Page 544 - 550

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 3

2020

Cyber Terrorism: A Disguise Impact of Internet Technology over Global Networks

SAKSHAM KUMAR[1] AND ARANYA CHATTERJEE[2]

ABSTRACT

Terrorism is spreading widely all over the world at a greater pace. Today terrorism doesn't restrict itself to physical/ Bodily injury rather has been extended to the terrorism through the virtual world i.e. the cyberspace. When the information system of a nation is attacked which in turn creates a situation of panic and puzzle in the minds of the people of the country, it amounts to cyber terrorism. In today's world, the internet has become an essential constituent and intrinsic part to every factor from which a nation runs and relies upon whether it is economic, social, legal parameters, security and protocols of a country or an individual. This paper aims to discussing the concept of cyber terrorism in depth by explaining to the readers the varied ill-effects which are a result of cyber terrorism and what causes cyber terrorism. Additionally, this paper also puts light on the ways in which cyber terrorism can be suppressed or rather eradicated in an efficient and effective manner.

***Keywords: -** Cyberspace; Cyber Terrorism; Virtual World.*

I. INTRODUCTION

Computers, as well as the Internet, together have been a blessing to mankind. It has rendered various aids to an individual in society since a long span of time. However, as every coin has two sides so is the case of computers and the internet? It is nothing less than a two-faced sword. It has uplifted the standard of life of every individual in society and on the other hand, it has also been causing some serious threats and hindrances to the legal world. With the expansion of Internet, computer systems have been assigned a greater degree of responsibility which has led to making it more and more complex and independent. With the expansion of Internet, computer systems have been assigned a greater degree of responsibility which has in turn made it even more complicated and vandalised and even it has caused terrorism using cyberspace which in turn is causing a greater level of threat to people at large. Whatsoever

[1]Author is a student at New Law College, Bharati Vidyapeeth University, Pune, India.
[2] Author is a student at New Law College, Bharati Vidyapeeth University, Pune, India.

the good internet renders to the people at large, it also has its dark sides[3].Cyber terrorism has been gaining momentum nowadays since the recent past. Cyber terrorism is nothing, but the electronic attack was done through the cyberspace, both internally as well as externally, in other words, it is the electronic attack which is done using the computer networks and internet. With the advancement and development in computer technology, as well as the dependence of human beings on computers and the Internet, has led to the cities development and increase in the case of cyber terrorism.

If we analyse the definition of given here, we understand that cyber terrorism comes into picture only when infringes the confidentiality integrity and availability (CIA) of the computers, networks and information stored; as well as cause violence or some sort of harm. Cyber terrorism was coined by Barry C. Collin.

II. DEFINITION OF CYBER TERRORISM:

A physical attack that hampers computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard, can also contribute to, or be called as cyber terrorism[4]

The FBI defined cyber terrorism as "The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents"[5].

NATO defines cyber-terrorism as "a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal*."*[6]

The Federal Emergency Management Agency (FEMA) defines cyber-terrorism as "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"[7].

The U.S. National Infrastructure Protection Centre defined the term as: "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and

[3]R.K.CHAUBEY, AN INTRODUCTION TO CYBER CRIME AND CYBER LAW (Kamal Law House 2012).
[4] Dan Verton, *A Definition of Cyber-terrorism*, COMPUTERWORLD, (August 11, 2003) [http://www.computerworld.com/securitytopics/security/story/0,10801,83843,00.html].
[5] Valarie Findlay, *Cyber-Terrorism and Canada's Cyber- Security Strategy*, SSR., April 2015, at 1, 1.
[6] Aditya Goyal, *Cyber Terrorism: An Analysis with an Indian Perspective*, 4 CMET. 74, 74 (2017).
[7] Clay Wilson, Botnets, *Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Cong. Research Serv., 4 (2018) (quoting from the FEMA toolkit for terrorism responses).

uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda"[8].

However, in the real picture Cyberspace and electronic devices is often used by the terrorists to communicate, plan, carry out attacks, obtain funding, arms procurement, intelligence gathering and to attract supporters. The motive for cyber terrorism is mostly destruction or manipulation of data, identity theft, hacking and computer viruses fall under the category of various reasons which are an instrument for the occurrence of cyber terrorism. Threatening a large bank is one of the serious issues which we can consider for cyber terrorism. The senior directors are left with the encrypted message which is done by the terrorist who has hacked into the system which in turn threatens the bank.

III. Causes Of Cyber Terrorism

- In general, cyber terrorism is growing its root because of the merit that it is cheaper than the other traditional methods.
- It can also have the advantage of impersonation, anonymously causing cyber terrorism.
- Convenience is also one of the reason due to which Cyber terrorism takes place
- Large numbers of people can also be targeted without any hindrances or physical barriers and at minimum risk of getting tracked.
- Cyber Terrorism can also take place in order to hamper the image of a company, an alliance or a nation.

IV. Impacts

- Cyber terrorism disturbs the economical and political stability of a country.
- The stock market, the consumption patterns of the consumers and the whole economy will be at stake due to the cyber terrorism
- Cyber terrorism is a serious threat to integrity and security of a nation.
- Cyber terrorism also impacts the infrastructure of a nation due to which tends to hamper the growth and development of the nation.
- The economy of a nation destroys the resources and manpower of a nation making it subject and vulnerable to military attacks.
- The businesses which run its operation on an online platform get severely affected due to cyber terrorism.

[8] R.K. CHAUBEY, AN INTRODUCTION TO CYBER CRIME AND CYBER LAW 474 (2d ed. 2015).

- The security of the nation is often subjected to getting endangered as cyber terrorism creates a significant impact on the sensitive and secret information of the nation

V. Illustrations And Case Laws

- A cyber attack worse than warfare, In today's century the technologies have been so developed that not only are online consumers inconvenient but also there is a cyber threat in digital platforms and so many countries have faced this threat.
- In 2007, in Estonia, the country faced horrendous cyber attacks[9], their one of the essential infrastructure collapsed without any explosion or any sign of the enemy, from newspaper to banks to power system everything collapsed.
- In 2005, in Ukrainehackers had hacked the power grid system and so many of the houses had gone too far for hours.
- In 2010, in India, there was a computer worm which attacked the digital platform of India and it was the third most affected country of this worm Stuxnet and it attacked the power grid and the state-owned oil corporation.

So, there should be an ardent system be made to save the online users, systems, and digital platforms from online perpetrators,Cyber terrorism is also often a result of the intention to get a personal, individual gain. Chaos Computer Club discovered in 1997 is one such example for it. This club created an article X control for the Internet that could trick the Quicken Accounting program for removing from the users' bank account a sum of money and they are the users who have the Quicken software installed in their personal computers. This file could destroy the users' networks, harming and annoying and it'll also be causing a distraction to the users.

- The hacking of the Ukrainian president's website 'Viktor Yushchenko'by the hackers marks another case of cyber terrorism[10].
- May 2007 so witnessed the greater cyber attack in the wake of removing the Russian World War II war memorial from downtown Tallinn[11]. In this Attack selected sites were bombarded with traffic in order to force them offline nearly all Estonian government ministry networks as well as to two major Estonian bank networks were knocked off.

---

[9]Boyte, Kenneth, __*A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Computer-Supported Warfare*, 7 IJCWT. 54, 56 (2017).
[10]M.N. SIROHI, CYBER TERRORISM AND INFORMATION WARFARE 13 (Alpha Editions 2015).
[11] A. KIYUNA, L. CONYERS, CYBERWARFARE SOURCEBOOK 92 (Lulu.com 2015).

- 1998 the famous Internet bombing which was done in against the Sri Lanka embassies by the Internet Black Tigers was one of the leading cyber terrorism cases.
- Ahmedabad bomb blast case On July 26, 2821 bomb blast manifested in a row across 70 minutes which resulted in the death of more than 70 people and at the same time approximately 200 people were injured. The media agencies reported that they received 14 pages long emails containing threats by the terrorist group named Mujahedeen, Islamic Militant Group (Harkat-Ul-Jihad-al-Islim) Who were claiming responsibility for the terror attack. According to the media agency, they received these emails just five minutes preceding the bomb attacks and these emails contained the reference of 2002 Gujarat Gupta Godhead train burning incident and seeking revenge for the same. These males arose a serious threat by declaring the phobia of death which was to be witnessed within five minutes after this mail according to the mail by the media agency. These Emails additionally threatened the Chief Minister of Maharashtra along with his deputy by reminding them of the historical 2006 Mumbai train bombings which took place on 11 July 2016 and the mail read as "we surprised at your memories" even MukeshAmbani was dragged into these threats and received such threatening emails
- Mumbai terror attack: - On 26th November2011 In the agony of Mumbai Terror attack was witnessed 12 synchronized bombing and shooting which lasted for 4 days. The terrorists entered Mumbai through the sea by navigating their way by Global Positioning Satellite systems, CD's with high-resolution satellite images, satellite images, different sites and multi-SIM cards which made it hard to track. The government of India just after the Mumbai terror attack due to its huge impact brought into consideration a series of the proposal of amendments to the original information technology act 2000, this proposal contains a certain specific provision regarding the cyber terrorism[12]

VI. LEGAL ASPECTS

- Information Technology Act,2000 (amended in 2008) defines and provides the punishment under Section 66F, according to which whoever does any act which results in intending to intimidate the unity, integrity, security or sovereignty of India and creates a sense of terror in the minds of people or even any section of people by the way of denial to authorised access of a computer resource or by gaining

[12]HalderDebarati, *Information Technology Act and Cyber Terrorism: A Critical Review*. SSRN Electronic Journal, 75 , 81 (2011).

unauthorised access and causing any disruption to the computer resources and if by the virtue of these acts it results or is likely to result in death or any injuries to any individual or it causes or is likely of cause any form of damage or destruction to any property, or it causes disruption to the supply of services which are essential to the life of the community or it can even cause an unfavourable effect on the critical information system as described under section 70 of the act. It also includes unauthorised access, knowingly or intentionally to the data, information which is crucial and was kept restricted for the security of the State and such data if obtained can even cause serious damage to the sovereignty and integrity of the nation, morality, public relations of the State, etc. Any person who commits or even who conspires to commit cyber terrorism is punishable with imprisonment which may extend to life imprisonment.

This section 66 F of the Information Technology Act, 2000 must be read along with a significant section 499 of the Indian Penal Code[13]

- Under Section 69A of the Act, empowers the Central Government or any officer officially authorised by it to give directions to block any content which it believes to put the sovereignty and integrity of the nation under threat.
- Unlawful Activities Prevention Act, 1967

It prevents the association of unlawful activities in India. It provides for the punishments for terrorist activities which is inclusive of the organisation of terrorist camps and recruitment of individuals for the purpose of carrying out terrorist ventures and for performing all these activities of cyberspace is used as a medium then it'll also be punished.

- Cyber Security Policy, 2013

It aims at strengthening the security of cyberspace. It keeps the cyberspace under blanket protection against all the terrorists and even other forms of anti-social elements that tend to possess a threat to the security of cyberspace.

- As such, the EU convention on cyber crimes, 2001 had laid down strategic roles for the member parties to corroborate with each[14].

VII. Measures to Curb Cyber Terrorism

- Making new and best possible security policies and strategies.
- Deployment Of high-security applications.

[13] Indian Penal Code, 1860, Sec. 499.

[14] The EU Convention on Cyber Crimes, 2001, art. 23-35

- Enculturation of an Effective Disaster Recovery plan.
- Lay more focus on Security awareness.
- Enactment of stricter cyber laws.
- Promotion of research and development

VIII. Conclusion

Cyber terrorism is a great challenge which exists to the security of an individual or a nation and it is growing in manifolds in the previous few years on a global scale. Advancement in technology dependence on computer networks has led to the people falling prey for cyber terrorism. Despite having existing cyber laws and other related laws related to cyber terrorism the problem of cyber terrorism has not yet been eradicated rather it has been increasing at an alarming rate. Ample cyber jurists[15]claim that the Information Technology Act, 2000 should be amended on the lines of criminal law to make it workable, was at last paid attention by the government[16]Hence, in a nutshell, it can be said That one should be paid enough heed the increasing problem of cyber terrorism before it's too late.

*****

[15]VIVEK SOOD, CYBER LAW SIMPLIFIED, (Tata McGraw Hill Publishing Companies, New Delhi, 2001).
[16]TALAT FATIMA, CYBER CRIME 246 (2d ed. Eastern Book Company, Lucknow 2016).

 [ISSN 2581-5369]