SECURITY COUNCIL

TOPIC A: Technology and terrorist groups

In times of global crises, whether triggered by conflict, natural disasters, or pandemics, an often-overlooked yet pervasive issue emerges: gender-based violence (GBV). This insidious form of violence, rooted in deeply ingrained gender stereotypes and power imbalances, disproportionately affects women and girls but can impact individuals of all genders.

Technology has two fundamentally different perspectives when it comes to conflict: first, as an instrument of terror, and, then, as a means of preventing and responding to acts of terror. Specific technologies are described in both parts. For terrorists, technology is involved in both the means of terror, including weapons of mass destruction and use of the Internet, and the targets of terror, including technological infrastructure targets. Technology can be a critical tool in counterterrorism too, through smart identification systems, sophisticated technologies for intelligence gathering and analysis, and the use of the Internet as a bridge builder to reduce tensions that can lead to terrorism.

Terrorists fight their conflicts in cyberspaces as well as on the ground. An example of a branch of technology terrorist groups use is the Internet. By exploiting the unregulated, anonymous, and easily accessible nature of the Internet to target an array of messages to a variety of audiences. Most recently, terror groups have begun employing drones and Artificial Intelligence (AI). Both can be harnessed to respond effectively to multiple security challenges, terrorists have deployed drones to attack state military assets, diplomatic sites, international trade, energy infrastructure, and civilian centers. State sponsorship of terrorist groups has also helped increase the number of drone attacks.

Governments' worldwide will also face a significant national security threat in adversarial use of small, unmanned aircraft systems (SUAS). Technology to produce swarms represents a multi-layered and unmanageable new threat. On the same parameter, AI has the potential to be abused by terrorists to recruit, spread hatred and support their insurgencies. Technology has already shown to have long-term societal implications.

Drones and AI will continue to evolve. Therefore, it is imperative that we deepen our understanding of how terrorists are harnessing technologies to increase their power in both the physical and psychological domains. The focus should not only be on disruption but also prevention, and the responsibility to act must be shared across government agencies, academic institutions and technology companies. We are finding ourselves in the trenches of an increasingly widening digital war and we have not yet mastered how to escape it while terrorist digitalis is marching ahead.

1. How can we limit terrorist access to dual-use technologies like drones and AI?
2. What steps can prevent terrorist recruitment and propaganda online?

3. How can governments and tech companies counter drone threats from terrorists?
4. How can AI improve counter-terrorism without harming privacy?
5. What can be done to protect infrastructure from cyberterrorism?

https://gnet-research.org/2024/07/04/the-digital-weaponry-of-radicalisation-ai-and-the-recruitment-nexus/

https://thesoufancenter.org/intelbrief-2024-october-3/

https://gnet-research.org/

https://www.gcsp.ch/publications/terrorist-digitalis-preventing-terrorists-using-emerging-technologies

https://thebulletin.org/2023/12/terrorists-are-using-consumer-drones-and-its-getting-harder-to-stop-them/