@2022 International Council for Education Research and Training 2022, Vol. 01, Issue 01, 21-25

Cyber Terrorism and India's Security

Dr. Satish Kumar,

Assistant Professor, Defence Studies, Govt. College, Hisar, Haryana

ABSTRACT

Cyber-terrorisin is now treated in military and political circles as seriously as conventional attacks with bombs and tanks. Conflicts can now be virtual but with consequences that are real and destructive: malware and other computer viruses can be directed to shut down infrastructure such as power grids, hospitals, water networks, financial markets and air security. A growing worry liere is that terrorist groups are using social networking to seek information not just about hard targets, but human ones. Furthermore cyberspace allows groups to spread propaganda & particular knowledge in new and innovative ways. An operation can be done by anyone anywhere in the world, for it can be performed tlıousands of miles away from a target. If any incident in the cyber world can create terror, it may be called a Cyber Terrorism. The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information and communication technology terrorists frave acquired an expertise to produce the most deadly combination of Weapons and technology, which of not properly safeguard in Que course of time, will take its own toll. The daniage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as cyber terrorism. It is said that the terrorist is also getting equipped to utilize cyber space to carryout terrorist attacks. The possibility of such attacks in future cannot be denied. Cyber terrorism is a greater challenge for India's national security where, several security establishments, business firms and national assets become vulnerable targets. As the cybercriminals, cyber field is potentially exploited by the terrorist to carry out their operations. This article is an effort to analyse different aspects of Cyber Terrorism.

Keywords *: Cyber-terrorism, National Security, Cyber attack, Hacking, Worms, Virus*

@2022 International Council for Education Research and Training 2022, Vol. 01, Issue 01, 21-25

What is Cyber Terrorism?

The FBI defines cyber terrorism as a "premediated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non combatant targets by subnational groups or clandestine agents.1 A key word here is "violence", yet many discussions sweep all sorts of nonviolent online mischief into the 'terror' bin. Various reports lump together everything from Hacktivism to Wikileaks and credit card fraud. Activism refers to normal, nondisruptive use of the internet in support of an agenda or cause. Hacktivism refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a target's internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web sit-ins and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms. 2

The final category, cyber terrorism, refers to the convergence of cyberspace and terrorism. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. But cyber terrorism is not limited to paralyzing computer infrastructure. It has gone far beyond that. It is also the use of computers, Internet, and Information gateways to support the traditional forms of terrorism as we saw in the case of 'Shami witness'.

There is an old saying that death or loss of property are the side products of terrorism, the main purpose of such incidents is to create terror in people mind. If any incident in the cyber world can create terror, it may be called Cyber Terrorism.3 Cyber terrorism is limited to actions by individuals, independent groups, or organisations. Any form of cyber warfare conducted by governments and states would be regulated and punishable under international law.

Methods of Cyber Attack

Cyber terrorist prefer using the cyber attack methods because of many advantages for it:

1. It is a cheaper and minimal resources are required than traditional methods of terrorism.

2. The action is very difficult to be tracked.

3. They can hide their personalities and location.

@2022 International Council for Education Research and Training 2022, Vol. 01, Issue 01, 21-25

4. There are no physical barriers or check points to CIOSS.

5. They can do it remotely from anywhere in the globe.

6. They can use this method to attack a big number of goals and targets.

7. They can affect a large number of people.

8. Greater 'fear factor', cyber terrorism fits with the terrorist's goal of infusing fear into the lives of their enemies.4

Tools of Cyber Terrorism

Cyber terrorists use certain tools and methods to unleash this new age terrorism. These are:

- ★ **Hacking:** The most popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing tempest attack, password cracking and buffer outflow facilitates hacking.
- ★ **Trojan Horses:** Programmes which pretend to do one thing while actually they are meant for oozing something different, like the wooden Trojan Horse of the 1st Century BC.
- ★ **Viruses**: It is a computer programme, which infects other computer, programmes by modifying them. They spread very fast.
- ★ **Worms:** The term 'worm' in relation to computers is a self contained programme or a set of programmes that is able to spread functional copies of itself or its segments to other computer systems usually via network connections.
- ★ **E-Mail Related Crime:** Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.
- ★ **Denial of Service:** These attacks are aimed at denying authorized persons access to a computer or computer network.
- ★ **Cryptology:** Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption. 5

@2022 International Council for Education Research and Training 2022, Vol. 01, Issue 01, 21-25

Cyber Attacks on India

India has experienced, and continues to undergo, cyber attacks in a variety of forms. On June 7, 1998, for example, an anti-nuclear group "Milworm" reportedly hacked into the Bhaba Atomic Research Center (BARC) network to India's nuclear tests. In the same time period, Pakistani hacker groups, such as Death to India, Kill India, Dr. Nuker, and G-force Pakistan, openly circulated instructions for attacking Indian computers.6 According to a 2003 account in The Hindu, for more than two years the hacker war between India and Pakistan has been intensifying, leading to the defacement of hundreds of websites on either side. “Earlier this year, newspaper reports had indicated that an unnamed virus launched by a secretive Indian hacker grouphad rendered 200 Pakistani websites inaccessible for several days and erased the hard disks of scores of computer (sic] in the Pakistani Government as well as the private sector in that country."7 Cyber attacks consequently pose more than a theoretical challenge to the Indian government's dayto-day national security agenda. In response to these attacks, the leaders of India's armed forces have embraced the need for change and have begun to build partnerships with industry intended to transform the military into a technologyfocused force. In the late 1990's, India undertook a review of Defence posture in the framework of what strategists call the "Revolution in Military Affairs” (RMA) posed by the application of digital technologies to precision guided weapons, battlefield awareness, and instantaneous communications.7 In a 2001 report, Challenges to the Management of National Security, political leaders focused on addressing military and related threats below the nuclear threshold and highlighted cyber offense and Defence: The emergence of non-state terrorist actors and the rise of their international influence is accelerating. Much of their activity is clandestine and outside the accepted international norms... India is at the receiving end of these violent elements and is likely to remain a target of international terrorism in the future. Strategies need to be evolved to counter the threat of Weapons of Mass Destruction Terrorism (WMD) as well as cyber terrorism; the latter especially against infrastructural and econo ic assets such as banking, power, water, and transportation sectors.8

Intended transformation in India's strategic doctrine and military operational art complemented the sweeping changes in the information technology economy that began in the early 1990's. Toward the end of that decade, India's IT sector internationalized for example

@2022 International Council for Education Research and Training 2022, Vol. 01, Issue 01, 21-25

through the U.S. IT industry's joint investment ventures with offshore companies to develop software. Manufacturers in India were logical partners for U.S. companies because the sub-continent offered a supply of well-trained, low-cost labor.9

Conclusion

To conclude, we should be more vigilant about politically motivated cyber attacks and the misuse of technology for selfish gains. Only through international cooperation the menace of terrorism can be tackled effectively. It is high time that all the countries realize the importance of cyber space which if well protected can alone safeguard the interests of developed and developing economies. A common vision is surely needed to put an end to all cyber crimes and see eye to eye with one another. The first step in this direction would be to make the common man aware of the growing danger of cyber terrorism. However, the fact remains that without a general understanding of the problem and bringing all the nations on a common platform this challenge to mankind as a whole cannot be countered.

References:-

1. Peter W. Singer, 'The Cyber Terrorism Bogeyman', The Brookings Institution, November 2012, URL: http:// www.brookings.edu/research/articles/2012/11/ cyber-terror

2. Quoted in Rick Montgomery, "Enemy in Site-It's Time to Join the Cyberwar," Daily Telegraph (Australia), April 19, 1999, p. 19.

3.http://en.wikipedia.org/wiki/Cyberterrorism

4. Kapender Singh, Cyber Terrorism and National Security, p. 162

5. Hinsdustan Times, December 19, 2000.

6. G. Anand, "Indo-Pak Hacker War Comes Here Too," The Hindu, June 9, 2003

7. Kapender Singh, Cyber Terrorism and National Security, p. 162