and to increase cyber awareness in society at large, the government must encourage debates on the subject in IT colleges, newspapers and magazines. A "Think Tank" of cyber experts also needs to be developed. The publicity must be created to initiate research in this field by way of scholarships , rewards, certificates of merit and so on.

Nothing in this world is perfect. The persons who legislate the laws and by-laws are also not perfect. The laws therefore enacted by them can not be perfect. Indian cyber laws have emerged from the womb of globalisation. It is at the threshold of development. In due course through exposure to varied and complicated issues, it will grow to be a piece of its time legislation.

References

1. Rohas Nagpal (2002): “Defining Cyber Terrorism”. In *The ICFAI Journal of Cyber Law*, Vol.1, No.1 (November) 75 at p.77.
2. *ICFAI Journal of Cyber Law* (2002).
3. *Indian Penal Code* (1860).
4. Yogesh Barua & Denzyl P.Dayal (2001): *Cyber Crimes*, New Delhi: Dominant Publishers & Distributors, pg3.
5. See, *http://.wikipedia.org/wiki/cyber-terrorism.*
6. See, *http://www.crime-research.org/eng/library.*
7. Dr. V.D. Dudeja (2001): *Information Technology and Cyber Laws-A Mission with vision*, Common Wealth Publishers, at 202.
8. *Amar Ujala*, Oct31,2005, Regional Daily Newspaper.
9. Krishna Kumar (2001): *Cyber Laws Intellectual Property & E- Commerce*, Dominant Publishers & Distributors at 295.
10. *Business Line*, Oct15, 2007, National Daily Newspaper.
11. *Danik Jagran*, Jan23, 2009, Regional Daily Newspaper.
12. *The Times Of India*, March30, 2009, National Daily Newspaper.
13. *Taxmann's Information Technology Act, 2000*, New Delhi, Taxmann Allied Services.
14. *The Information Technology (Amendment) Act, (2008)*, Delhi, Universal Law Publishing Co. Pvt. Ltd.