INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 2 | Issue 2

2020

A Synopsis on Cyber Terrorism Dark Side of Cyber Space

SIDRAH JAMI[1]

ABSTRACT

Cyber Terrorism is one of the most alarming issue in India and across the world. The paper focuses on the concept of cyberterrorism and how it evolved so rapidly worldwide. Firstly, the paper pro-vides an introduction to the cyber warfare and cyberattacks and focuses on the evolution of cyber terrorism. Secondly, the paper emphasis on cyber-attack, definition of cyber terrorism and cyber threats which can be characterized as cyber espionage, cyber warfare, cyber terrorism and cyber-crime. Thirdly, the paper focuses on the modes of cyber terrorism like computer system, encrypted programs, satellites, worms and on reasons of growth of cyber terrorism. Fourthly, the paper focuses on cyber terrorism given under Section 66F of Information Technology Act 2002 and various other Indian Laws like the Indian Penal Code 1860. Fifthly, the paper deals with the challenges to the national security of India and the response of the government. The last section of the paper provides a conclusion and strategies for cyber defense to combat the issue of cyber terrorism all across the world.

I. INTRODUCTION

Hans Morgenthau said that the security of the nation depends upon the borders and the institutions which exist in the country. However, since 2016, many things starting from the elections to electrici-ty have been computerized and displayed on the internet. The major threat to national security is derived from cyberspace. It is a complex and multidimensional against which no degree of technical superiority is likely to suffice. Cyber warfare has been happening in the world for many years. It has led to a major threat to national security, public safety and provides challenges to the economy of the country. Technology is considered to have good effects but also portrays certain negative ef-fects on the country. It becomes a double edge sword. Cyber-attacks harm the computing networks and damages critical infrastructure like telecommunication, electric power, air traffic, water supply which is controlled by the computer. As there is a very fine interconnection between the elements in the computers, one single attack in one computer can lead to failure with the deadliest

[1] Author is a student at Amity Law School, Noida, India.

consequenc-es. Therefore, technology has provided power to the organized criminal groups criminal hackers and terrorist networks to disrupt the infrastructure of a nation providing challenges to national security, economy, public safety, commerce and military security.

II. Evolution of cybercrime

The first cyber-terrorism attack which happened on communication lines was in Germany. After World War 2 to 1991, there were two superpowers the (1) the United States of America (USA) and (2) the Soviet Union[2]. There was a conflict going on between them, though it was not a physical war and was called cold war. From the 1960's to 1980's many hackers started coming up and took their shape to Information Super Highway. In 1986, the West German hackers hacked and accessed the Department of Defense Systems of the USA. In 1988, Osama Bin Laden established

'AL- Qaeda' based on 'Jihad'. Cyber terrorism was found in a large number during the Gulf War. Gulf War was considered to be the first information war. The USA implemented the National Infra-structure Protection Act, 1990 to control cyber terrorism. The UK constructed the Defense Evalua-tion and Research Agency in the year 1998. Later on, many countries like Switzerland, France, Germany, Norway, Sweden and Finland came together to combat the crime of cyber warfare. Dur-ing

the 1990s the World Wide Web (WWW) became very popular in India. There were various attacks planned in India like the attack done by the LTTE group or the attack done by Aftab Ansari on American Centre in Kolkata. He communicated with his terrorist group from Dubai. Cyber Terror-ism has been considered as an important issue in the global parameters. Terrorists have started using cyberspace to do attacks by bombing at certain places. They use the internet for communicating the events and to use advanced new technologies.

III. What is cyber attack?

A cyber-attack is one where the hackers implant a malicious code that disrupts or harms the data and the output. The hackers usually put these software, viruses, worms etc into computer systems that are lacking the security software or have a faulty system configuration. Once a virus is implant-ed the hacker has full control over the computer, can send commands to spy on the contents of the computer and to attack or disrupt other computers.

IV. Definition of cyber terrorism

Cyber terrorism is a phrase used to describe the use of Internet-based attacks in terrorist

[2] Dr. M. Dasgupta, Cyber Crime in India-A Comparative Study, pp. 191-193, Eastern Law House, 2009.

activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses[3].

Terrorism which is related to cyber is called cyber terrorism. Cyber terrorism is a collective form of cyberspace and terrorism. It consists of the unlawful attacks and threats which happen against the computer, networks and the private information which is stored on the computer. It is usually done to pose a threat to national security and the government. Cyber terrorism can lead to violence and destruction against a person and his property. It can death and serious befit harm through explo-sions, water contamination, plane crashes or severe economic losses. Cyber terrorism directly attacks the lives and the infrastructure which are located within the national boundaries. Their aim is to cause a state of terror and panic amongst the civilians living in the country.[4]

There can be two concepts of cyber terrorism;

- Under the first concept, the terrorist uses information technology to hack the computer through implanting malicious software, codes, viruses to the computer which can be used as a target or a weapon against the national security of the nation and the government.

- Under the second concept, the terrorist uses the information technology to hack the computer through methods like cyber fraud, theft, cyber pornography or spamming which can cause threat in the minds of the people.

V. CYBER ATTACKS

Cyber-attacks are defined as the "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these sys-tems or networks". Cyber-attacks can be distinguished between four types:

(i) Cyber Warfare: Under this, the action of hacking is done by one state to penetrate another na-tion's computer or networks for causing destruction and damage to the data.[5]

(ii) Cyber Crime: Under this, the external organizations try to get into someone else's

[3] "Cyber Security 2012", Available on http://zspatel.org/upload/files/BCA%20Notes/ cyber%20crime.pdf?

[4] Tara Mythri Raghavan (2003), "In Fear of Cyberterrorism: An Analysis of the Congressional Response", Illinois College of Law, USA.

[5] Devendra Parulekar (2014), "Cyberspace: A focus on India", retrieved from http://www.ey.com/Publication/ vwLUAssets/EY-CFO-need-to-know-cyber- security-a_focus-on-india/$FILE/EY-CFO-need-to-know-cyber security-a-focus-on- india.pdf

computer to use, control and infiltrate data from that organization.[6]

(iii) Cyber espionage: Under this, there is a penetration into computers and networks for obtaining data and information for intelligence purposes.

(iv) Cyber terrorism: Under this, the non-state actors like terrorist groups try to hack the network and the computers of destructive proposes

There has been a rise in the cases of cyber-attacks. The hackers usually hack computers who have weak authorization systems. They exploit the system by implanting viruses and malicious software.[7]

VI. Modes of cyber terrorism

There are different modes of cyber terrorism:

(i) Computer system and internet facilities

Under this, the terrorist groups use the computer system and facilities to develop their network and websites for sending messages to each member all across the world.[8]

(ii) International Cyber Attack

Under this when any international organization of terrorist communicates or links together through the internet and then attacks a nation, it will be considered as an international cyber terrorist attack. e.g.: The 9/11 attacks happened attacking the World Trade Centre and Pentagon whereas in the same year on 13 December 2001, there was an attack in the Indian Parliament.

(iii) Encryption Programs and Programs

Under this, the cyber-terrorist uses encryption programs and Digital signature for their coordination and communication amongst their members. The USA has been keeping a close watch since 1990's use of such programs.

(iv)Information and Communication Technology (ICT) including Satellite Transmission

Nowadays, terrorists use ICT which includes cellphones, satellite transmission etc so that they can communicate and coordinate with each other for planning a cyber-attack.

(v) Virus, Worms, Trojan Horse

[6] "Cybersecurity–An Overview" (2012), in "India's Cyber Security Challenge", IDSA Task Force Report, New Delhi

[7] Col. S S Raghav (2010), "Cyber Security In India's Counter Terrorism Strategy", http://ids.nic.in/art_by_ofds/Cyber%20security%20 in%20india%20by%20Col%20SS%20Raghav.pdf

[8] Muktesh Chander, "Cyber Terrorism: A Myth or Possibility", Indian Police Journal, July- September, 2003, p. 25.

Under this, the terrorist groups use viruses, norms, trojan horse etc to disrupt the working of gov-ernmental departments like intelligence, commerce, defense, health and academic. This is one of the most common ways which increases cyber terrorism in country.

VII. REASONS FOR INCREASE IN CYBER TERRORISM

There has been a rapid increase in cyber terrorism in many nations. Some of the reasons for the growth of cyber terrorism is:

(i) A threat in mind: Interest is being used widely amongst all counties. It is the easiest medium that can create a fear or threat in minds of the people.

(ii) Spread of terror: The use of the internet can lead to a larger terror attack on a wide scale. The attack can be committed by terrorist groups at different places at the same time.

(iii) Disability of government functions: The countries have started using digital operations for processes that can give chances for the hackers to slow down the functions of the country.

(iv) Easy to execute: The hacker need not be present at a target spot but can easily operate it through the computers. It is an easy process for the attacker to execute the attack.

Section 66 F of the Information Technology Act 2000, provides punishment for cyber terrorism.

Section 66F: Punishment for cyber terrorism. -(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 au-thorized 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 authorization 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 incite-ment 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 Terrorists ac-tivities being done by foreign it would be obligatory to read insertion 66F along with Section 75 of this Act.

Cyber Terrorism with other laws

Cyber Terrorism is a kind of offence that is committed against the state and is given under Chapter VI of the Indian Penal Code. It talks about the offence that is committed against the country.

It can also be read with Section 499 of the Indian Penal Code along with Section 66 of the Infor-mation Technology Act.

VIII. Challenges to national security

The combination of the virtual and the physical world has led to the creation of a new threat called cyber terrorism. Cyber terrorism inhibits fear and ignorance in the minds of people. There has been a failure to distinguish between hacktivism and cyber terrorism which has led to cyber terrorism. There have been a number of targets and a lack of proper safeguards to combat the threat of cyber terrorism.[9] In the 21st century, most of the terrorist groups existing in India have used the internet to develop psychological warfare, recruitment, data mining, network and information sharing. Ter-rorists have started using communication, weapons and new techniques for destruction to a person’s life and his property. They work in a decentralized manner which makes them difficult to trace and locate. They work, prepare and execute operations through the use of the internet.

After liberalization, there has been a huge change in the information technology, electricity and the telecom sector existing in the country. However, there has been an inadequate focus on the prepar-edness of disasters. The government has now introduced a comprehensive disaster preparedness and recovery strategy. India has been expanding its e-governance and

[9] S R R Aiyengar (2010), “National Strategy for Cyberspace Security”, Manekshaw Paper no. 23, Centre for Land Warfare Studies, New Delhi

e-commerce and infrastructure towards the natural and manmade disaster, it has reduced the effects on our national security.[10]

IX. The response of the government

In 1999, the Indian government merged the national informatics center (NIC), department of elec-tronics (DOE), established a new ministry of information technology (MIT) and electronics and software export promotion council. The Indian legislature also implemented The Information Act of 2000 but it contained no provision of cyber terrorism. Later the amendment act was passed which dealt with the provision of cyber terrorism. Cyber terrorism was given under Section 66F of IT Act.

To commit the office of cyber terrorism the act must be committed with the interrelation of threat-ening the sovereignty, security, integrity and unity of the nation through interfering and accessing a computer resource, or obtaining unauthorized access to computer and damaging its data. This act Is punishable if it causes serious injury or death to a person, or damage and destruction to property or disrupt the essential suppliers service and affects the information infrastructure. In 2004, the Indian government established the Indian Computer emergency response Team (CerT-In) for cyber security.[11] CERT-in functions under the DIT regarding the cyber threat in the nation. It was established to prevent cyber security incidents.[12] The Indian government also established a centralised mech-anism called the National Cyber Coordination Centre [NCCC] for analysing and coordinating the information collected from interest accounts throughout the nation. It looks after the cybersecurity threats in the country and tries to prevent and coordinate them through intelligence and various agencies like the National Technical Research Organization (NTRO), Research and Analysis Wing (RAW), Department of Telecommunications, CERT-In, Intelligence Bureau (IB) and , Defense Re-search and Development Organization (DRDO), and different military services.[13]

X. Strategies for cyber defense

If a nation forms a proper strategy for cyber defense then and nation can develop in it's technical, security or economic sector. There can be various strategies made for combatting cyber terrorism in the country. Firstly, there should be a proper National model agency that

[10] M M Chaturvedi and MP Gupta and Jaijit Bhattacharya (2015), "Cyber Security Infrastructure in India: A Study", Department of Management Studies, Indian Institute of Technology Delhi, New Delhi.

[11] M M Chaturvedi and MP Gupta and Jaijit Bhattacharya (2015), op. cit., no16

[12] Zachary Keck (2013), "India Sets Up Domestic PRISM-Like Cyber Surveillance?", the diplomat, June 14, http://thediplomat.com/2013/06/india-sets-updomestic-prism-like-cyber-surveillance/

[13] S R R Aiyengar (2010), op. cit., no15

looks after the coordina-tion of matters relating to cyber security in the country. Secondly, the government should launch a National Mission in Cyber Forensics for the effective and fair prosecution of cyber terrorists and criminals. Thirdly, there should be strong security models that can protect the sectors of security and infrastructure. Fourthly, there should be specified and proper training given to people in order to assist users in IT security. Fifthly, there should be proper identification and information exchange adopted for combatting malicious cyber activities.

XI. Conclusion

Taking everything into account, it very well may be said that the customary ideas and techniques for terrorism have taken new measurements, which are more dangerous and lethal in nature. In the peri-od of data innovation, the terrorists have gained a mastery to deliver the most destructive blend of weapons and innovation, which if not appropriately protected at the appointed time of time, will incur significant damage. The internet is powerless against a wide assortment of episodes, regardless of whether deliberate or unplanned, synthetic or normal, and the information traded on the internet can be misused for detestable purposes by both country states and non-state entertainers. The world is confronting the most exceedingly awful type of fear mongering, prominently known as cyber ter-rorism. The articulation of cyber terrorism incorporates a purposeful negative and harmful utilization of the data innovation for producing ruinous and harmful impacts to the property.

The law dealing with terrorism is not sufficient to meet the precarious goals of these terrorists and requires restoration in the light and setting of the most recent advancements in the world. The laws need to deal with the issues starting at the worldwide level on the grounds because the Internet, through which these terrorist exercises are done, perceives no geographical limits. In this way, a cyber-terrorist can collapse the entire structure of a nation from a spot. The crucial way to safeguard this situation is to use the latest technologies and innovations. Thus, a good blend of the most recent security innovation technology and a law managing terrorism is the need of the hour.

*****