IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cyberterrorism -An Emerging Cybercrime International And National Scenario

Dr. Shashya Mishra

Assistant Professor

Amity Law School

Amity University Lucknow

Abstract-

We are living in the era of the globalistaion. In the globalised world technology plays a very important role. Cyberspace has emerged as a new path for creating connections and communication in India in starting of year 2000.Internet is used for creating new connections and at the same time it is a place for committing illegal activities. These illegal activities known as cybercrime are not only against individual or organisation but also against the nation. Cyberterrorism is an example of cybercrime against the security and sovereignty of nation. United nations has created many international conventions and treaties for maintaining peace and security. In 2001 Convention on Cybercrime has emerged as one of the document for curbing cybercrime. Similarly, in India Information Technology Act 2000 was made for curbing issues related to cybercrime, The said legislation was amended ion the year 2008 and it has included cyber terrorism as one of the emerging crime in India. Indian judiciary is also doing commendable job to tackle the issue of cyber terrorism in India.

Key Words -cybercrime, cyber terrorism, United Nations, IT Act 2000

"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner."

—Ban Ki-moon

Introduction

Crime in cyberspace is now a worldwide phenomenon. We are tending towards the technology to a great extent. This excessive use of technology has its own pros and cons. On the one hand is connecting people all around the globe. But on the other hand this virtual world is used by the criminals to commit crime. Now cybercrime is not just limited to financial frauds. There are new dimensions of cybercrime which not only effect individual or organisation but also has a tendency to affect the sovereignty and integrity of the nation. Cyberterrorism is one such cybercrime which disturbs the security of the nation. Cyberterrorism is

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 At international level there are various treaties dealing with privacy and security in cyberspace. Similarly, in India there are laws and policies to curb cyber crime. This research work will analyse the actions of international organisation in curbing cybercrime or cyber terrorism and legislative measures opted by India for effectively combating with new emerging cybercrime like cyber terrorism.

Meaning Of Cybercrime

As per Dr. Debarati Halder and Dr. K. Jaishankar cybercrimes are "Crimes that are done against persons or groups of persons with a unlawful motive to deliberately damage the repute of the prey or cause bodily or psychological damage, or harm, to the target straight or ramblingly, using contemporary telecommunication systems such as Cyberspace (Chat rooms, emails, notice boards and groups) and mobile headsets.

The oxford Dictionary defined the term cyber crime as "Illegal actions carried out by means of processers or the net." "Cybercrime may be said to be those species, of which, kind is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"8 "Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them

Cyber Terrorism- Concept -

The word "Cyber Terrorism" is of recent vintage and was invented by computer *whiz Barry C. Collin*. A widely acceptable definition of cyber terrorism is " a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda." According to the *U.S. Federal Bureau of Investigation*, " *Cyber terrorism is any premeditated, 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]

Cyberterrorism is often defined as any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population. Attackers often do this by damaging or disrupting critical infrastructure.[2]

[1] Pujari; Amaresh, CYBER TERRORISM World Wide Weaponisation https://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf
[2] Sheldon; Robert, Hanna; Terrell Katie, cyberterrorism, https://www.techtarget.com/searchsecurity/definition/cyberterrorism

Cyber terrorism is defined by researchers *Jordan Plotnek and Jill Slay* as a premeditated attack or the threat of such an attack by nonstate actors intending to use cyberspace to cause physical, psychosocial, political, economic, ecological, or other damage. The goal of the cybercriminals is to induce fear or coerce government or nongovernment bodies to act in a way that furthers the criminals' social, financial, or ideological objectives.[3] Cyber Terrorism attacks us at the point at which the "physical world" and "virtual world" converge. The "physical world" is physical matter that is seen, touched, and ingested every day. The "virtual world" is symbolic, that place in which computer programs function and data moves. Increasingly, people's experience of the physical world is dependent on the operations of the virtual world. This dependence and intersection of the physical world and the virtual world make masses of people vulnerable to the Cyber Terrorist. A Cyber Terrorist could remotely access the processing control systems of a cereal manufacturer to sicken and kill the children of a nation. A CyberTerrorist could place computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb receiving each other's pattern, so if one bomb stops transmitting, all bombs detonate simultaneously[4]

International Organisation- Cyber Terrorism-

The *United Nations General Assembly* addressed various ways States could strive to combat the criminal misuse of information technologies. Various other Resolutions have been adopted, among them Resolution 57/239 in 2002 on the Creation of a global culture of cyber-security. The General Assembly adopted a new Resolution 58/199 in 2003, on the Creation of a global culture of cyber-security and the protection of critical information infrastructure. This Resolution also invited the member states to take into account the principles in the preparation for the ***World Summit on the Information Society (WSIS) in Tunis in 2005.*** Based on the 2005 World Summit Outcome Document, a global counter-terrorism strategy was adopted by the General Assembly in 2006[5].The Security Council's Counter-Terrorism Committee[6] is the main committee and leading body to promote collective actions on counter-terrorism efforts in the United Nations.

The United ***Nations Office on Drugs and Crime in Vienna***, is the organizer of the *United Nations Crime Congresses* and has established the Terrorism Prevention Branch. The Crime Congress in 2005 in Bangkok, Thailand, discussed issues of computer-related crime in a special workshop, and the strengths and weaknesses of the international legal instruments on counter-terrorism in a special committee.[7] The United Nations have at least 12 universal instruments on terrorism and 85 States (December 2006) have ratified all of them. The UNODC Terrorism Prevention Branch provides legal advices to States on becoming parties to these universal instruments and promotes global cooperation.

[3] Cyber Terrorism: What It Is and How It's Evolved, https://online.maryville.edu/blog/cyber-terrorism/#what-is
[4] U.S. Department of Justice Office of Justice Programs Future of Cyberterrorism: The Physical and Virtual Worlds Converge https://www.ojp.gov/ncjrs/virtual-library/abstracts/future-cyberterrorism-physical-and-virtual-worlds-converge
[5] adopted by the General Assembly on September 8, 2006 (A/res/60/288)
[6] The committee was established by the Security Council on September 28, 2001
[7] Office on Drugs and Crime https://www.unodc.org/unodc/crime_congress_11/documents.html

The ***Council of Europe Convention on Cybercrime*** was adopted in 2001,and entered into force on July 1, 2004. By ratifying or acceding to the Convention, States agreed to ensure that their domestic laws criminalize the conducts described in the substantive criminal law section and establishes the procedural tools necessary to investigate and prosecute such crimes. The section on substantive criminal law contains of offences covering attacks against the critical information infrastructure of computer data, networks and systems.[8] Cyberterrorism has been defined as unlawful attacks and threats of attack against computers, networks, and stored information. It has to intimidate or coerce a government or its people in furtherance of political or social objectives. An attack should result in violence against persons or property, or at least cause enough harm to generate fear. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact.

The Ministers and Leaders of the ***Asian Pacific Economic Cooperation (APEC)*** have since 2002 43 made commitments to endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the Council of Europe Convention on Cybercrime. The APEC Telecommunications and Information Working Group Meetings have made similar recommendations.[9]

Incidents of Cyberterrorism In India -

Recently in the month of December 2021 a breach of Prime Minster Modi's Twitter allowed hackers to Tweet from the account that India officially adopted bitcoin as legal tender. This Tweet also included a scam link promising a bitcoin giveaway.[10]

Website of CBI is hacked by hackers in 2010 by 'Cyber Army of Pakistan'. In August 2013 Indira Gandhi International Airport (IGI) encountered Cyber attack. A damaging computer program called as 'technical snag' hit the operations of terminal no. 03. This malevolent code was spread remotely for the trespassing- 'the security system of Airfield'. The cyber attackers tried to take benefit of faintness of safety structure. The enquiry of 26/11 Mumbai attack exposed the- indication of Cyber telecommunication of terrorist group, with the assistance of which they aware with map, inhabitants structure, place etc. They use the "Google earth" to perform their strategy, moveable net for grasp and control, social media to trail the movement of Indian Rescue and defence armies. Another Cyber attack was in year 2011, bomb blast in

[8] Article 2 - Illegal access: …the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. Article 3 - Illegal interception: …the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. Article 4 - Data interference: …the damaging, deletion, deterioration, alteration or suppression of computer data without right. Article 5 - System interference: …the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data

[9] Schjolberg; Stein, Terrorism in Cyberspace – Myth or reality? https://www.cybercrimelaw.net/documents/Cyberterrorism.pdf

[10] Center For Strategic & International Studies , https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

marketplace Jhaveri , Mumbai. In Varanasi bomb blast case of 2010, which was also performed with the aid of E-Communication.[11]

A Mumbai sessions court find guilty a 32-year-old technologist and sentenced him to life captivity on charges which involved cyber terrorism. Anees Ansari was under arrest in October 2014 and had been in prison since on claims that he had used the computer and information superhighway service of the private company he worked at to obtain data towards a plan to attack an American School in the Bandra Kurla Complex zone of the town. He has been punished for five years in jail under this section. He has also been directed to pay a fine of Rs 25,000 under provision 43(a)[12] of the Information Technology Act. The court held that Ansari was provided access to a computer and the net at his private office for authorized work and he had formed a false account on Facebook on the official device. The Maharashtra Anti-Terrorism Squad (ATS) had alleged that from August 2, 2011 till October 10, 2014, Ansari, through his fake account, conversed with people and sent "offensive messages" on ISIS dogma to "lurk the harmony and honor of the nation.[13]

Information Technology Act 2000 and Cyberterrorism-

There are several sections under the Information Technology Act which provides punishment for the offences conducted in cyberspace. Section 66 deals with offences related to computer hacking. Section 66 C provides for identity theft. Under IT Act 2000 government has the power to issue directions for seizure or monitoring or decoding of any data through any computer resource.

Then we have Section 66 F of the IT Act which provides for the punishment of cyber terrorism. As per section 66F of the Act any activity in the cyberspace which has the tendency to affect the unity and integrity of the nation will be considered as cyber terrorism. The offence of cyber terrorism is punishable with imprisonment which may extend to life imprisonment[14].

---

[11] Raman; Shiv, Sharma; Nidhi, Cyber Terrorism in India: A Physical Reality Orvirtual Myth Indian Journal of Law and Human Behavior Volume 5 Number 2 (Special Issue), May - August 2019 https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf

[12] compensation for failure to protect data

[13] Modak; Sadaf, Mumbai: Man convicted, sentenced to life for cyber terrorism October 26, 2022 https://indianexpress.com/article/cities/mumbai/mumbai-man-convicted-life-sentence-cyber-terrorism-8222973/

[14] 66-F. 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 authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised 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 authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons

Further Sec. 69B of IT Act 2000 provides power to permit to monitor and accumulate traffic data through any computer resource for cyber security. Sec. By amendment of 2008 section 70B was added to the Act which provides for the creation of Indian Computer Emergency Response Team to serve as nationwide agency for incident response. Moreover there are provisions for the abatement of offences under IT Act 2000.

The National Cyber Security Policy of India, released in 2013, purposes to secure Indian information superhighway and concretise its elasticity from cyberthreats in all sectors. It targets at evolving tactics to protect India's critical information infrastructure (CII) and mechanisms to reply against cyber threats and attacks efficiently. It additionally emphases on producing a harmless and reliable cyber ecology in India. The policy has enabled the formation of a safe calculation atmosphere and established extraordinary belief and self-assurance in automatic businesses. Moreover, a disaster management plan has been instituted to counter cyber-enabled terror outbreaks.[15]

In order to protect the sovereignty and integrity of nation and for maintain peace and harmony government of India has issued various guidelines such as -

• *Implementation of Information Technology (IT) Security Guidelines, 2000*.

• *The Information Technology (Procedure and Safeguard for Interception Monitoring and Decryption of Information) Rules, 2009*.

• *The Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009*.

• *The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009*.

• *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*.

• *The Information Technology (Guidelines for Cyber Cafe) Rules, 2011*.

• *The Information Technology (Electronic Service Delivery) Rules, 2011*.

• *The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties Rules, 2013*.

---

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.]

[15] Juyal; Rebant, Cybersecurity and Threats: Cyberterrorism and the Order Today, JOURNAL OF DEFENCE STUDIES April-June 2021 Volume: 15 Issue: 2 https://idsa.in/jds/cybersecurity-and-threats-15-2-2021

Conclusion –

Attacks on the cyberspace can come in the form of bugs, malware, email phishing, social media fraud - the spectrum of cyber threats is immeasurable. We are more unified than ever before, but for all of the advantages, that connectivity leaves us vulnerable to the risks of fraud, theft, abuse, and attack. Cybercrime can have wide-ranging influences, at the distinct person at local levels and countrywide levels. Thus, cyber terrorism is now we can not say as a new kind of cybercrime against society or nation. At international level several resolutions and conferences are conducted by the United Nations to trace out the causes of cyber terrorism . But still the problem of cyber terrorism is at peak. Similarly in India there are legislation and policy but these two are not effective enough to reduce incidents of cyber terrorism. It takes years to decide a specific case related to cyber crime which actually makes the justice delivery system weak. So, the task of securing data starts from a individual himself. An individual must restrict himself from clicking on any redundant mails. Moreover, we should be more vigilant while accepting any friend request on social media platforms. We should keep on changing password for the sake of cyber security. Thus, for reducing the issue of cyber terrorism the need of the hour is to make law effective at the same time government should try to ensure more digital literacy for securing safety in cyberspace.