Cyber Terrorism: A Threat In India

Ms. Charu Srivastava

Assistant Professor of Law, School of Law, University of Petroleum and Energy Studies, Dehradun

Abstract

With growing dependency on the cyber technology, cyber-crimes boomed in the 21st century whose consequences can be devastating in the future. More and more our infrastructure gets dependent upon the technology, it also becomes vulnerable. We all have witnessed numerous cyber-crimes such as internet fraud, cyber stalking, phishing, cyber pornography etc. Cyber terrorism is a cyber-crime which is understood as an attack on electronic communication networks.

Indeed, several extremist's groups and organizations such as Al-Qaeda, cyber- Jihadist are using cyberspace for terrorists' activities. This leads to another understanding of the term cyber terrorism where it is also used to describe the use of internet by terrorists to create terror or to spread their messages, propaganda etc or to threat government.

In the past there have been several such attacks, for instance recently several Banks have blocked their customers' ATM as a preventive measure against security breach. Internet has been used in several serious attacks, for example in the year 2007; the two Indian doctors involved in the Glasgow airport attack used Computers for terrorists' activities. Further one of the deadliest attacks on 26/11/2008; the Bombay blasts militants examined the landscape of city by using internet.

The author in this paper will analyse the definition and understanding of the term cyber terrorism and will examine the various tools and methods used for cyber terrorism and will highlight the cases where internet has been used for cyber terrorism in India. This will be followed by an analysis of the legislative measures taken by government to combat cyber terrorism and their effectiveness.

1. Definition of Cyber terrorism

Cyber terrorism is a new kind of terrorism which exploded with the advent of internet. Hence it is the most necessary question for the UN and other international organization to answer and define the term cyber terrorism since it is an international issue. There is a need to create a link between the term 'cyber' and 'terrorism' to give a better understanding of the term "cyber terrorism."

Most accepted definition of cyber terrorism is by UN which was adopted in The UN General Assembly Resolution 49/60 on December 9, 1994, titled "Measures to Eliminate International Terrorism,":

"Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them."

The Indian government uses definition which is same as one widely used by Western nations as well as the United Nations which is:

"Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons,

whereby the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat and violence-based communication processes between terrorist organisation, victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought." [116]

These definitions look at different aspects such as the people, the location, the targets, the tools, the purpose etc. However, there is no agreed-upon definition of terrorism which makes it difficult to take appropriate countermeasures. Now coming to the definition of cyber it means "the science of communications and automatic control systems in both machines and living things"

Drawing a connection between these two terms cyber terrorism would mean control of a computer programme by another which releases a chain reaction to spread terror or damage. Usually cyber terrorism is synonymously used as cyberwarfare, cyber espionage. For example cyber warfare is controlling A's country system which leads to disruption of an air/Water defense network, while other country B is bombing its nuclear facility.[117] Another example is when in the year 2012, a Trojan virus gathered critical information about government and other agencies in Middle East which is a case of cyber espionage. All all these instances are understood as cyber terrorism since we do not have a common definition of cyber terrorism.

Referring to the definitions of cyber terrorism, one of the widely accepted definitions of cyber terrorism is given under Denning's Testimony before the Special Oversight Panel on Terrorism (Denning, 2000), which is:

"Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[118]

Peter Flemming and Michael Stohi have identified two important components in their work entitled "Myths and Realities of Cyber terrorism"[119] Firstly, Computer technology is used for political propaganda, terrorism financial assistance, for influencing people to join their groups, for

[116] The FBI (Federal Bureau of Investigation) also came up with a definition for terrorism, "the unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (FBI, 2002) For more information See: Ministry of Personnel, Public Grievances & Pensions Department of Administrative Reforms and Public Grievances, Combating Terrorism Protecting By Righteousness. Second Administrative Reforms Commission, Eighth Report, June 2008.

[117] Available at http://arc.gov.in/8threport.pdf (Last seen 15/07/2018). As happened in Syria, where Syrian air defence network system was controlled, while Israel was bombing an alleged Syrian nuclear facility in September 2007.

[118] Sarah Gordon Senior & Richard Ford, Cyberterrorism? 'Elsevier Science Computers and Security Journal', Symantec Corporation Available at https://www.symantec.com/avcenter/reference/cyberterrorism.pdf (Last seen 15/07/2018).

[119] Peter Flemming and Michael Stohi, Myths and Realities of Cyber terrorism, Published in Countering Terrorism Through International Cooperation, Alex P. Schmid (ed.), ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program), Vienna, 2001, pp: 70-105. Available at https://pdfs.semanticscholar.org/46ff/81edf2fb60a34bed1fc0e9e99655b3a35bab.pdf (Last seen 20/07/2018).

coordination, information gathering etc., in essence for facilitating terrorism. Secondly, computer technology as a weapon which includes computer technology used for attacking public utilities such as transportation, commercial institutions, political or ethnic group, and security forces etc.

Further relating cyber terrorism to loss of life, there has been no instances of cyber terrorism which have caused catastrophic loss of life or destruction of infrastructure. The threat, however, remains real and may cause potential destruction in future.

Summarizing the definition, it can be said that, there is no uniform definition of cyber terrorism and it may vary from nation to nation however the basic attribute is that cyber terrorism is an activity to spread terror or an act or threat of violence with the help of information technology for political reasons.

2. Cases of Cyber terrorism

As we have concluded in the previous part that a consensual definition of cyber terrorism is not yet framed and it varies from country to country, however there have been several instances where information technology has been used majorly or minutely to create terror. Since cyber terrorism has various facets and dimensions it is difficult to define its boundaries.

For instance in Ahmadabad Blast case of 2008, unsecured WIFI Router of Kenneth Haywood's House at Navi Mumbai, Medical College at Vaghodiya, Baroda, Kamran Power Limited at Bombay were misused to send emails which were sent from email id alarbi_gujrat@yahoo.com.[120] Similarly in 26/11 attack several Terrorists accessed email from 10 IP addresses five from Pakistan, two USA, two Russia and one Kuwait.[121] Following the attack India adopted amendments to Information Technology Act, 2000 in December 2008. These amendments include provisions dealing with cyber terrorism. Pakistan also adopted similar legislation in the year 2007.

Other instances are where terrorists' organizations maintain their own websites to broadcast their messages or spread their propaganda and influence potential terrorists to join their groups. As per the newspaper reports before almost all the attacks terrorists group had send out e mails to various media organization to create terror or to threat such as in Jaipur (Rajasthan) bombings, Bangalore (Karnataka) serial blasts, Ahmedabad (Gujarat) serial blasts, Delhi serial blasts; the Pune German Bakery blasts and the Mumbai serial blasts of July 13, 2011.

As per a news report, CERT-In had sent warnings to banks regarding Trojans that steals information, credentials to alert them against cyber-attacks. Lately on October 7, 2016 it warned about 'expected targeted attacks from Pakistan", in the wake of India's counterstrike across the border after terrorist attacks in Jammu and Kashmir. After these surgical strikes, there was rise in the number of attacks on various Indian websites some reports say the numbers of such attacks are around 7,000 by Pakistani hackers. Experts have also opined that Indian system is not prepared to tackle cyber terrorism and lack the infrastructure for monitoring. They are also of the view that India needs to increase spending enough on cyber security if it wants to hold off cyber terrorism.[122]

Further at the India Conference on cyber security & Internet Governance in the month of September 2016, Gulshan Rai, the National Cyber Security Coordinator in the Prime Minister's

[120] Cyber Terrorism in India, available at http://www.lawyersclubindia.com/articles/Cyberterrorism-in-India-With-special-emphasis-on-Ahmadabad--2059.asp (Last seen 20/07/2018).

[121] `Terrorists accessed email from 10 IP addresses, 5 from Pak` http://zeenews.india.com/news/nation/terrorists-accessed-email-from-10-ip-addresses-5-from-pak_558521.html (Last seen 20/07/2018).

[122] Available at http://zeenews.india.com/business/news/finance/cyber-terrorists-targeting-indian-banks-like-never-before-time-to-be-on-high-alert_1942390.html (Last seen 25/07/2018).

Office (PMO) has said that 70 per cent of terrorists and terror groups across the globe are using various cyber medium tools to spread the evil of terrorism and further their goals. He added that 70-75 per cent of terrorists are using tools like voice over internet telecom, social media and even encryption to spread the menace of terrorism and further their goals.[123]

Comparing Indian system with other countries such Russia, China, North Korea, Iran, the United States and Israel all have robust and indigenous cyber warfare capabilities. However, under the Modi government, India has also started work on developing its own cyber capabilities. It has also been said by experts in Nasscom that in India by 2025 million job opportunities will be created.

3. Legislative regime of cyber terrorism in India

Awakened by the several terrorist attacks, the Government of India took strong steps to strengthen the cyber security, including prohibition of terrorist activities through cyber space by way of amending the existing Indian Information Technology Act, 2000. The information Technology Amendment Act 2008 was placed in the Parliament and was passed towards the end of 2008.

Some of the notable features of the amendment Act are as follows Inclusion of some additional cyber-crimes like cyber terrorism.

Sec 66F mentions that

(1) Whoever, -

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) Introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

[123] Available at http://www.ndtv.com/india-news/over-70-per-cent-terrorists-using-cyber-space-pmo-cyber-coordinator-1468511 (Last seen 25/07/2018).

Examining the definition, it can be said that the cyber terrorism is an act of hacking or computer contaminating which hinders the authorized person from accessing his computer system. It is an act which to gain or obtain unauthorized access to any information which is restricted information for the purpose of national security etc. these acts are done to threaten the security, sovereignty and integrity of India or to terrorize citizens of Indian. However, the usage of informational technology in the past by terrorists for attacks have been to communicate using unauthorized Wi-Fi of other organizations etc. and not as such to gain protected information.

The Information Technology Act, 2000 (amended in 2008) had taken efforts to secure protected systems, which is defined by Section 70 as follows: "The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system." Explanation further says that the "Critical Information Infrastructure" would mean that vital computer resource regarding national security, economy, public health and safety, which if destructed or damaged, shall have a "debilitating impact" on these issues.

Judiciary has also played an important role by adopting a rigorous approach towards cyber terrorism. However, the issue regarding jurisdiction is the first obstacle before invoking judicial powers. Since the internet is in virtual space not owned by anyone, there are no centralized rules or laws governing its use. The absence of geographical boundaries may make one act which legal in one country illegal in another. Since there is no uniform and harmonized law governing this aspect, the jurisdictional issue always remains the moot contention. However, there are few theories which are put forward by scholars:

- Objective territoriality: a country may claim jurisdiction when an activity takes place within the country.
- subjective territoriality: when an activity takes place outside a nation's borders but the primary effect of the action is within the nation's borders.
- a country may assert jurisdiction based on the nationality of either the actor or the victim,
- in exceptional circumstances, providing the right to protect the nation's sovereignty when faced with threats recognized as particularly serious in the international community.[124]

Traditional international doctrine provides for a reasonable connection between the offender and the forum. Courts looks for whether the activity of an individual has a substantial and foreseeable effect on the territory, whether there is a link between actor and forum the character of the activity and the importance of the regulation giving rise to the controversy.[125] It must be noted that by virtue of section 1(2) read with section 75 of the Information Technology Act, 2000 the courts in India have "long arm jurisdiction" to deal with cyber terrorism.[126]

4. Conclusion

The problem of cyber terrorism is multilateral having several dimensions. It requires a cooperative approach from all the nations since it is not just an act towards a victim nation but towards the humanity. It is a human rights issue since it violates a human being's inherent right to live. Its solutions require rigorous application of energy and infrastructure. Law cannot change

[124] Praveen Dalal, Cyber terrorism and its solutions: An Indian perspective, available at http://www.naavi.org/cl_editorial_04/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm (Last seen 25/07/2018).

[125] Dawson Cherie; "Creating Borders on the Internet- Free Speech, the United States and International Jurisdiction", Virginia Journal of International Law, V-44, No-2 (Winter, 2004).

[126] Supra Note 9.

with the advancement of technology since technology is an idea which is the most powerful weapon if implemented so it becomes important to keep law updated with technology as much as possible. It is the need of the hour to take precautions and build our technology to tackle cyber terrorism.

References

1. Available at http://arc.gov.in/8threport.pdf (Last seen 15/07/2018).
2. As happened in Syria, where Syrian air defence network system was controlled, while Israel was bombing an alleged Syrian nuclear facility in September 2007.
3. Sarah Gordon Senior & Richard Ford, Cyberterrorism? 'Elsevier Science Computers and Security Journal', Symantec Corporation.
4. Available at https://www.symantec.com/avcenter/reference/cyberterrorism.pdf (Last seen 15/07/2018)
5. Peter Flemming and Michael Stohi, Myths and Realities of Cyber terrorism, Published in Countering Terrorism Through International Cooperation, Alex P. Schmid (ed.), ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program), Vienna, 2001, pp: 70-105.
6. https://pdfs.semanticscholar.org/46ff/81edf2fb60a34bed1fc0e9e99655b3a35bab.pdf (Last seen 20/07/2018).
7. Cyber Terrorism in India, available at http://www.lawyersclubindia.com/articles/Cyberterrorism-in-India-With-special-emphasis-on-Ahmadabad--2059.asp (Last seen 20/07/2018).
8. `Terrorists accessed email from 10 IP addresses, 5 from Pak` http://zeenews.india.com/news/nation/terrorists-accessed-email-from-10-ip-addresses-5-from-pak_558521.html (Last seen 20/07/2018).
9. http://zeenews.india.com/business/news/finance/cyber-terrorists-targeting-indian-banks-like-never-before-time-to-be-on-high-alert_1942390.html (Last seen 25/07/2018)
10. http://www.ndtv.com/india-news/over-70-per-cent-terrorists-using-cyber-space-pmo-cyber-coordinator-1468511 (Last seen 25/07/2018).
11. Praveen Dalal, Cyber terrorism and its solutions: An Indian perspective, available at http://www.naavi.org/cl_editorial_04/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm (Last seen 25/07/2018).
12. Dawson Cherie; "Creating Borders on the Internet- Free Speech, the United States and International Jurisdiction", Virginia Journal of International Law, V-44, No-2 (Winter, 2004).