CYBER TERRORISM IN INDIA: AN APPRAISAL

Written by ***Dr. Jharasri Paikaray***

Faculty of Law, P.G. Department of Law, Utkal University, Bhubaneswar, Odisha

ABSTRACT

Cyber Terrorism is a burning issue in the domestic as well as global arenas. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate-emails, attacks on sensitive computer networks etc. In this paper the author focused on modes of cyber terrorism, different methods of identifying this crime. The author stressed on legal frameworks against cyber terrorism and its accessibility all over the country. In this crime the terrorists easily access the information with the help of internet and possess information for political, religious, social and ideological objectives. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

Key words: *Terrorism, hacking, destroys, attack, sovereignty, integrity, cyber space.*

INTRODUCTION

Cyber terrorism denotes unlawful attacks and threats of attack against computers, networks and information stored therein to intimidate or coerce a government or its peoples for propagating hidden political or unlawful social and religious agendas. These attacks result in violence against persons or property or cause public unrest. For examples Plane crashes and severe losses. Terrorists are known to use internet to prepare the schemes, raise funds and spread cyber terrorism. Example- Razmi yourself who was a key person behind world trade Centre attack had details schemes to destroy U.S. airlines encrypted files in his laptop.[i]

"The premeditated, politically motivated attack against information, computer system, computer programs and data which result in violence against noncombatant targets by subnational groups or clandestine agents" - Mark M. Pollitt

CHARACTERISTICS

Generally speaking cyber terrorism has several distinct characteristics. These features help to better differentiate the time-line between a cyber-terror attack versus a cyber-attack or activities of a hacker. Cyber terrorism may display following codes:

- Attack is predefined and victims are specifically targeted.
- Attack has an objective to destroy or damage specific targets such as political, economic, energy, civil and military infrastructure.
- Attack may even target specific opposing religions groups information, infrastructures to insight religious rocket.
- The purpose of any attack is to create fear of the groups intentions and further their own political agenda or goals or gain fellowship by succeeding in their attacks.[ii]
- Destroy enemy's capabilities to further operate within their own arena.

MODES OF CYBER TERRORISM:

The terrorism commits the crime of cyber terrorism in any of the following ways:

- Hacking into the systems and database owned by the government of the target country and appropriating sensitive information of national importance.
- Destructing and destroying the entire database of the Government hosted on cyber space along with all backups by introducing a virus into the system.
- Temporarily causing disruptions to the network of the government of the target nation and distracting the top officials so that they can pursue other means of terrorism.[iii]
- Distributed denial of service attacks. The terrorists through this attack first infect the systems by introducing viruses and then take control over the systems. The systems are then accused by the terrorists from any location who manipulate the data and access the information.[iv]

CYBER TERRORISM – AN APPEALING CHOICE:

There are quite a few reasons for cyber terrorism becoming an appealing and attractive option for the terrorists. They are:

- It is economical than any other traditional terrorist method. They just need a personal computer and an outline connection to create all kind of these chooses.
- Cyber terrorism is anonymous to a very greater extent than normal terrorism. Here terrorists use some kind of nicknames or may log on to a website as an unspecified "guest user".[v]
- The multiplicity of targets. The Cyber terrorist could aim the computers and computer networks of governments, individuals, public utilities etc.
- This kind of terrorism does not need any kind of physical training, psychological investment and no risk of morality is faced by them etc.
- Next, as the I Love You virus should. Cyber terrorist has the potential to affect directly a large numbers of Pf than traditional terrorist methods.

IDENTIFYING CYBER TERRORISM

There are three different methods of attack are identified based on the effects of the weapons used. These methods are the following:

- A physical attack involves conventional weapons directed against a computer facility on its transmission lines.
- An electronic attack involves the use of electromagnetic energy as a weapons mere commonly as an EMP to overload Computer Circuit but also in a less violent form to insert a stream of malicious digital code directly into an enemy microwave radio transmission.[vi]
- A Computer Network attack. It usually involves malicious code used as a weapon is input enemy computers to exploit a weakness in software in the system configuration or in the corruption security practices of an organization on computer uses.

LEGISLATIVE FRAMEWORKS

1. Section 66F of the Information Technology Act defines Cyber Terrorism. This section has been introduced by way of amendment of the Act in the year 2008. This amendment was the outcome of the most leading 26/11 terror attack in India. This section also prescribes the punishment for those attack in India. This section also

prescribes the punishment for those who commit or conspire to commit cyber terrorism.

2. Section 69A of the IT Act also empowers the central government or any of its authorised employees to direct any agency of the government to block access by the public any information from a computer resource in the interest of sovereignty and integrity of the nation.
3. Section 70B of the IT Act, the CERT team is set up which provides immediate alerts of incidents challenging cyber security and also lists out the emergency measures for handling incidents threatening cyber security of the nation.
4. In Indian Penal Code, 1860 the term property used in these Act in connection with punishment for theft and such connected crimes has been extended to cover data too and includes within its ambit the crime of data theft. Therefore where material information in the form of data is stolen by the terrorism against the sovereignty and integrity of the nation, it will amount to a crime under the IPC.[vii]
5. Unlawful Activities Prevention Act, 1967 lays down punishment for terrorist activities. Though Cyber Terrorism does not fall under the definition of terrorism as contemplated under this Act. This Act also prescribes punishment for recruiting persons for terrorist activities and for organizing terrorist camps.
6. Cyber Security Policy, 2013. In 2013 India introduced the national level Cyber Security Policy. This policy lays down the broad the framework for upholding and protesting the cyber space security. The main aim of this policy is to create a broad umbrella of cyber security framework in the country.[viii]

THREAT TO INDIA

The sensational episodes of online warfare are high against the nation. But still one witness that mostly we are not prepared to counter the cyber terror attack by China and Pakistan against our great India.[ix] Recently shown when a Swadish "ethical hacker" blogged details of e-mail accounts and passwords of several Indian Government institutions including the Defence Research and Development Organization, the National Defence Academy etc. the matter assumes significance particularly because China has been steadily strengthening its ability to

wage electronic warfare alongside its rapid and (non-transparent) modernization of its military and armory.[x]

CONCLUSION

Now it's high time to take action. It is a fact that counter terrorists are duty bound to save property and lives. We all are increasingly connected, dependents and vulnerable. With combination of knowledge, responsibility and expertise a counter- cyber terrorism team can build an effective policy for preventing cyber terrorist incidents, managing threats and responding to Cyber Terrorist Acts. So now we agree the fact that the traditional concepts and methods of terrorism have taken new dimensions which are more deadly and destructive in nature. The law dealing with Cyber Terrorism is however not adequate to meet the precarious intentions of these cyber terrorists and requires a transformation in the light and context and requires a transformation of the latest developments all over the world. Thus a good combination of the latest security technology and a Law dealing with cyber terrorism is the need of the hours.

ENDNOTES

[i] Brickey, J. 2012 Defining cyber terrorism, capturing a broad range of activities in cyberspace. Combating Terrorism Centre at west point.5(8)
[ii] Centre of Excellence Defence Against Terrorism (2008) Responses to Cyber Terrorism. Amsterdan:IOS Press p.34
[iii] Wilson, C. Computer attack and Cyber terrorism: Vulnerabilities and policy issues for congress,2005
[iv] Worth, Robert (25 June 2016): "Terror on the Internet: The New Arena, The New Challenges: New york Times Book Review.21
[v] Sundaram, P.M.S. and Jaishankar, K. (2008). Cyber terrorism: Problems, perspectives and prescription. Crimes of the Internet, Pages 593-611
[vi] Foltz c.B.(2004).Cyber terrorism, computer crime and reality. Information Management & Computer Security, 12(2):154-166
[vii] https://www.shodhganga.inflibnet.ac.in
[viii] www.techopedia.com
[ix] https://www.reodynh.gov
[x] Iqbal, M.(2003). Defining Cyber terrorism, J.Marshall J. Computer & Info. L., 22: 397