INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE PSYCHOLOGY OF CYBER TERRORIST - UNDERSTANDING MOTIVATION AND BEHAVIOUR

AUTHOR - ANKUR SHARMA* & DR. AISHWARYA PANDEY**

* STUDENT AT AMITY UNIVERSITY, LUCKNOW

** ASSISTANT PROFESSOR AT AMITY UNIVERSITY, LUCKNOW

BEST CITATION - ANKUR SHARMA & DR. AISHWARYA PANDEY, THE PSYCHOLOGY OF CYBER TERRORIST - UNDERSTANDING MOTIVATION AND BEHAVIOUR, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (8) OF 2025, PG. 96-99, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The study of the psychological aspect of cyber terrorists is a sensitive and broad subject that endeavours to uncover the causes of setting up cyber terrorists. The existing research in the field of cyber terrorism is further analyzed in this abstract concentrating on the psychological orientation of the cyber terrorists themselves including their reasons for the act, the manner they think and the behavioral characteristic they exhibit.

It is expectable that cyber terrorists act on basis of Sizes; Ideologies and & political reasons ; Money; Revenge[70]. These motivations are the same as those of traditional terrorists but done via the use of technology. Lives will be at stake; emotional wellbeing will be affected; those on the receiving end become stressed, anxious and feel insecure[71]. It is also worthy of note that cyber terrorists are intelligent, technical, and are usually associated with great risks. Furthermore, Both the narcissism, the need for acknowledgment or power may also contribute to their behaviours.

Knowledge of these psychological factors, therefore, is important if one has to come up with countermeasures and defenses against the problem. Understanding the psychological profile of cyber terrorists can therefore help officials design strategies to counter act threats from these groups. This abstract brings into perspective of the psychological perspectives that require integration to enhance the fight against cyber terrorism in the contemporary society.

Keywords : Cyber terrorist , Cyber terrorism , Radicalization , Psychological behaviour

[70] "The Psychology of Cybercriminals: Understanding Motivations and Behaviour by Grady Anderson & MoldStud Research Team"

[71]"Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes : *Journal of Cybersecurity*, Volume 3, Issue 1, March 2017, Pages 49–58"

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 8 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

INTRODUCTION

Imagine a person slumped in front of a computer in the pale light of the monitor, and he or she typing avidly, with intensity greater than simple inquisitiveness. This is not just any hacker; this is a cyberterrorist, who is motivated as much as he is dangerous. Nevertheless, what pushes a person to go from simple pranking to being a cyberterrorist? Which psychic elements do we have in front of us?

Picture a youth, one that is disillusioned or blinded by his own belief system or ideas on what the world is or should be. This person gain comfort and strength through cyberspace because they can control everyone even those who is far from them. The threat of cyberterrorism is not limited to disruption, but this is also something that provides a psychological mastery. It provides people with an opportunity to exert some amount of control, to express their rebellion against power to some extent, and to tell their grievances to power and the world.

Looking at the psyche of a cyberterrorist requires analyzing the actions and behaviour of a perpetrator. Are they doing it for political reasons, for religious reasons, or for a grudge? What role does the contingency of their background, experience, and psychological makeup play in their behaviour? Hence, addressing these questions will help to unravel a complex picture of factors underlying motivation to engage in cyberterrorism.

This adventure into the cunning of an antagonist is more than about threats, it is about the explicit human supermarket behind the screen. It's about the signs that can make one end up there and the means of dealing with them before turning into reality. In this endeavor, we hope to inform what lies at the root of the psychological perspectives of cyberterrorism, and advance knowledge that may be useful for making the digital sphere a safer space in the future.

ORIGINS OF CYBERTERRORISM: TRACING THE PATH TO RADICALIZATION

While there is no known direct route to becoming a cyberterrorist, it is very possible when one is already in the business and working in the background filled with discontent and disillusionment. To a myriad, the road map to extremism is well lit with woes, socio-economic challenges, and resource lessness apart from having no place in society. Sometimes such people may have a feeling that they are unwanted, isolated from their neighbors, or are victims of their country's political powers[72]. This list can make them inclined to consider the radical ideologies that offers them the feeling of participation and belonging.

The internet becomes a perfect breeding ground for radicalization where individuals are behind masks and easily convene to air their displeasures with the rest of society. Uncensored and secret social networks, blogs, forums and messenger applications become preaching places where extremism is promoted. Here people can argue that their opinion is right and that they should do something about it.

Radicalization is mostly a continuum over time with people moving through phases of adoption of radical messages, engagement in radical activities and/or ideologies and intensification of their activities and beliefs[73]. Such a process can be affected by numerous factors concerning personal experiences of the participants in unfair situations or witnessed violent actions, and the impact of inspiring leaders or recruiters who take advantage of respondents' weaknesses. Such recruiters are capable of inflicting psychological and emotional responses of people and creating

[72] "Qasemi, Hamid Reza (2016). "Chapter 12: Iran and Its Policy Against Terrorism". In Dawoody, Alexander R. (ed.). *Eradicating Terrorism from the Middle East*. Policy and Administrative Approaches. Vol. 17. Springer International Publishing Switzerland. p. 201 – 206"

[73] "Canetti, Daphna; Gross, Michael; Waismel-Manor, Israel; Levanon, Asaf; Cohen, Hagit (1 February 2017). "How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks". *Cyberpsychology, Behavior, and Social Networking*. **20** (2): 72–77"

narratives that make people join their teams and feel pressed for time[74].

To some people, the journey from mere cheerleader to actual actor in cyberterrorism stems from their own desire to exact vengeance or to exert some measure of influence in a universe that seems to them to be impersonal and beyond their control. The digital realm offers a unique appeal: that lets people hurt others in some way without physical contact being involved still gives people the feeling of power and having accomplished something, at least on their terms.

Explaining the development of cyberterrorism cannot be done without the help of representatives of psychology, sociology, and political science. As we map the process of radicalization[75], we can understand where to intercede and prevent a person from walking down that path, while at the same time reducing the frustration that has led to radicalization.

PSYCHOLOGICAL PROFILES: UNDERSTANDING THE CYBERTERRORIST MINDSET

In order to characteristic a cyberterrorist, one has to avert to understanding the different psychological factors that create independent motives and actions of a person that lead him towards performing cyber terrorism. Cyberterrorists' behaviour is rather specific compared to the broad array of criminal profiles familiar to law enforcement officers.

It is, however, important to point out that one of the characteristics that any of the cyberterrorists seem to possess is ideological hardness[76]. Regardless of if it is for political, religious or social reasons these people are usually utterly and completely convinced that they are in the right. This means this ideology passion can be used to give them a clear reason for their actions and the suffering that they may cause to other people.

There is another essential element of the worldview of a cyberterrorist – a person is isolated and does not have anyone to vote for. Most cyberterrorists holding this worldview, feel socially disadvantaged, they are secluded from mainstream society, they have suffered from injustice, they feel oppressed. It can lead to resentment and desire for revenge, and therefore they turn into workable for radicalization.

Also, cyberterrorists reveal good levels of skills in computing and demonstrate intellectual interest. Most of the time they are computer savvy experts in computer science and cybersecurity that fully grasp the technological environment. That technical skill not only allows them to conduct complex attacks but also gives them a way to stake a claim in a society they may otherwise feel they have no control over.

Moreover, the work of cyberterrorists may reflect their psychological patterns: they are narcissistic and demanding recognition. The Internet allows them to work without likely reprisal since their identities may not be known or discernible, and the worldwide sphere of their actions can make them feel important. This makes them seek to perform higher activities with the aim of proving the outputs of the earlier actions they carried out so that they can gain recognition.

PREVENTIVE MEASURES: ADDRESSING THE ROOT CAUSES AND MITIGATING RISKS OF CYBERTERRORISM

The prevention and correction to cyberterrorism are rooted, and mitigate the risk for them are a multi-faceted approach. Here are some key strategies:

Preventive Measures

1. Education and Awareness: Preventing cyberterrorism can be done by educating the public and organizations to the risks of attacks, and teaching them best practices to ensure that their systems are secure. Second of all,

[74] "Iqbal, Mohammad. "Defining Cyberterrorism". *The John Marshall Journal of Information Technology & Privacy Law*. **22** (2): 397–408"
[75]"Anderson, Kent (13 October 2010). "Virtual Hostage: Cyber terrorism and politically motivated computer crime". The Prague Post"
[76] "Worth, Robert (25 June 2016). "Terror on the Internet: The New Arena, The New Challenges". New York Times Book Review: 21"

employees need regular training on spotting phishing attempts, and other such cyber threats.

2. Robust Cybersecurity Infrastructure: One easy means to secure systems against unauthorized access is thru implementing strong cybersecurity methods that include firewalls, encryption routines as well as multi factor authorization[77].

3. Legislation and Policy: In doing so, governments can legislate within the law and the regulation that compels organizations to observe pointed and strict requirements for cybersecurity[78]. Mandatory reporting of cyber incidents and reasonable security audits[1] are included.

4. International Cooperation: The problem of cyberterrorism is a global issue and it is critical that we work as a global community. Indicating and mitigating threats more effectively is a function of sharing intelligence and best practices among countries.

5. Addressing Socio-Economic Factors: By reducing the pool of potential cyberterrorists[79], you tackle the underlying socio – economic issues that may have caused people to become cyber terrorists such as poverty and lack of education.

Corrective Measures

1. Incident Response Plans: Incident response plans are all about fixing things after they go wrong.

2. Regular Audits and Assessments: Running regular security audits and vulnerability assessments allows us to detect and close up potential holes before they are taken advantage of.

3. Recovery and Remediation: After that, it is important to have mechanisms in place in order to restore data and recover systems after an attack. That is, making backups and having disaster recovery plans[80].

4. Continuous Monitoring: The real time detection and response of suspicious activities is possible through the implementation of continuous monitoring systems[81].

CONCLUSION & SUGGESTION

Our increasingly digital world is a threat of cyberterrorism. Critical infrastructure remains vulnerable to terrorist exploitation, terrorists and extremists can use the internet to spread propaganda, and coordinate attacks online. To counter cyberterrorism, governments and organizations should:

1. Strengthen resilience of critical systems, as well as cybersecurity.

2. It improves the information sharing between public and private sectors.

3. Increase detection and response ability

4. Build the international cooperation on the cybercrime

5. Cyber education and workforce development – invest.

To avoid becoming involved in cyberterrorism:

1. Check online information and propaganda.

2. Be suspicious of online behaviour and report it to authorities

3. Be good at practicing good cybersecurity habits

4. Don't interact with extremist content or extremist groups online.

5. Instead of finding people and communities that promote violence, look for those that provide positive ways.

[77] " Centre of Excellence Defence Against Terrorism (2008). Responses to Cyber Terrorism. Amsterdam"
[78] "The Current State of Cyber Security in India". Kratikal Blogs"
[79] "Softness, Nicole (Winter 2016). "Terrorist Communications: Are Facebook, Twitter, and Google Responsible for the Islamic State's Actions?". Journal of International Affairs. 70: 201–215 – via EBSCOhost"
[80] "Cyberpsychology, Behavior, and Social Networking". Cyberpsychology, Behavior, and Social Networking"
[81]" William L. Tafoya, Ph.D., "Cyber Terror", FBI Law Enforcement Bulletin (FBI.gov)"