Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Cyberterrorism: An Analysis

Anant Chhabra[a]

[a]Symbiosis International University, Pune, India

Received 17 August 2022; *Accepted* 05 September 2022; *Published* 12 September 2022

Cyberspace is an astounding place, but as everything comes with some disadvantages, this is no exception. Cyberterrorism is one of the cons of cyberspace which came to life only with the advent of cyber technology. Cyberterrorism combines the physical and virtual worlds, which may turn out to be disastrous at the least. In this research article, the author discusses Cyberterrorism, how it is done, and the primary objectives with which it takes place around the world. Although there are various national and international laws to prevent cyberterrorism, they are not enough to control it. The world at large and India need new laws related to cyberterrorism as the existing ones are unable to keep in check cyberterrorism. The author also tries to show how cyberterrorism takes place by highlighting various incidents which can be termed cyberterrorism around the world. The main objective behind this Article is to spread information about cyberterrorism so that more people know about this devastating thing and can be aware of it because that is the only thing that can prevent cyberterrorism.

Keywords: *cyberterrorism, cyberspace, cyber laws, technology.*

INTRODUCTION

In this era, the attacks on mankind are already increasing, and in this era of tech, Cyberterrorism has become a major concern. Cyberterrorism is defined as a kind of attack which is politically motivated and pre-planned. These attacks are conducted by way of using computer technology to engage in terrorism. These types of attacks are against data systems of the world by disrupting

them or destroying them completely, and the main motive behind these kinds of attacks is creating violence.

WHAT IS CYBERTERRORISM

Cyberterrorism can be termed as, "The convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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.[1] Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.[2] Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be termed acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[3]

According to Section 66F of the Information Technology Act, 2000,[4] "Anyone who attempts to deny access to anyone with authorization to access a computer resource, or causes the denial of access to someone with authorization to access a computer resource, or exceeds authorised access, or introduces or causes to introduce any computer contaminant, with the intent to threaten the unity, integrity, security, or sovereignty of India or to terrorize the general public or any group of the general public; or knowingly or intentionally breaches or accesses a computer resource without authorization or goes beyond the scope of authorised access, and through this conduct obtains access to information, data,[5] or a computer database that is restricted for reasons of national security or international relations, or any restricted information, data, or computer database, with reasons to believe that such restricted information, data, or computer database so obtained may be used to cause or likely to cause, or

[1] G Wiemann, 'Cyberterrorism How Real Is the Threat?' (*US Institute of Peace*, December 2004) <https://www.usip.org/sites/default/files/sr119.pdf> accessed 08 August 2022
[2] *Ibid*
[3] *Ibid*
[4] Information Technology Act 2000, s 66F
[5] *Ibid*

to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism."[6]

Cyber terrorism is a modern type of terrorism as compared to traditional terrorism which includes violence in a physical form.[7] Moreover, it can also be said that it is a much cheaper means as compared to traditional terrorism as the terrorist will only require a computer and good internet connectivity. Technology is the backbone of most countries in the current era, and as a result, the developed countries pose a much higher risk from cyberterrorism as compared to less developed countries as they are highly dependent on tech and a cyberterrorist with good skills can easily be termed as a source of danger for such countries.[8] "The United Nations telecommunications agency warns that the next world war could well be in cyberspace."[9]

METHODS USED FOR CYBER TERRORISM

In this era of tech, there are various methods through which cyberterrorism can take place. Some of them are as follows –

1. The first comes to ATP (Advance Persistent Threats), these kinds of cyberterrorism are both analytical and precise. It is used to get access to a network system. The primary motive of these kinds of attacks is to steal information from the user by staying undetected for a period. The primary sectors which get attacked by this kind of cyberterrorism are the defense and finance sectors of the country.[10] This data is used by the terrorist to gain undue advantage of the situation of which the host is unaware.
2. Hacking can also be termed as a type of cyberterrorism.[11] Hacking is used to get into a network and steal the important information of the user or organization. The primary purpose behind hacking can be termed the same as behind ATP.

[6] 'Information Technology Act 2000' (*Info. Technology* Law, 7 October 2019) <https://www.itlaw.in/> accessed 08 August 2022
[7] *Ibid*
[8] 'Chapter II Cyber Crime and Its Classification' (*BBAU*) <https://www.bbau.ac.in/dept/Law/TM/1.pdf> accessed 08 August 2022
[9] *Ibid*
[10] *Ibid*
[11] Technology Law (n 6)

3. Worms, Malware, and computer viruses are also other forms of cyber-crimes that can be termed cyberterrorism. These are used to get whole control of the IT structure by using various means with the primary motivation being stealing data and using it for terrorist activities.[12] DoS is also a type of cyberterrorism, which stands for Denial of Service. In DoS, the attacker that is the cyberterrorist prevents the legitimate user of the network to get access to the system. As the legitimate user is unable to access his network system, he can do nothing to stop cyber terrorists.

OBJECTIVES OF CYBER TERRORISM

The primary motive behind any kind of act of cyber terrorists is the destruction of the subject material whether it is tangible or intangible, or to cause harm to life and property. Given this, it can be claimed that everything has benefits and drawbacks, and technology is not exempt. Although technology has many benefits, it also plays a vital part in giving cyberterrorists a chance to hack into the IT system and utilize data maliciously to inflict harm.

The first and primary objective of cyberterrorism is the same as traditional terrorism which is the destruction of life and property. This type of terrorism takes place by the way of computers and modern technology. Although there is no case yet of cyberterrorism at this time, it can be said that it is just a matter of time. As the world increasingly turns towards technology, more it is prone to these kinds of cyber-attacks.[13] The second objective of cyber terrorism can also be said as an organizational objective. By way of this recruiting, instigation training, fundraising, communication, planning, spying, etc take place. The primary requirement for cyberterrorism is the people who are knowledgeable about upgrades in the technology systems of the world and are well versed with them. By way of organizational objectives, terrorist organizations recruit people for cyberterrorism.

Creating hindrances in the normal life of people by disrupting network systems and their software is also one of the objectives of cyber terrorism. These strategies have been demonstrated

[12] *Ibid*
[13] *Ibid*

to be effective given how heavily Western nations rely on online infrastructure to supply essential services. Despite the fact that these cyberterrorist actions have largely inflicted little harm to anyone as of now, they cannot be ignored.

CONTEMPORARY INCIDENTS OF CYBERTERRORISM

There has been a rise in the incidents of cyberterrorism in recent times due to more reliability in the technology, especially in western countries. The incidents of cyberterrorism have caused huge damage to countries in the recent past. Some of the below incidents can be termed cyberterrorism –

India and Pakistan Conflict: There have always been tussles between India and Pakistan since the partition regarding Kashmir. As a result of same India was attacked several times by the cyber terrorist groups of Pakistan to get information about the various things which can be further used by Pakistan to gain control over the land of Kashmir. Many important organizations in India, like the Zee Network, the India Institute of Science, and the Bhabha Atomic Research Center, have been damaged or had their services interrupted by groups like G-Force and Doctor Nuker.[14] The United States Air Force Computing Environment and the Department of Energy's website were both targeted by the Pakistani Hackerz Club Group.[15]

Cyber-attack by Tamil Tigers: With escalating acts of violence in Sri Lanka over several years, cyberspace was the next frontier to be attacked in 1998. Over 800 emails per day were sent by the murderous rebel group known as the Tamil Tigers to Sri Lankan embassies.[16] This was done over the course of two weeks. "We are the Internet Black Tigers, and we are doing this to interrupt your communications," the attack's email message declared.[17] After the communications caused such severe disruption, local intelligence officials were sent to look into

[14] Michael A Vatis, 'Cyber Attacks during the war on terrorism: A predictive analysis' (*Dartmouth College*, 22 September 2001) <https://apps.dtic.mil/sti/pdfs/ADA395300.pdf> accessed 12 August 2022
[15] *Ibid*
[16] Rajeev Puran, 'Beyond Conventional Terrorism...The Cyber Assault' (*SANS.Org*, 6 April 2003) <https://www.sans.org/white-papers/931/> accessed 12 August 2022
[17] *Ibid*

the matter. The attack was the first documented attempt by terrorists to target a computer system in Sri Lanka, according to the police.

Yugoslavia Conflict: Yugoslavia was hit by air strikes by NATO and as a result, of the same, the hackers of Yugoslavia attacked the servers of NATO. All 100 servers of NATO were subjected to "ping saturation," DDoS attacks, and a barrage of tens of thousands of emails, many of which included viruses. The attacks on NATO servers happened at the same time as multiple internet defacements of the American military,[18] government, and commercial sites by Yugoslavia-supporting Serbian, Russian, and Chinese individuals. The communications infrastructures of NATO are severely disrupted by these attacks.[19]

Sony PlayStation Network, Microsoft's Xbox Live network case: A group named Lizard Squad who classify themselves as cyberterrorists attacked the servers of Sony in 2014, and in this attack, information related to the employees, movies, and other kinds of sensitive information was leaked due to which Sony faced huge losses in revenue. "The motivation for these cyberterrorist operations is the potential for collateral harm and the acts' clear connections to geopolitical issues. Cyberterrorism is perhaps one of the biggest concerns facing the United States today, according to the former president of the United States Barack Obama.[20] Unfortunately, the assaults are not only here to stay but are also probably going to get much worse given how heavily we rely on the Internet today."[21]

Attacks in the Middle East: There have been several types of cyber-attacks taking place in the middle-eastern countries such as Palestine and Israel. There have been various instances where these countries attack each other cyber systems to gain advantage of the situation.[22] "The attacks

---

[18] Cyber Crime (n 8)
[19] *Ibid*
[20] Dan Holden, 'Is Cyber-Terrorism the New Normal?' (*Wired*) <http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/> accessed 13 August 2022
[21] *Ibid*
[22] Ethan Zuckerman & Ors, 'Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites' (*Harvard*, December 2010) <https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf> accessed 13 August 2022

were a volley of e-mail floods,[23] DoS attacks, and Ping flooding of such sites as the Israel Foreign Ministry,[24] Israeli Defence Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah."[25]

LEGAL FRAMEWORK

India is a developing country and in a country like ours, it becomes most important to protect the data of individuals or to prevent any kind of cyber-attacks from anywhere so that people can trust technology completely. In the beginning, phase if people lose trust in the technology then it would be much more difficult to build that trust again, and as a result of the same, we would not be able to develop at a faster pace. To prevent cybercrime, India addresses issues with several laws which are as follows-

The information technology Act, 2000 is one such Act to prevent cybercrimes. "Due to the absence of a particular provision in the IT Act of 2000 dealing with cyber terrorism, the Information Technology (Amendment) Act of 2008[26] added a new section 66F. Given the rise in terrorist operations in India and its neighbors,[27] the IT Amendment Act of 2008's move is to be applauded."[28]

> *According to Section 66F of the Information Technology Act, 2000, "(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 authorization or exceeding authorized access; or (iii) introducing or causing to introduce any computer contaminant, and using 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*

[23] *Ibid*
[24] Rajeev Puran (n 16)
[25] *Ibid*
[26] Information Technology (Amendment) Act 2008
[27] *Ibid*
[28] Cyber Crime (n 8)

to cause damage or destruction of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70[29]*; or*

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and using 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 about contempt of court, defamation or incitement to an offense, or the advantage of any foreign nation, group of individuals or otherwise, commits the offense of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life."[30]

INDIAN COMPUTER EMERGENCY RESPONSE TEAM

According to Section 70B[31] of the IT (Information Technology) Act, the CERT-In team was established to offer timely notifications of incidents posing a threat to cyber security as well as a list of emergency procedures for dealing with those situations.[32]

CYBER SECURITY POLICY

The cyber security policy was released in 2013, and it was the first time in history that any policy was released for the security of the network system in India.[33] The primary purpose behind the Cyber security policy was to protect cyberspace from outside attacks. One more important feature of this cyber security policy was to protect Indian Cyberspace from the attacks of cyber

[29] Information Technology Act 2000, s 70
[30] Information Technology Act 2000, s 66F
[31] Information Technology Act 2000, s 70B
[32] *Ibid*
[33] Dan Holden (n 20)

terrorists.[34] Over time it has been seen that there has been various kind of loopholes in this policy due to which cyberspace is not protected properly. As a result of the same, it can be said that this policy needs amendments so that Indian cyberspace and users and be protected.

LAWS AT THE INTERNATIONAL LEVEL TO TACKLE CYBERTERRORISM

International Telegraph Union-United Nations

Information and communication technology-related matters are handled by the International Telegraph Union ("ITU"), a specialized organization of the United Nations. Building cyber security in all of its member nations and fostering international collaboration are two of ITU's fundamental responsibilities. The ITU developed the Global Cybersecurity Agenda in 2007 in order to accomplish this, and all of its members are required to adhere to it.

Budapest Convention on Cyber Crime – Council of Europe

The Budapest Convention was one of the first conventions which deal with cybercrime and cyberterrorism. This treaty's primary goal is to foster international cooperation between states. It has established a unified strategy to combat cybercrime and cyberterrorism. The security of data in cyberspace is another topic covered.

North Atlantic Treaty Organisation

NATO is also one of the organizations which take stapes to prevent cyberterrorism. Although the prevention of cyberterrorism is not its primary objective in order to ensure cyber security and stop terrorism, it established the Cyber Defence Management Authority. Additionally, it has established a Rapid Reaction Team to defend against cyberattacks. Aside from the organizations and activities stated above, each nation has its own set of cyber and defense laws[35] with the express purpose of ensuring cyber security and preventing cyber terrorism.

[34] *Ibid*
[35] *Ibid*

CONCLUSION

Summing up, it can be concluded that cyberterrorism is an upcoming threat, and there needs to be increasing awareness regarding it. The damage done due to such attacks has been increasing over time, from official communication disruptions to large-scale losses for companies. The key way to prevent such attacks is awareness since these attacks often take advantage of those systems through people who are unaware of such incidents or their possibility. The Legal Acts and Policies are another way of protecting people from cyberterrorism. There have been various laws and policies framed at national and international levels to prevent cyberterrorism but most of them need amendments as the existing ones are unable to control cyberterrorism. As a result of the same, it is flourishing at a much faster pace. It can be said that the need for the prevention of such incidents is high, with the increased dependence upon technology.