

RADICALIZATION AND RECRUITMENT ON THE INTERNET: CONFRONTING THE WHOLE OF SOCIETY APPROACH

*Camilo Graziani**

I. INTRODUCTION

Terrorist organizations systematically and globally exploit youth, especially those subjected to social vulnerability. This exploration represents an important contemporary criminal justice challenge. States and their institutions must reassess their traditional strategies for confronting terrorism in the face of this modern challenge. Contemporary terrorist organizations have developed an incredible understanding of the social vulnerability of young people, have developed sophisticated strategies to exploit these vulnerabilities and have been very successful in radicalizing and recruiting young people to their causes. To successfully address the exploitation of youth by terrorist organizations, according to Neumann (2023), States must focus on the root causes of the problem, especially on stabilizing the lives of young people and strengthening protective factors, such as family, education, and community ties.

II. COUNTER-TERRORISM IN BRAZIL: CURRENT DYNAMICS, CHALLENGES AND STRATEGIC RESPONSES

Brazil's counter-terrorism approach reflects a sophisticated understanding of the transnational nature of contemporary terrorist threats. Despite not having experienced direct terrorist attacks on its soil, the country has developed a proactive strategy focused on prevention, intelligence gathering, and international cooperation. The Federal Police's Division for Combating Terrorism (DETER) plays a central role in monitoring and mitigating potential terrorist risks.

The Brazilian counter-terrorism model demonstrates several good practices:

- a. Legal Framework:** Law 13.260/2016 provides a comprehensive legal basis for identifying and prosecuting terrorist activities, enabling a structured approach to threat management.
- b. International Cooperation:** Brazil actively participates in global anti-terrorism networks, sharing intelligence and maintaining alignment with UN Security Council resolutions regarding recognized terrorist organizations.
- c. Multifaceted Intelligence Strategy:** DETER employs a holistic approach, monitoring not only direct terrorist activities but also related criminal domains such as money-laundering, document fraud and clandestine immigration.
- d. Cyber Monitoring:** Recognizing the digital nature of modern radicalization, Brazilian authorities have developed capabilities to track online recruitment and extremist content dissemination.

However, there are significant challenges that complicate Brazil's counter-terrorism efforts:

- a. Online Radicalization:** The increasing vulnerability of young Brazilians to online extremist content represents a critical challenge for preventive strategies.

* Commissioner of Police, Head of the Counter-Terrorism Division, Brazilian Federal Police, Brazil.

- b. Diverse Threat Landscape:** Brazil must monitor multiple terrorist groups with different motivational backgrounds, from religiously motivated organizations like ISIS and Hezbollah to ideologically driven violent extremist movements.
- c. Migration Dynamics:** Humanitarian visa policies, particularly those related to conflict zones like Afghanistan, create potential vulnerabilities in border control and terrorist infiltration.
- d. Limited Historical Experience:** The relative absence of direct terrorist attacks can potentially lead to complacency in threat perception and preparedness.

In order to address these challenges, Brazil may consider some strategic countermeasures:

- a. Enhanced Digital Deradicalization Programmes:** Develop comprehensive educational and psychological intervention strategies targeting potential online recruitment vulnerabilities.
- b. Technological Intelligence Upgrades:** Continuously invest in advanced technological capabilities for digital surveillance and threat detection.
- c. Interdisciplinary Training:** Create specialized training programmes for law enforcement and intelligence personnel that integrate psychological, sociological and technological perspectives on counter-terrorism.
- d. Community Engagement:** Develop robust community-level programmes that promote social inclusion, intercultural dialogue and early identification of potential radicalization indicators.

Summing up, Brazil's counter-terrorism strategy demonstrates a nuanced, proactive approach that balances preventive intelligence, legal frameworks and international cooperation. By continuously adapting to the evolving global terrorist landscape, the country can effectively mitigate potential risks while maintaining its commitment to democratic principles and human rights.

III. RECENT TRENDS IN YOUTH TERRORIST RECRUITMENT

The reality of recruitment for terrorist purposes has evolved significantly in recent years. Contemporary terrorist organizations have operated simultaneously in the physical and virtual domains, but with great emphasis on the latter. These organizations today have a massive virtual presence, where they can easily propagate their ideas, ideologies and narratives. This propaganda especially targets young individuals, with personality, character and values still in formation, searching for identity, purpose and belonging.

As Selim (2022) notes: "Preventing the next generation of recruits for terrorism has become more important than ever. A generation ago, individuals may have been radicalized by members of their local communities over several years; Now, while this is still happening, it is much more common to self-radicalize online."

Contemporary terrorist organizations are at an increasing level of sophistication when it comes to recruiting young people, sometimes adopting age-specific approaches. In this segmentation, preference is given to pre-adolescents and adolescents, in whom developmental vulnerabilities are explored.

Regarding the reality of the physical territory, traditional recruitment continues in conflict zones, educational institutions, schools, community centres, family environments and other social circles such as scout youth groups (in relation to the latter environment, it is found that it has been frequently used by Hezbollah in southern Brazil, where there is a significant Lebanese Shiite community).

In the virtual environment, the Internet and social media have become the preferred stage for terrorist groups to disseminate their ideals, ideas and narratives. The internet has become the main environment for communicating ideas, radicalization, recruitment and inspiring attacks by small groups or even lone actors

(lone wolves). According to Gonçalves and Reis (2023), in the information age, the Internet serves as a precondition for terrorism.

IV. PREVENTIVE APPROACHES AND SOLUTIONS

Strategies to confront and prevent this phenomenon of radicalization and terrorist recruitment do not only involve public security. Strong public security, intelligence-based, interagency and international cooperation are important, and the response of states to this phenomenon is essential. The discovery of the sources of radicalization, the means used and the investigation and arrest of recruiters and radicalizers are essential from the point of view of disruption and deterrence. But the solution cannot be limited to public security. The solution must be the product of a holistic and integrative whole-of-state and whole-of-society approach that should focus on the root causes of the problem.

A. Educational Intervention

Education is a key pillar in tackling terrorist radicalization and recruitment targeting young people. Quality education during childhood and adolescence builds strong and lasting values and prevents the influence of radical and extremist worldviews. In addition, quality education develops independent and critical thinking, gives a better cultural and historical understanding to young people, and develops the capacity for resilience against radical and extremist narratives.

In addition, not only schools but the family and community around young people must be involved in the education process. Priority should be given to the establishment, maintenance and strengthening of relevant family ties. The family should also be aware of the types of friendships and relationships maintained by its young members and should encourage healthy relationships. Finally, a sense of belonging to that society and to that group must be developed in young people so that they do not feel isolated and are attracted to radical and extremist groups, which also maliciously exploit this sense of belonging.

B. Digital Counterstrategy

Allied to the pillar of education, states must develop their own and effective strategies to confront radicalization and terrorist recruitment on the Internet. These strategies must consider the peculiarities of each country. Nevertheless, they can be based on the strategy developed by the European Union, which is quite comprehensive and useful. This strategy emphasizes:

1. Mechanisms for the early detection and identification of:
 - i) Risk behaviours;
 - ii) Radical ideological narratives;
 - iii) Online recruitment standards.
2. Preventive Monitoring through the implementation of:
 - i) Social media surveillance systems;
 - ii) Content filtering mechanisms;
 - iii) Information campaigns and counter-narratives.

V. MITIGATION STRATEGIES

Also based on the European Union's "Strategy to Combat Radicalization and Recruitment for Terrorism", in addition to technological detection and monitoring mechanisms, effective responses to these phenomena

must include a social support system, with the implementation of family support programmes, community engagement initiatives and projects to train young people for work.

While the social support pillar is the family, the school, and the community, which play an essential role in relation to the virtual environment, technology companies also play a fundamental role. Digital platforms must have responsibility for content moderation and the protection of their users and must develop and make available educational resources for responsible use of the Internet and offensive or harmful content. In addition, technology companies should engage in collaborative initiatives to develop monitoring systems, unified response protocols, proactive collaboration with law enforcement agencies, and removal of offensive, disinformation, extremist and violent content.

VI. DIGITAL RADICALIZATION AND RECRUITMENT: A CASE STUDY OF JUVENILE VULNERABILITY TO ISLAMIC STATE EXTREMISM IN BRAZIL

The case of Fábio Samuel provides a compelling analysis of digital radicalization processes and the challenges of preventing youth involvement in terrorist organizations. In mid-2023, Brazilian counter-terrorism authorities apprehended Samuel while attempting to depart from Guarulhos Airport in São Paulo, with the explicit intention of joining the Islamic State (IS).

The investigation, conducted by the Specialized Counterterrorism Division (DETER) in collaboration with the Federal Bureau of Investigation (FBI), emerged from an intelligence-driven approach that spanned approximately one year. The investigation transitioned from intelligence gathering to a formal police investigation, revealing Samuel's direct communications with terrorist group members and systematic online recruitment strategies.

Samuel employed sophisticated digital recruitment techniques targeting adolescents through multiple social media platforms, including WhatsApp, Telegram and Discord.

His recruitment strategy involved:

- i) Sharing extremist Islamic State propaganda;
- ii) Distributing violent multimedia content;
- iii) Discussing potential terrorist attack plans;
- iv) Positioning himself as a religious mentor.

Investigative evidence included:

- i) Social media group postings related to the Islamic State;
- ii) Travel planning communications;
- iii) Video recordings expressing intent to work with the terrorist organization;
- iv) One-way ticket purchase to Istanbul.

In 2022, DETER conducted an early intervention with Samuel, then a minor, involving:

- i) Personal interviews;
- ii) Counselling;
- iii) Family guidance;

- iv) Social service involvement;
- v) Psychological support.

Despite this comprehensive, multidisciplinary approach, the intervention failed to interrupt Samuel's radicalization trajectory. The judicial process recognized the Islamic State as an internationally condemned terrorist organization. Samuel was ultimately convicted of promoting terrorism and the corruption of minors. He was sentenced to eight years of imprisonment, highlighting the legal system's response to digital terrorist recruitment.

This case illuminates critical challenges in contemporary counter-terrorism efforts, specifically:

- i) The vulnerability of adolescents to online extremist ideologies;
- ii) Limitations of current deradicalization strategies;
- iii) The sophisticated nature of digital terrorist recruitment.

Samuel's case represents a significant example of how terrorist organizations leverage digital platforms to target and radicalize vulnerable youth. The case demonstrates the complex landscape of digital radicalization, revealing the vulnerabilities of young individuals to extremist ideologies and the limitations of current deradicalization strategies in Brazil. It underscores the urgent need for more effective prevention and intervention strategies.

VII. CONCLUSION

Confronting the radicalization and recruitment of young people by terrorist organizations requires states and society to have holistic and multifaceted strategies beyond the traditional and limited approach of public security and law enforcement. This confrontation requires the involvement of the whole society in a true whole-of-society approach, which provides for preventive measures, focused especially on quality education, strong family ties and the development of a sense of belonging of young people to the community that surrounds them. In addition, states, in partnership with technology companies, must develop robust systems for detecting, monitoring, cooperating and disseminating effective counter-narratives. Only through this comprehensive approach will we be able to confront and counter the sophisticated strategies of radicalization and terrorist recruitment aimed at our youths. When all these tools fail, then criminal law must be applied and those involved must suffer the consequences of the law.

References

- Aly, A. (2023). "Social Media and Radicalization: Understanding Active Audiences." *Journal of Terrorism Studies*, 16(2), 178-195.
- European Union. (2005). "The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism." EU Counter-Terrorism Strategy Document.
- Gonçalves, R., & Reis, M. (2023). "Internet as a Pre-condition for Modern Terrorism." *International Security Review*, 12(4), 267-284.
- Matos, H. (2023). "Preventive Monitoring in Counter-terrorism Strategy." *Security Studies Quarterly*, 28(3), 145-162.
- Neumann, P. (2023). "Youth Work in Preventing Violent Extremism." *Counter-Terrorism Studies*, 19(1), 89-106.
- Selim, G. (2022). "Evolution of Online Radicalization Processes." *Journal of Digital Security*, 15(4), 223-241.