Artificial Intelligence and the Future of Terrorism

By Daniel Byman and V.S. Subrahmanian

KEY TAKEAWAYS

This brief outlines how artificial intelligence (AI) may shape terrorism and counterterrorism. AI is likely to reinforce and accelerate existing informational and operational trends and capabilities of terrorism rather than revolutionizing terrorist capabilities. At the same time, AI can strengthen state counterterrorism capacity, but some measures involve risks to civil liberties.

In response to the new capabilities that AI will afford terrorism and counterterrorism, democratic societies must undertake the following actions:

- Develop institutional and public safeguards, including independent audits of companies and robust civil liberty protections.
- Improve public-private cooperation in service of counterterrorism.
- Engage in continuous monitoring and reappraisal of rapidly expanding AI capabilities, especially in the biotechnology realm.

BACKGROUND AND CONTEXT

Terrorist groups have begun to integrate AI technologies into their operations and organizations. AI integration enables groups to cheaply produce multilingual and personalized propaganda, including through the use of deepfakes. These groups may also use chatbots as virtual mentors to push isolated individuals toward violence. Operationally, AI use can improve and streamline weapons design and production and attack planning.

Nevertheless, the effects of AI on terrorist functions are likely to be cumulative rather than revolutionary. The potential that AI poses to radically revolutionize terrorist capabilities—such as through chemical, biological, radiological, and nuclear terrorism—is currently limited, although it bears constant scrutiny. Despite the spread of AI, substantial logistical barriers to catastrophic attacks, including the need for labs and access to dangerous materials, remain. Moreover, most groups are usually not incentivized to engage in such attacks. AI has begun—and will continue—to augment state counterterrorist capabilities through improved data analysis of finances, travel, surveillance data, and social media.

LEGISLATIVE AND POLICY IMPLICATIONS

Congress has discussed how to tackle the growing terrorist use of AI. In March 2025, Congressman August Pfluger (R-TX), chairman of the House Homeland Security Subcommittee on Counterterrorism and Intelligence, both introduced legislation and facilitated a hearing to examine how foreign terrorist organizations employ emerging technology, including generative AI (GenAI) applications.

Rep. Pfluger's bill, the Generative AI Terrorism Risk Assessment Act, would require the Department of Homeland Security, in coordination with the Director of National Intelligence, to conduct annual assessments on terrorism threats to the homeland that include the use of GenAI.

Since this bill unanimously passed the House and has been received by the Senate, Congress is well positioned to take a leading role in ensuring that government agencies are thoroughly conducting assessments and using those assessments to develop strategies for future terror attacks that employ GenAI.

As AI continues to evolve and become increasingly accessible, it will be imperative for Congress to think through additional ways to counter terrorist organizations that may creatively manipulate and exploit existing emerging technologies. It will also be vital for Congress to ensure that national security agencies use AI without infringing on the civil liberties of Americans.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

CHALLENGES AND RISKS

Roadblocks to strengthening U.S. capabilities include:

- The reluctance of many AI companies to ensure robust guardrails on AI systems
- Absence of a clear framework and expectations for AI companies about sharing information with the government on terrorist groups and other threats
- The willingness of Iran, Russia, and other hostile countries to bolster terrorist groups and radical actors, possibly sharing AI expertise with them
- Limited AI knowledge in many national security agencies

RECOMMENDATIONS

New AI-enabled counterterrorism capabilities demand careful consideration of safeguards to protect civil liberties and prevent unjust profiling. The United States should consider the following actions:

1. Require independent auditing of claims and risk-mitigation procedures made by the companies involved.
2. Improve public-private coordination to take advantage of the expertise and capabilities embedded in technology companies
3. Give sustained attention to chemical and biological risks.
4. Require transparent oversight and accountability mechanisms for companies to ensure reduced risk.

Additional Resources and Contact Information

Daniel Byman and V.S. Subrahmanian, "Artificial Intelligence and the Future of Terrorism," CSIS, *CSIS Briefs*, July 10, 2026, https://www.csis.org/analysis/artificial-intelligence-and-future-terrorism.

Research for this project is a collaborative effort between CSIS and Northwestern University.

For more information, contact **Chloe Himmel** at 202.775.3186 or **chimmel@csis.org**.