DE JURE NEXUS LAW JOURNAL

Author:

Gunjeet Kaur

UIL, Panjab University

5th Year, BA LL.B. (Hons.).

CYBERTERRORISM AND STATE SPONSERED TERRORISM

It's Official: Cyber Terror is the new yellowcake uranium.

– Kevin Poulson

INTRODUCTION

It is said that, information is power and now it is becoming a reality. To begin with, let us understand the literal meaning of Cyberterrorism. It is a convergence of two things i.e. Cyberspace and Terrorism. Cyberspace is the virtual space, considered as the new space for social as well as political activities; whereas terrorism is use of intentional violence for political or religious purposes. "Cyberterrorism" when combined refers to the unlawful attacks against computers, networks, information technology to create terror in the minds of the people with the intention of fulfilling their political, religious or social motive. From historical perspective, the word "cyberterrorism" was first used in 1980s when Collin, a senior researcher at the Institute for Security and Intelligence in California, devised this hot techno-phrase by blending two linguistic elements: cyberspace and terrorism. The FBI explains it as "premeditated, politically encouraged attack on information, computer programs, and data that translate into violence against non-combatant targets by large groups or clandestine agents."[1] Cyberterrorism is becoming more and more important on social networks today. As the Internet becomes

[1] Arturoloroli, Cyberterrorism,(27june,2020,5:00), https://wiki2.org/en/Cyberterrorism

more widespread altogether areas of act, individuals or groups use anonymity offered by cyberspace to threaten citizens, communities and full countries, without the inherent threat of capture, injury or death to the attacker.

Hacktivism Different from Cyberterrorism

Hacktivism is electronic civil disobedience consisting of writing codes in order to promote political ideology. Hacktivists are cyber protesters but not cyberterrorists as they do not cause harm to information systems.

Hackers dig into systems but have no intention to destroy it. Cyberterrorism, on the other hand is integrally a communicative process. Cyberterrorism is more severe form of hacktivism and which can be more destructive.

KINDS OF CYBERTERRORISM[2]

- ✓ ***Simple-Unstructured*****:** the ability to perform basic hacks against individual systems using tools created by someone else. The organization has little capacity for target analysis, command and control, or learning.
- ✓ ***Advanced-Structured***: the ability to conduct more sophisticated attacks against multiple systems or networks and, possibly, modifies or creates basic hacking tools. The organization has a basic capacity for target analysis.
- ✓ ***Complex-Coordinated*****:** the capacity for a coordinated attack capable of causing mass disturbances against integrated and heterogeneous defenses. Ability to create sophisticated hacking tools. Target analysis, high performance command and control capacity and organizational learning capacity.

CYBERATTACKS -MODUS OPERANDI

- ➢ ***Physical Attack-*** IT infrastructure is damaged by using conventional methods like bombs, fire, etc.
- ➢ ***Semantic Attack-*** It's more dangerous because it exploits trust of the user in the system. During the attack, the information entered in the system upon entering and leaving the system is changed without the user knowledge to induce errors,

[2] Arturoloroli, Cyberterrorism,(27june,2020,5:00), https://wiki2.org/en/Cyberterrorism

cybercrime is not only limited to deafening PC foundations, but it is in addition to the use of PC, Internet and data portals-to help the usual types of fear-based oppression like suicide bombings. The web and email can also be used to deal with militant psychological abuse. The most regular use of the Internet is to plan and transfer sites on which false advertising can be placed. This falls under the classification of the use of innovation for mental combat.

- **Syntactic Attack-** IT infrastructure is damaged by modifying system logic to introduce a delay or make the system unpredictable. Computer viruses and Trojans are Syntactic attacks.

CYBERTERRORISM- LEGAL FRAMEWORK

66-F of the Information Technology Act, 2000 talks about Cyberterrorism. It states 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—

- *denying or cause the denial of access to any person authorised to access computer resource; or*
- *attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or*
- *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*

(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 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.*[3]

Mumbai Attack 26/11-

The 2008 Mumbai attacks also denoted to as 26/11 were a series of terrorist attacks that took place in November 2008, when 10 members of Lashkar-e-Taiba, an extremist Islamist terrorist organization based in Pakistan, carried out 12 coordinated shooting and bombing attacks lasting four days across Mumbai.[4] The attackers used a minimum of 3 SIM cards purchased on the Indian aspect of the border with Asian country there have been conjointly reports of a SIM card purchased within the USA state New Jersey. The attackers used a satellite phone and cell phones to speak to every alternative moreover as their handlers that were primarily based in Pakistan. In transcripts intercepted by Indian authorities between the attackers and their handlers, the handlers provided the attackers with encouragement, plan of action recommendation, and knowledge gained from media coverage. This incident prompted the Indian government to introduce important new institutions as well as legal mechanisms to counter terrorism.

STATE AFFILIATED TERRORISM

State affiliated or State-sponsored terrorism is government support for violent non-state actors involved in terrorism. Where possible, state-sponsored actors use standard attack methodologies used by other typical cybercrime actors and penetration testers. They usually involve targeted phishing emails followed by the use of recent and known

[3] Section 66F of the Information Technology Act,2020

[4] Shanthie D'Souza, Mumbai terrorist attacks of 2008, (23 June,2020, 11:31), https://www.britannica.com/event/Mumbai-terrorist-attacks-of-2008

exploits and use the data to spread threat in the minds of the people. Military actions predominantly directed against non-combatant targets have also been referred to as state terrorism.

As the world is becoming digitally sophisticated, the cybercrimes are on the rise. **Dorothy Denning**, an Information Security researcher quoted, “Cyber Terrorism could become more attractive as the real and virtual worlds become more closely coupled, with Automobiles, Appliances and other devices attached to the internet.”

Dr. Pavan Duggal, Cyber Law Expert and Advocate Supreme Court of India, quoted “Most servers are soft targets as they are not well-protected. Cyber secrecy and network security are extremely relevant in today’s context, both the requirements of national sovereign government as those of balancing the needs of data protection and privacy have to be appropriately addressed.”[5]

Julie Gommes, cybersecurity expert, opined that India should be alert to acts of cyber terrorism. European countries of Jihadi cyberterrorism, India remains as vulnerable to cyberterrorism as any other Jihadi-targeted country.

In a recent report, Defence Minister, **Rajnath Singh** said state sponsored terrorism is testing India’s patience, he said, "Terror and its related violence have posed serious challenge to the international environment and the inter-play between state and non-state actors as proxies to spread violence have further increased the threat,"[6]

[5] Dr.Pavan Duggal, PAVAN DUGGAL IN NEWS,(27june,2020,6:00), http://pavanduggal.com/pavan-duggal-in-news/

[6] PTI, State-sponsored terrorism testing India's patience: Rajnath Singh,(23June,2020,13:00), https://economictimes.indiatimes.com/news/defence/state-sponsored-terrorism-testing-indias-patience-rajnath-singh/articleshow/73908627.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

According to **Amos Guiora, Security Expert**, "there is a direct link between cyber security, cyber terrorism and the financing of terrorism which is deeply troubling."[7]

Some incidents of cyber terrorism

- The 2008 Ahmedabad bombings were a series of 21 bomb blasts that hit Ahmedabad, India, on 26 July 2008, within a span of 70 minutes. Fifty-six people were killed and over 200 people were injured. Warnings of attacks were sent through e-mail. Several news agencies described about receiving a 14-page e-mail five minutes before the explosions with the subject line: "Await 5 minutes for the revenge of Gujarat." Investigators have got names of at least 40 other persons from across Gujarat, including Ahmedabad, who were engaged with the brothers regarding IS activities across the globe.[8]
- Terrorist groups like the Islamic State (ISIS), Lashkar-e-Taiba and the Taliban to name a few have been using social media and their digital publications to influence the youth and lure them towards so-called `jihad', says Yoana Barakova, a research analyst associated with Amsterdam-based the European Foundation for South Asian Studies (EFSAS).[9]

Covid-19- A phisherman's friend

Millions of professionals are at home and online, adapting to new routines and concerned about their work. That makes them perfect and apt to click on an e-mail which claims to come from their boss or from a supplier requesting a payment. Law enforcement officials in many countries have reported an increase in cybercrime since the start of the pandemic. Covid 19 pandemic extended the

[7] Wharton University Discussion ,Security Expert Amos Guiora: 'Cyber Terrorism Poses an Enormous Threat'(27june,2020,6:00), https://knowledge.wharton.upenn.edu/article/security-expert-amos-guiora-cyber-terrorism-poses-an-enormous-threat/

[8] Sarfaraz Sheikh, Gujarat terror suspects revealed names of 40 Islamic State operatives,(24 June,2020,19:00), https://economictimes.indiatimes.com/news/politics-and-nation/gujarat-terror-suspects-revealed-names-of-40-islamic-state-operatives-cops/articleshow/57387178.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[9] ANI, Terror Groups Using Digital Platforms To Promote `Jihad', Says EFSAS Researcher,(27june,2020 7:05),http://www.businessworld.in/article/Terror-Groups-Using-Digital-Platforms-To-Promote-Jihad-Says-EFSAS-Researcher/22-06-2020-289892/

network's security chain to its limits, with literally millions of potential weak links to be exploited by seasoned cybercriminals.

Some Recent Incidents

- German officials found that a Russian hacking group associated with the FSB had compromised the networks of energy, water, and power companies in Germany by exploiting IT supply chains. [10]
- Cyber criminals managed to steal $10 million from Norway's state investment fund in a business email compromise scam that tricked an employee into transferring money into an account controlled by the hackers.[11]
- Iranian hackers conducted a cyber-espionage campaign targeting air transportation and government actors in Kuwait and Saudi Arabia.
- U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. research into a coronavirus vaccine.

CONCLUSION

Hence to encapsulate, the reality is that criminals have changed their strategies and started hoping for advanced technology, therefore the enforcement authorities, businesses and non-public organizations should change their mechanism to bout it. Cyberterrorism is probably better perceived as an operational tactic aimed at a distinct psychological outcome rather than as a field of research that links the cyber domain at the hip to terrorism in real space. In particular, while cyberterrorism research and policy has become somewhat of a gridlock in recent years, people are taking its advantage to create fear in the minds of people. As quoted by Jeh Johnson, "Cybersecurity is a shared responsibility: In Cybersecurity, the more systems we secure, the more secure we are." The Internet is clearly changing the background of political discourse and advocacy. It offers new and inexpensive methods of collecting and publishing information, communicating and coordinating actions on a global scale and communicating with decision-makers. It supports open and private communications. Rights groups and

[10] Center for Strategic and International Studies (CSIS), (25,June,2020,12:00), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

[11] Center for Strategic and International Studies (CSIS), (25,June,2020,12:00), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

individuals around the world take advantage of these features to try to influence foreign policy. To control it, additional consultants should be given the necessary technical equipment and computer code so that they quickly combat cyber terrorists. The law cannot afford to be static; it must be changed with dynamic times as many applications of technology can be used for the welfare of mankind. Thus, the necessary facilities should be established in various components of the country so that crime in the virtual world can be controlled.