



THE
SOUFAN
CENTER

TSC INSIGHTS

Terrorist Misuse of AI:

A Framework
for U.S.-PRC
Cooperation

Authored by
**Mollie Saltskog &
Clara Broekaert**

September 2026

Table of Contents

Introduction	4
Counterterrorism Priorities in the People’s Republic of China	5
Counterterrorism Priorities in the United States	8
Challenges to U.S.-China AI Cooperation	10
Observed Terrorist Misuse of AI	12
Anticipated Exploitation of AI Systems	14
Axis 1: Informational and operational exploitation – Lower Risk, Higher Probability	14
Axis 2: Anticipatory CBRN concerns – Higher Risk, Lower Probability	15
Axis 3: Cross-cutting concerns	16
Cooperation Framework on Countering the Terrorist Misuse of AI	16
Pillar 1: Working Group on Mitigating Terrorist Misuse of AI	18
Pillar 2: CBRN Cooperation, Beginning with Nucleic Acid Synthesis Screening	19
Pillar 3: Track II Dialogue to explore U.S.–PRC AI Risk Reduction of Terrorist Misuse	19
Pillar 4: Parallel Threat Taxonomies and Crosswalk	20
Pillar 5: Incident Information Sharing Mechanism	21
Acknowledgements	22

Introduction

Both Beijing and Washington have acknowledged the urgent imperative of ensuring artificial intelligence (AI) systems are not exploited by non-state actors, including for terrorist purposes. During the Trump-Xi Summit in Beijing on May 14–15, 2026, U.S. Treasury Secretary Scott Bessent stated that the People's Republic of China (PRC) and the United States would “set up a protocol” on “best practices for A.I. to make sure non-state actors don't get a hold of these models.”¹ Following Trump's state visit to the PRC, the Chinese Ministry of Foreign Affairs confirmed this nascent cooperation: “During President Trump's visit to China, the two heads of state had constructive exchanges on artificial intelligence and agreed to carry out an intergovernmental dialogue on artificial intelligence.”²

The pace of technological innovation and the emergence of new AI models, coupled with a lack of clear, uniform guardrails, are increasing the risk of AI misuse by non-state actors. The increasing sophistication, relatively low cost, and wide availability of frontier AI models are lowering the barrier to entry for non-state actors seeking to misuse the emerging technology. While the term “non-state actors” can encompass everything from cyber-criminals to transnational criminal organizations, an immediate and acute priority should be to mitigate the misuse of AI by violent non-state actors (VNSAs). And among VNSAs, terrorists merit first priority. In the U.S.–PRC context, this specific non-state threat is an area where the two states' interests are aligned, with both Beijing and Washington continuing to recognize the Islamic State (IS), al-Qaeda (AQ), and their global affiliates as an immediate threat to global security and stability as well as national security.

AI safety frameworks, domestic laws, and remarks by PRC and U.S. officials in domestic and international fora indicate that both states see significant risk in terrorists adopting and exploiting AI capabilities.³ For cooperation purposes, terrorist exploitation of AI is understood narrowly: it consists of the malicious use or repurposing of any AI system, whether proprietary or open-source, to plan, facilitate, finance, incite, or execute acts of terrorism. The enclosed evidence and recommendations align with such concerns, including the Chemical, Biological, Radiological, and Nuclear (CBRN) uplift they may provide.

While there are many challenges to Beijing and Washington arriving at a broader AI cooperation framework, on the issue of cooperation against AI misuse by terrorists, the positive signals from the Trump-Xi Summit in Beijing earlier this year bode well for both countries' willingness to come together on this issue for the benefit of the international community. As Brookings Fellow and China expert Kyle Chan has written: “As the world's two AI superpowers, the United States and China have a unique capacity and responsibility for mitigating the potential risks from AI use by non-state actors.”⁴ Nothing would be more pressing, or signal more goodwill to the world, than a cooperation framework to mitigate the risk of terrorists misusing AI.

This is neither unprecedented nor unrealistic, as the U.S. and PRC have established bilateral working groups to address security issues before. For example, the U.S.-PRC Counternarcotics Working Group (CNWG) emerged from the Biden-Xi summit in November 2023. While momentum later slowed, Trump and Xi agreed during their 2025 meeting in South Korea on a bilateral consensus on fentanyl and curbing precursor chemicals.

On a separate track, law enforcement cooperation has intensified. A counternarcotics working group has formed as part of a law enforcement exchange between the Federal Bureau of Investigation (FBI) and the Ministry of Public Security (MPS). Working groups now exist on cyber fraud, violent crimes against

1. Evelyn Cheng, “U.S. can hold AI talks with China, Bessent tells CNBC as nations plan safety protocol,” CNBC, May 14, 2026, <https://www.cnbc.com/2026/05/14/us-china-ai-rules-bessent-us-lead.html>.

2. “China, U.S. agree on intergovernmental dialogue on AI,” State Council of the People's Republic of China, May 19, 2026, https://english.www.gov.cn/news/202605/19/content_WS6a0c2a5ec6d00ca5f9a0b169.html.

3. Zhang Jun, “Remarks by Ambassador Zhang Jun at the UN Security Council Briefing on Artificial Intelligence: Opportunities and Risks for International Peace and Security” (remarks, UN Security Council, New York, July 18, 2023), Permanent Mission of the People's Republic of China to the UN, https://un.china-mission.gov.cn/eng/hyyfy/202307/t20230719_11114947.htm; Generative AI Terrorism Risk Assessment Act, H.R. 1736, 119th Congress (2025), <https://www.congress.gov/bill/119th-congress/house-bill/1736>.

4. Kyle Chan et al., “AI risks from non-state actors,” Brookings, January 29, 2026, <https://www.brookings.edu/articles/ai-risks-from-non-state-actors/>.

children, counternarcotics, and fugitives.⁵ Current FBI Director Kash Patel, in July 2026, met with Minister of Public Security Wang Xiaohong, appearing to commit to working on shared issues such as drugs, online fraud, and anti-money laundering. Under Patel, cooperation with MPS has included Chinese officials visiting multiple FBI facilities to work on these shared issues.

While this law enforcement cooperation is promising, cooperation on AI misuse by terrorist organizations requires a different logic than that for other issues such as counternarcotics, which can be regulated and conceivably stopped. The distributed, largely intangible nature of AI systems poses a different set of challenges.

Realistic cooperation to counter AI misuse by terrorist organizations, such as a bilateral consensus, understanding, or framework, need not serve as a steppingstone to or a negotiating tactic for broader U.S.-PRC AI cooperation.⁶ Instead, it should be designed as a narrowly scoped cooperation framework focused on mitigating risks to shared security interests, with practical, technical, and operational implementation to prevent terrorists from harnessing AI for financial, operational, recruitment, and other malign purposes. Such a narrowly scoped principle was agreed on before. In 2024, both sides took an important first step in agreeing that humans, rather than AI, should make decisions regarding the use of nuclear weapons.⁷ Nonetheless, this was a leader-to-leader political commitment that has remained a principle rather than being enshrined in any working group or institutional entity.

The AI safety field, while still focused on catastrophic risk, has started to treat non-state actor misuse as a distinct problem. The Safe AI Forum convened the International Dialogues on AI Safety in London in April 2026, bringing together technical experts on malicious misuse by non-state actors. The Brookings–Tsinghua Track II dialogue has approached the non-state actor misuse issue from a national security perspective, and evaluation work is underway at the UK AI Security Institute, Concordia AI, and elsewhere, including the Oxford Artificial Intelligence Governance Initiative and among sovereign AI consortia.

Designing a cooperation framework on preventing terrorist misuse of AI would require an understanding of PRC and U.S. counterterrorism priorities, including their differences, to ensure the framework does not run afoul of U.S. priorities and values. This would also require technical and expert knowledge of how terrorists use AI today, how they may use it tomorrow, and the threat posed to the U.S., China, and the international community. Such subject-matter expert knowledge is necessary to design technically sound and operationally feasible cooperation and mitigation mechanisms that are both actionable and durable. It will also be important to design such a framework with the inherent challenges of the broader U.S.-PRC AI cooperation environment in mind, so as not to create something too ambitious that risks becoming a mechanism for political posturing in future negotiations or dialogues.

It would be a win for Trump, Xi, the United States, the PRC, and the whole international community if the Trump–Xi meeting in Washington, D.C., on September 24, 2026, produced a common understanding or even a draft framework for cooperation to counter AI misuse by violent non-state actors, such as terrorist organizations.

Counterterrorism Priorities in the People’s Republic of China

Ambassador Fu Cong, China’s Permanent Representative to the United Nations, most recently set out the PRC’s counterterrorism priorities in July 2026. While Fu warned against the “politicization and instrumentalization” of counterterrorism, he also strongly underscored the need to enhance global counterterrorism capabilities, strengthen cooperation on intelligence sharing, and continue building consensus on combating terrorism. He also singled out terrorist abuse of emerging technologies for “propaganda, incitement, recruitment, financing and the planning of terrorist attacks,” urging to “build forward-looking defenses against terrorism.”⁸

5. Jana Winter, “Under Patel, FBI forges unprecedented law enforcement ties with China, Russia,” Reuters, August 5, 2026, <https://www.reuters.com/world/china/under-patel-fbi-forges-unprecedented-law-enforcement-ties-with-china-russia-2026-08-05/>.

6. Mark MacCarthy and Carl Schonander, “How the US and China can cooperate to reduce urgent AI risks,” Brookings, July 14, 2026, <https://www.brookings.edu/articles/how-the-us-and-china-can-cooperate-to-reduce-urgent-ai-risks/>.

7. Jarrett Renshaw and Trevor Hunnicutt, “Biden, Xi agreed that humans not AI should control nuclear weapons,” Reuters, November 17, 2024, <https://www.reuters.com/world/biden-xi-agreed-that-humans-not-ai-should-control-nuclear-weapons-white-house-2024-11-16/>.

8. Fu Cong, “Statement by Ambassador Fu Cong at the General Assembly Debate on the Ninth Review of the United Nations Global

Fu had sketched the threat landscape as seen from the PRC in greater detail at a United Nations Office of Counter-Terrorism event, where in April 2026 he underlined the terrorist use of emerging technologies, including AI.⁹ He laid out Beijing's view of the main terrorist threats: the East Turkestan Islamic Movement/Turkistan Islamic Party (ETIM/TIP); groups with branches globally like al-Qaeda (AQ) and Islamic State; and regional groups like Tehrik-e-Taliban Pakistan (TTP) and the Balochistan Liberation Army (BLA).

PRC ties concerns about ETIM/TIP to Afghanistan since the Taliban takeover in 2021 and the fall of Bashar al-Assad's regime in Syria in 2024, which saw many Uyghur fighters becoming integrated into Syrian armed forces, with others remaining outside the fold of the new state apparatus.¹⁰ The group sits at the core of Beijing's counterterrorism priorities, which are rooted in its "three evil forces" framework of terrorism, separatism, and extremism.¹¹ Beijing also claims that ETIM continues to operate in Xinjiang, which the CCP has used to justify draconian security measures and mass surveillance, incarceration, and prosecution of Muslim minorities. In 2020, the U.S. State Department noted it had "seen no credible evidence for more than a decade that the group still exists and removed ETIM from the Terrorist Exclusion List in November."¹² This removal of ETIM was met with harsh criticism from the PRC.

Fu also called out the expanding threats in "regions such as West and Central Africa, South Asia, and Central Asia." The callout to South and Central Asia likely references regional branches such as Islamic State Khorasan Province (IS-K), which continues to explicitly threaten the PRC in its propaganda materials.¹³ The TTP and the BLA, both active in and around Pakistan, have also become counterterrorism priorities for the PRC. Both groups have targeted Chinese nationals and economic interests, casting a shadow over the China-Pakistan Economic Corridor (CPEC).¹⁴ PRC diplomats at the UN have called for the Security Council to list the BLA under the 1267 regime.¹⁵ China's concern with this group aligns with the U.S., which designated it as a Foreign Terrorist Organization (FTO) in August 2025. However, the U.S. does not see sufficient evidence linking the BLA to IS and AQ, making the 1267 regime, in Washington's view, inapplicable.¹⁶ As in Central and South Asia, Chinese economic and geopolitical interests on the African continent are also

Counter-Terrorism Strategy," Permanent Mission of the People's Republic of China to the United Nations, July 2, 2026, https://un-china-mission.gov.cn/eng/dbttx_141670/czdbzjds/fcdshd/202607/t20260707_11976483.htm.

9. Fu Cong, "Remarks by China's Permanent Representative to the UN Ambassador Fu Cong at the UNOCT-Pakistan Joint Event on New and Emerging Trends in Terrorism" (remarks, UNOCT-Pakistan Joint Event, New York, April 24, 2026), Ministry of Foreign Affairs of the People's Republic of China, https://www.fmprc.gov.cn/eng/xw/zwbdt/202605/t20260506_11905196.html.

10. *Thirty-Seventh Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2734 (2024) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities* (United Nations Security Council, February 3, 2026), <https://docs.un.org/en/S/2026/44>; Mollie Saltskog and Colin P. Clarke, "It's China's Turn to Face Transnational Terrorism Threats," *Defense One*, April 21, 2025, <https://www.defenseone.com/ideas/2025/04/its-chinas-turn-face-transnational-terrorism-threats/404689/>; United Nations Security Council, *Thirty-Eighth Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities*, UN Doc. S/2026/651, August 10, 2026, 3, <https://undocs.org/S/2026/651>.

11. Zamir Ahmed Awan, "China's Successful Experience of Overcoming Terrorism: A Model for Global Peace and Development," *People's Daily Online*, July 7, 2025, <https://en.people.cn/n3/2025/0707/c98649-20336762.html>.

12. U.S. State Department, "Country Reports on Terrorism 2020: China (Hong Kong and Macau)," *U.S. Department of State*, <https://www.state.gov/reports/country-reports-on-terrorism-2020/china/>.

13. Lucas Webber et al., "The Historical Evolution of the Islamic State's Anti-China Propaganda," *CTC Sentinel* 19, no. 7 (July 2026): 17, <https://ctc.westpoint.edu/the-historical-evolution-of-the-islamic-states-anti-china-propaganda/>.

14. Neeraj Singh Manhas, "Amid Geopolitical Tensions, Baloch Militant Attacks Undermine Sino-Pakistan Projects," *Terrorism Monitor* 23, no. 4 (2025), <https://jamestown.org/amid-geopolitical-tensions-baloch-militant-attacks-undermine-sino-pakistan-projects/>; Amira Jadoon and Colin P. Clarke, "The War on Iran Has a Balochistan Problem," *East Asia Forum*, May 31, 2026, <https://easiasiaforum.org/2026/05/30/the-war-on-iran-has-a-balochistan-problem/>.

15. The UNSC Resolution 1267 established a sanctions regime in 1999 to target the Taliban, al-Qaeda, and later ISIS. The UNSC Resolution 2713 established a sanctions regime targeting al-Shabaab in Somalia. Geng Shuang, "Remarks on Threats to International Peace and Security Caused by Terrorist Acts by Ambassador Geng Shuang at the UN Security Council Briefing," Permanent Mission of the People's Republic of China to the UN, https://un.china-mission.gov.cn/eng/hyyfy/202508/t20250821_11693453.htm; Sun Lei, "Remarks by Ambassador Sun Lei at the Security Council Meeting on Threats to International Peace and Security Caused by Terrorist Acts," Permanent Mission of the People's Republic of China to the UN, February 4, 2026, https://un.china-mission.gov.cn/eng/chinaandun/securitycouncil/202602/t20260205_11851411.htm. Note: 1267 covers Islamic State and Al-Qaeda affiliates and 2713 covers Al-Shabaab – it is unclear how such sanction regime would apply to BLA.

16. "Terrorist Designation of The Majeed Brigade," U.S. Department of State, August 11, 2025, <https://www.state.gov/releases/office-of-the-spokesperson/2025/08/terrorist-designation-of-the-majeed-brigade/>; Pranab Dhal Samanta, "US, UK and France block Pakistan-China move at UN to list BLA, Majeed Brigade as terror groups," *Economic Times*, September 19, 2025, <https://economic-times.indiatimes.com/news/international/world-news/us-uk-and-france-block-pakistan-china-move-at-un-to-list-bla-majeed-brigade-as-terror-groups>.

exposed to the burgeoning terrorism threat there, the region with the most terrorism-related deaths.¹⁷ Multiple attacks by al-Qaeda and Islamic State affiliates against Chinese nationals involved in economic projects on the African continent have occurred, prompting an increasingly assertive counterterrorism approach by the PRC there.¹⁸

It is important to acknowledge that the PRC's main concerns as it relates to AI safety appear to be regime stability. As exemplified in a recent article by the Minister of State Security, Chen Yixin, where the top risk identified is how AI "Systemically affects the political security environment."¹⁹ Other risks identified in the piece include AI's impact on cybersecurity, espionage, and military capabilities. There are also serious safety risks of Chinese models that the PRC does not publicly acknowledge. As Ryan Fedasiuk, an expert on AI and U.S.-PRC relations, notes: "Beijing, meanwhile, erected stringent controls on training data and model outputs — but these measures were principally designed to protect political stability rather than personal or national security. Even as it began requiring developers to censor politically inconvenient content under regulations like TC260, Beijing has generally refused to concede the serious safety deficits of Chinese models, preferring instead to look the other way as Western researchers succeeded in jailbreaking DeepSeek to produce bioweapons or help with offensive cyber operations."²⁰

However, in addition to the aforementioned statements by PRC officials at the UN, Beijing has also articulated its concerns about terrorist exploitation of AI systems in various AI safety governance frameworks and technical documents. Frontier models are of particular concern in the Chemical, Biological, Radiological, and Nuclear (CBRN) domain, while AI more broadly is framed as a concern for producing and disseminating terrorist content. CBRN applications appear more present in official documents and align with the fact that low-probability, high-impact risks continue to dominate the AI safety debate.

The PRC's AI Safety Governance Framework 2.0, released in September 2025, included an explicit warning that terrorists may be able to acquire relevant knowledge about the design of such weapons, calling for the "exclusion of sensitive training data in high-risk fields such as nuclear, biological, and chemical weapons and missiles."²¹ That same framework stated that AI systems can additionally be used to "spread content related to terrorism, extremism, and organized crimes." Framework 3.0, released on September 14, 2026, has significantly elevated the CBRN issue set. The PRC no longer defines weapons knowledge as merely a problem of training data but also one of access, cautioning against the "loss of control over knowledge related to nuclear, biological, chemical, and missile weapons." The newly updated framework states that AI "significantly lowers the threshold for accessing specialized knowledge" in those fields, and warns that, combined with retrieval-augmented generation, these capabilities may be maliciously exploited by "criminals, extremist groups, or terrorists."²² While it previously argued for filtering the training data of models to exclude such knowledge, it now also speaks of access controls: "Controls at the source should be strengthened through user authentication, identification of intended use, and other measures to prevent AI from being used in high-risk scenarios such as the manufacture of nuclear, biological, chemical, and missile weapons."²³

Framework 2.0 framed open-source and open-weight model safety risk as related to model defect prop-

17. Christopher Faulkner, and Raphael Parens, "Shaping the Security Landscape: How Russia and China Approach the Issue of Security in Africa," Delphi Global Research Center, April 6, 2026, <https://delphigrc.org/research/shaping-the-security-landscape-how-russia-and-china-approach-the-issue-of-security-in-africa>; Institute for Economics & Peace, *Global Terrorism Index 2026: Measuring the Impact of Terrorism* (Institute for Economics & Peace, March 2026), <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf>.

18. Cobus Van Staden, "Chinese Counterterrorism in Africa," Stimson, July 31, 2024, <https://www.stimson.org/2024/chinese-counterterrorism-in-africa/>; Jason Warner, "Understanding China's New Counterterrorism Ambitions in Africa," *CTC Sentinel* 18, no. 8 (2025): 20–31, <https://ctc.westpoint.edu/understanding-chinas-new-counterterrorism-ambitions-in-africa/>.

19. Chen Yixin, "Comprehensively Fortify the AI Security Barrier and Promote the Healthy and Orderly Development of AI," China Cyberspace, translated by ChatGPT and edited by Sinocism, <https://sinocism.notion.site/Chen-Yixin-Comprehensively-Fortify-the-AI-Security-Barrier-and-Promote-the-Healthy-and-Orderly-Deve-3da84ece41d7816c9720eef8aef74cc1>

20. Ryan Fedasiuk, "AI Coordination Without Illusion," American Enterprise Institute, May 7, 2026, <https://www.aei.org/commentary/ai-coordination-without-illusion/>

21. AI Safety Governance Framework 2.0, https://www.cac.gov.cn/2025-09/15/c_1759653448369123.htm.

22. AI Safety Governance Framework 3.0, 69, <https://www.tc260.org.cn/tc260/xwdt1/202609/e879077a3caa4722b2206d1bcaed5a6c.shtml>.

23. AI Safety Governance Framework 3.0, 82.

agation, eventually making it easier for criminals to train “malicious models.”²⁴ The response was thus seen as a post-release issue to be dealt with by developers. Framework 3.0 now frames it as a misuse risk, stating that “safety mechanisms may be removed, weakened, or bypassed, and global updates and repairs cannot be achieved.”²⁵ Interestingly, it shifts responsibility also to open-source providers and communities around misuse, tasking them with the “responsibility and obligation to inform users downloading models of potential risks,” and to “clearly define prohibited actions for downloading and using open-source models, in order to prevent misuse or malicious use.”²⁶ This is not a restriction on open release at all – pivotal to the PRC’s AI strategy. Nonetheless, it does acknowledge risk related to misuse of open-weight and open-source models.

This is consistent with China’s dominance in open-weight models, a deliberate strategy that challenges U.S. AI dominance and bypasses hardware export controls imposed by Washington. Interestingly, the framework also highlights the risk posed by “addiction and dependence on anthropomorphic interaction.” While this is not expressly tied to terrorism, real-world cases have shown that such personal bot dependence and violent, ideologically inspired acts can go hand in hand.²⁷ In July 2026, China’s interim measures for the administration of AI anthropomorphic interaction services, issued jointly by the Cyberspace Administration of China (CAC), the National Development and Reform Commission (NDRC), Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), and State Administration for Market Regulation (SAMR), came into effect. In preparation, Chinese AI providers ByteDance and Alibaba moved to disable customized agent features in their *Doubao* and *Qwen* products.²⁸ Beijing’s most explicit articulation of the imperative to stop terrorist misuse of AI also came in July 2026. The Chair’s Statement at the World Artificial Intelligence Conference called for participants to “jointly prevent and fight against the abuse and malicious use of AI technologies by terrorist and extremist forces, and transnational organized criminal groups, and establish necessary crisis management and emergency response mechanisms on a global scale.”²⁹

Counterterrorism Priorities in the United States

The most recent U.S. Counterterrorism Strategy, released in May 2026, identifies three priorities: narco-terrorism and transnational gangs, legacy Islamist terrorists, and violent left-wing extremists, including antifascists and anarchists.³⁰

The U.S. counterterrorism apparatus currently focuses on incapacitating the operations of drug cartels and other transnational criminal organizations that have a footprint in the U.S. homeland. Since 2025, drug cartels like Sinaloa, Jalisco New Generation Cartel (CJNG), and Tren de Aragua have been designated as FTOs, as have gangs in Haiti like Viv Ansanm and Gran Grif.³¹ Operation Southern Spear, launched by the current administration to kinetically interdict illegal narcotics and drug traffickers, has struck dozens of vessels in the Caribbean Sea and Eastern Pacific Ocean — a departure from the previous law enforcement-led counternarcotics strategy.³² Additionally, the U.S. operation Absolute Resolve, which captured

24. AI Safety Governance Framework 2.0.

25. AI Safety Governance Framework 3.0, 55.

26. AI Safety Governance Framework 3.0, 92.

27. Priyank Mathur et al., “The Radicalization (and Counter-Radicalization) Potential of Artificial Intelligence,” International Centre for Counter-Terrorism, May 1, 2024, <https://icct.nl/publication/radicalization-and-counter-radicalization-potential-artificial-intelligence>.

28. Wendy Chen, “ByteDance and Alibaba to disable humanlike AI custom agents as new rules loom,” *South China Morning Post*, July 5, 2026, <https://www.scmp.com/tech/big-tech/article/3359482/bytedance-and-alibaba-disable-humanlike-ai-custom-agents-new-rules-loom>.

29. “Chair’s Statement of the 2026 World Artificial Intelligence Conference & High-Level Meeting on Global AI Governance,” July 17, 2026, Permanent Mission of the People’s Republic of China to the United Nations, https://un.china-mission.gov.cn/eng/zgyw/202607/t20260717_11984715.htm.

30. White House, *U.S. Counterterrorism Strategy*, May 2026, <https://www.whitehouse.gov/wp-content/uploads/2026/05/2026-USCT-Strategy-1.pdf>.

31. “Designation of International Cartels,” U.S. Department of State, February 20, 2025, <https://www.state.gov/designation-of-international-cartels>; Marco Rubio, “Terrorist Designations of Viv Ansanm and Gran Grif,” press statement, U.S. Department of State, May 2, 2025, <https://www.state.gov/releases/office-of-the-spokesperson/2025/05/terrorist-designations-of-viv-ansanm-and-gran-grif>.

32. Lead Inspector General, *Operation Southern Spear: Lead Inspector General Report to the United States Congress, January 1, 2026–March 31, 2026* (Department of War Office of Inspector General, May 21, 2026), https://media.defense.gov/2026/May/21/2003935694/-1/-1/1/OSS_Q2_MAR2026_FINAL_508.PDF.

the de facto leader of Venezuela and alleged head of *Cartel de los Soles*³³ Nicolás Maduro, has been presented as a law enforcement operation related to charges of narcoterrorism, conspiracy to import cocaine, and weapons possession.³⁴ The United States additionally continues to target Salafi-Jihadist and other Islamist militant groups in kinetic strikes. The U.S. has executed strikes against the Houthis during Operation Rough Rider in 2025,³⁵ as well as various IS and AQ branches in Syria, Iraq, and Somalia.³⁶ It also appears that the U.S. is executing an unacknowledged campaign against al-Qaeda in the Arabian Peninsula (AQAP) in Yemen.³⁷ In Africa, it has targeted Islamic State West Africa Province (ISWAP) in strike campaigns carried out with the Nigerian Armed Forces.³⁸ It is also contemplating strikes against al-Qaeda affiliate Jama'at Nusrat al-Islam wal-Muslimeen (JNIM) in Mali.³⁹

The 2026 U.S. counterterrorism strategy notes that terrorist actors may misuse AI and other emerging technologies.⁴⁰ A 2023 Executive Order already defined “dual-use foundation models” by their potential for catastrophic misuse, including “substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons.”⁴¹ While President Donald Trump rescinded this executive order, the concern is also expressed in his *America's AI Action Plan* released in 2025, which states that AI “could create new pathways for malicious actors to synthesize harmful pathogens and other biomolecules” and strengthens nucleic acid synthesis screening as a mitigation measure — requiring institutions receiving federal research funding “to use nucleic acid synthesis tools and synthesis providers that have robust nucleic acid sequence screening and customer verification procedures.”⁴² It also calls for developers to evaluate frontier AI in coordination with the Center for AI Standards and Innovation, though these remain voluntary commitments.

The U.S. Department of Homeland Security (DHS) has similarly warned that advanced AI is already of interest to terrorists of various ideological leanings, with both foreign and domestic violent extremists (DVEs) having shown interest in using “DNA modification to develop biological weapons to target specific groups.”⁴³ However, beyond catastrophic risks related to the potential exploitation of AI models to support the development of chemical or biological agents, other sub-catastrophic risks have also been articulated. For example, FTOs and DVEs have attempted to leverage AI technologies to improve their operations, recruitment methods, and communications. Concerns expressed by different agencies, including DHS and FBI, are thus not just about AI-enabled terrorist attacks but all upstream phases: operational planning, providing technical expertise, and expanding the digital footprint of their cause through AI-translated propaganda.⁴⁴

33. While *Cartel de los Soles* was designated an FTO by Treasury Department in 2025, the Department of Justice in 2026 referred to it as a patronage system that has facilitated widespread drug trafficking rather than a formal organization. See: Charlie Savage, “Justice Dept. Drops Claim That Venezuela’s ‘Cartel de los Soles’ Is an Actual Group,” *New York Times*, January 5, 2026, <https://www.nytimes.com/2026/01/05/us/trump-venezuela-drug-cartel-de-los-soles.html>.

34. Expressing the Sense of the Senate in Support of Operation Absolute Resolve, S. Res. 582, 119th Cong. (2026), <https://www.congress.gov/119/bills/sres/582/BILLS-119sres582is.pdf>.

35. “U.S. Attacks Houthi, Sends Signal to Iran,” IntelBrief, The Soufan Center, March 17, 2025, <https://thesoufancenter.org/intel-brief-2025-march-17/>.

36. US Africa Command. “U.S. Forces Conduct Strikes Targeting al-Shabaab.” Press release, July 13, 2026. <https://www.africom.mil/pressrelease/36755/us-forces-conduct-strikes-targeting-al-shabaab>; U.S. Central Command (@CENTCOM), “CENTCOM Forces Kill ISIS Chief of Global Operations Who Also Served as ISIS #2,” X, March 14, 2025, <https://x.com/CENTCOM/status/1900737395915440260>; “US Military Says Senior Islamic State Group Leader Killed in Syria Air Strike,” France 24, June 24, 2026, <https://www.france24.com/en/middle-east/20260624-us-military-says-senior-islamic-state-group-leader-killed-syria-air-strike>.

37. David Stermann, “Is the U.S. Conducting Air Strikes Against Al Qaeda in Yemen?” *Just Security*, February 12, 2026, <https://www.justsecurity.org/129392/us-airstrikes-alqaeda-yemen/>.

38. Chris Gordon, “US Hits ISIS in Nigeria as Pentagon Steps Up Counterterrorism Campaign,” *Air & Space Forces Magazine*, May 19, 2026, <https://www.airandspaceforces.com/us-strikes-isis-nigeria-africa-counterterrorism-campaign/>.

39. Silja Fröhlich, “Could U.S. airstrikes stop insurgency in Mali?” DW, July 28, 2026, <https://www.dw.com/en/could-us-airstrikes-stop-insurgency-in-mali/a-78141641>.

40. White House, *U.S. Counterterrorism Strategy*.

41. Executive Order No. 14,110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75,191 (Nov. 1, 2023), <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>.

42. White House, *Winning the Race: America's AI Action Plan* (White House, July 2025), 3, <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.

43. U.S. Department of Homeland Security, *Homeland Threat Assessment 2025* (U.S. Department of Homeland Security, 2024), 4, https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-ha-final-30sep24-508.pdf.

44. U.S. Department of Homeland Security, *Homeland Threat Assessment 2025; Worldwide Threats to the Homeland: Hearing Before the H. Comm. on Homeland Security*, 119th Cong. (2025) (statement of Michael Glasheen, Operations Director, National

The clearest congressional articulation of concern over terrorist exploitation of artificial intelligence since January 2025 is the Generative AI Terrorism Risk Assessment Act. The bill passed the House in November 2025 and would require the Secretary of Homeland Security, in consultation with the Office of the Director of National Intelligence, to conduct annual assessments for five years on threats to the United States posed by the use of generative AI in terrorism.⁴⁵ This includes an analysis of incidents in the preceding calendar year in which a group or individual used or attempted to use the technology to spread terrorist messaging, radicalize and recruit to violence, or enhance their capacity to develop and deploy CBRN weapons. As passed by the House, the bill is behavior-based, not just covering designated groups but also unaffiliated individuals who use generative AI models for the purpose of terrorism. A Senate companion bill is currently pending.

Both Chinese and U.S. frameworks, remarks, and legislation clearly indicate a two-pronged concern regarding AI and terrorism: AI-enabled propaganda, radicalization, and operational planning on the one hand, and anticipatory concern over CBRN capability uplift on the other.

These sections, showing both PRC and U.S. counterterrorism priorities, indicate that the narrow overlap concern is the uplift AI may provide to Islamic State, al-Qaeda, and their affiliates. This should be the analytical basis for scoping a cooperation framework around terrorist misuse of AI.

Challenges to U.S.-China AI Cooperation

AI has become the frontier of U.S.-PRC strategic competition. Washington and Beijing seek to harness AI to drive economic prosperity, military capability, technological innovation, and strategic influence — with the notion that the state that wins the global AI race will have a clear advantage as the dominant power in the 21st Century.

Applying AI to the strategic competition between the U.S. and PRC inherently complicates cooperation. In 2025, the Trump White House published “America’s AI Action Plan,” which stated: “The United States is in a race to achieve global dominance in artificial intelligence (AI). Whoever has the largest AI ecosystem will set global AI standards and reap broad economic and military benefits.”⁴⁶ The Chinese Communist Party (CCP) has emphasized the need for China to become “the world’s primary AI innovation center,”⁴⁷ to “seize the commanding heights of science and technological development,”⁴⁸ and to “resolutely win the battle over key and core technologies.”⁴⁹ On July 17, 2026, Xi Jinping opened the World Artificial Intelligence Conference in Shanghai, saying: “The development of artificial intelligence should not be a solo performance by any single country but rather a symphony of international cooperation,” signaling that Beijing also sees AI as a key diplomatic and geopolitical tool.⁵⁰

Differences in governance and regulatory models create additional barriers for cooperation. The PRC and the United States have fundamentally different political and institutional systems, which translates into different approaches to governance — including technology governance. The result is differences in data governance, transparency, oversight, and verification, which inherently complicates any AI governance and cooperation mechanism between the two. The PRC’s AI Safety Governance Framework 3.0 techni-

Security Branch, FBI), <https://www.fbi.gov/news/speeches-and-testimony/worldwide-threats-to-the-homeland-121125>.

45. Generative AI Terrorism Risk Assessment Act, H.R. 1736, 119th Cong. (2025), <https://www.congress.gov/bill/119th-congress/house-bill/1736/text>.

46. White House, *Winning the AI Race: America’s AI Action Plan* (Washington, DC: The White House, July 2025), 4, <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.

47. State Council of the People’s Republic of China, “New Generation Artificial Intelligence Development Plan” (新一代人工智能发展规划), July 20, 2017, trans. Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo, DigiChina, Stanford University, August 1, 2017, <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>.

48. *Outline of the 15th Five-Year Plan (2026–2030) for National Economic and Social Development of the People’s Republic of China*, trans. Mandarin Peel, *Mandarin Peel* (Substack newsletter), March 26, 2026, <https://mandarinpeel.substack.com/p/chinas-15th-five-year-plan-full-english>.

49. Xi Jinping, speech at the joint session of the 20th General Assembly of the Chinese Academy of Sciences, the 15th General Assembly of the Chinese Academy of Engineering, and the 10th National Congress of the China Association for Science and Technology, Beijing, May 28, 2021, trans. Zichen Wang, *Pekingnology* (newsletter), June 8, 2021, <https://www.pekingnology.com/p/xi-jinpings-speech-on-science-and->

50. Xi Jinping. “Joining Hands to Build a Just and Equitable System for Global AI Governance.” Keynote address at the opening ceremony of the 2026 World AI Conference and High-Level Meeting on Global AI Governance, Shanghai, July 17, 2026. *China Daily*, July 17, 2026. <https://www.chinadaily.com.cn/a/202607/17/WS6a5a35b7a310986e2b465eb8.html>.

cally carries no legal force, and its closest American counterpart, the National Institute of Standards and Technology (NIST) risk management framework, is also voluntary.⁵¹ In practice, Framework 3.0 calls for AI safety legislation to be “advanced,” and its risk-grading appendix is written to help establish industry-specific rules.⁵²

Chinese providers whose services may affect public opinion must pass a security assessment and file their algorithms with the Cyberspace Administration.⁵³

In the United States, Executive Order 14409 “Promoting Advanced Artificial Intelligence Innovation and Security,” signed in June 2026, establishes a voluntary framework in which frontier model developers can grant federal agencies access to their models before release to assess advanced cyber capabilities. As seen in June 2026, model releases are also managed through other, nonvoluntary instruments. The Bureau of Industry and Security used export controls to suspend access to Anthropic’s Fable 5 and Mythos 5 by any foreign national. As Anthropic could not reliably screen users by nationality, it disabled both models. The export controls were lifted 19 days after, with access restored to Fable but Mythos 5 access restricted to approved U.S. users.⁵⁴

The military-technology competition between the United States and the PRC is another area that complicates AI cooperation between the two countries. Since he came to power, Xi Jinping has articulated the goal of transforming the People’s Liberation Army (PLA) into a “world-class military” by 2049. This includes military modernization with integrated “intelligentization” — integrating AI and other emerging technologies into operational capabilities.⁵⁵ The PRC’s military-civil fusion (MCF) strategy is a key component to aid this goal, seeking to break down barriers between the private sector, academia, research and technology, and the PLA, enabling the latter to employ any dual-use industries and technologies for military advancements and capabilities development.⁵⁶ This has raised concerns of PRC-enabled cyberespionage, intellectual property theft, and the illegal transfer of dual-use technologies from private sector and research institutions in other countries. Simultaneously, the U.S. has instituted export controls and technological decoupling in the name of protecting national security and preventing unauthorized technology transfer. Beijing sees such action as efforts to kneecap its technological advancement and contain China’s rise to a global power. This mistrust and mismatch of goals was evident in the May 2024 U.S.–PRC AI talks in Geneva, where the issue of AI cooperation veered into export controls and other political issues.⁵⁷

The military-technology competition between Washington and Beijing is frequently framed in existential or zero-sum terms, with some experts drawing parallels to the 1940s nuclear weapons race. This intensifying competition in military AI applications has raised legitimate concerns about the world’s two major powers falling into the spiral model. As *Army of None* author Paul Scharre aptly pointed out: “During periods of disruptive technological change, what determines a military’s relative success is how well it employs new technology.”⁵⁸ Integrating AI into military applications could lead to miscalculation and escalation in conflict. The lack of transparency, guardrails, and ethical considerations in AI development further complicates any cooperation efforts. And the lack of an international framework governing AI — as opposed to how the world decided to govern other technology with the prospect of human annihilation,

51. Matt Sheehan and Scott Singer, “How China Views AI Risks and What to Do About Them,” October 16, 2025, Carnegie Endowment, <https://carnegieendowment.org/research/2025/10/how-china-views-ai-risks-and-what-to-do-about-them>.

52. AI Safety Governance Framework 3.0, 85, 111–12.

53. Provisions on the Security Assessment of Internet Information Services That Have Public Opinion Properties or the Capacity for Social Mobilization [具有舆论属性或社会动员能力的互联网信息服务安全评估规定] (promulgated Nov. 15, 2018, effective Nov. 30, 2018), trans. China Law Translate, <https://www.chinalawtranslate.com/en/provisions-on-the-security-assessment-of-internet-information-services-that-have-public-opinion-properties-or-the-capacity-for-social-mobilization/>.

54. Siladitya Ray, “U.S. Lifts Restrictions On Anthropic’s Mythos 5 And Fable 5 AI Models,” *Forbes*, July 1, 2026, <https://www.forbes.com/sites/siladityaray/2026/07/01/trump-administration-lifts-export-controls-on-anthropics-mythos-5-and-fable-5-ai-models/>.

55. “Annual Report to Congress: Military and Security Developments Involving The People’s Republic of China,” *U.S. Department of Defense*, <https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF>.

56. “IntelBrief: China’s Military-Civil Fusion Strategy,” *The Soufan Center*, August 13, 2020, <https://thesoufancenter.org/intelbrief-chinas-military-civil-fusion-strategy/>.

57. Jamey Keaten and Kelvin Chan, “In First AI Dialogue, US Cites ‘Misuse’ of AI by China, Beijing Protests Washington’s Restrictions,” Associated Press, May 15, 2024, <https://apnews.com/article/artificial-intelligence-china-united-states-biden-xi-geneva-506da7b-5fa72d5fe1bcd54fb8ec4f898>.

58. Paul Scharre, “Losing the War of the Future: How New Technologies Threaten America’s Military Advantage,” *Foreign Affairs*, July/August 2026, <https://www.foreignaffairs.com/united-states/losing-war-future-paul-scharre>.

like nuclear weapons — could increase mistrust and uncertainty and even lead to conflict. Lt Gen. (Ret.) Jack Shanahan noted “The United States and China are neck-and-neck in the adoption of AI across their economies and national security ecosystems. Historically, such rough parity was stabilizing rather than destabilizing. This is not the case with AI.”

The main differences between the 1940s and today’s competition for AI supremacy are the actors that lead the race (top-secret military projects versus private sector companies) and the barriers to entry: building a nuclear bomb is still a highly difficult endeavor requiring vast resources and technical expertise, whereas frontier AI models, open-source models, and real-world applications can spread globally after launch. Development of a nuclear weapon is also detectable and, once developed, expensive and difficult to maintain. During the nuclear arms race, there were self-imposed, practical, and agreed-to limits by the major parties involved. Despite competition and mistrust in other areas of AI development and co-operation between the two countries, given that AI is cheaper, easier to produce, more amorphous, and provides more agency to more actors, including terrorists, than nuclear weapons, there is a significant incentive for the U.S. and the PRC to agree to selectively cooperate on shared AI risk, especially terrorist misuse of AI.

While the authors acknowledge the many challenges — ranging from mistrust to the ongoing competition for AI supremacy — to Beijing and Washington arriving at an AI cooperation framework on the issue of AI misuse by terrorist actors, the positive signals from the Trump-Xi Summit in Beijing earlier this year hopefully bode well for both countries’ willingness to come together on this issue for the benefit of the international community.

Observed Terrorist Misuse of AI

Terrorist groups and radicalized individuals have leveraged generative AI across different terrorism-related operations. The following section focuses on abuses by al-Qaeda and Islamic State, including their affiliates, and the individuals inspired by them. Nonetheless, terrorists across the ideological kaleidoscope have used AI systems in their operational planning, including on U.S. soil.⁵⁹ Most recently, a September 2026 report by Anthropic details how the Houthis sought to use Claude to develop advanced guided missiles.⁶⁰ Terrorist misuse and uplift are not the same. Instead, terrorist misuse occurs along a spectrum: access to a model, a model complying with a malicious request, a model reproducing an answer that other information sources already provide, a model supplying novel information and removing a bottleneck (i.e., uplift), adoption of the output of the model by the actor, to effect, where an operation causes harm because of terrorist misuse of AI.

In June 2025, Islamic State Khorasan Province (IS-K), a terrorist group with a dense history of targeting both U.S. and Chinese interests and calling for violence against the two countries and their nationals, published an endorsement for the use of AI through its *Voice of Khorasan* magazine — the most explicit call for the use of AI by a Salafi-Jihadist group’s flagship media foundation so far.⁶¹ While the article did not elaborate on how such models may be used for operational planning or specific recruitment workflows, it signaled an early organizational-level endorsement of appropriating the technology.⁶² Observed abuses by Islamic State, al-Qaeda, and inspired individuals span multiple categories:

Propaganda, translation, recruitment

AI-generated content has appeared in the sprawling ecosystem of supporter accounts and unofficial media foundations that populate al-Qaeda and Islamic State’s Rocket.Chat servers, pastebin websites, chat

59. Clara Broekaert and Lucas Webber, “AI Use in Terrorist Plots and Attacks Surges in 2025,” *Militant Wire*, December 23, 2025, <https://www.militantwire.com/p/ai-use-in-terrorist-plots-and-attacks>.

60. Jon Gambrell and Abby Sewell, “Users in Houthi-Held Yemen Tried to Develop Advanced Weapons with AI, Anthropic Says,” Associated Press, September 11, 2026, <https://apnews.com/article/yemen-houthis-anthropic-ai-missiles-9b20934e031ff3d99dd8bb49d-85d97a9>

61. Clara Broekaert and Colin P. Clarke, “The Pandemonium Narrative and Its Limits: Artificial Intelligence and the Islamic State’s Innovation Pattern,” *Current Trends in Islamist Ideology*, Hudson Institute, May 11, 2026, <https://www.hudson.org/terrorism/pandemonium-narrative-its-limits-artificial-intelligence-islamic-states-innovation-clara-broekaret-colin-p-clarke>.

62. Much of the *Voice of Khorasan* issue, including the June 2025 article on AI, is flagged as AI-generated by AI detection tool Pangram.

platforms, and mainstream social media platform footholds.⁶³ Many of these supporters, particularly in the case of Islamic State, are increasingly young and have adopted the aesthetics more typically associated with the extreme right.⁶⁴ AI-generated content production aligns with this trend of aesthetic appropriation and has produced a flood of meme-like propaganda videos often accompanied by *anasheed* (“chants”).

Islamic State supporters have shown early experimentation with generative AI: there was the *News Harvest* series, AI-generated dispatches styled as a news broadcast in the aftermath of IS-K’s Crocus City Hall massacre in March 2024. Two months later, after the Bamiyan attack in Afghanistan, a similar AI-generated broadcast called the “Khurasan TV” segment claimed responsibility.⁶⁵ These early experiments with AI sparked conversations about the technology’s doctrinal permissibility and the display of an unmasked AI-generated face, leading to blurred anchors’ faces in later *News Harvest* clips.

AI-assisted translation of propaganda materials has also been observed and is a relevant application for the efficiency thesis of AI adoption by terrorist groups: AI-assisted propaganda translation can, at speed and scale, produce linguistically and culturally apt outputs, thereby directly reducing the friction of rendering Arabic materials into the languages of al-Qaeda and Islamic State target audiences. For the Islamic State, the apparatus that manages the translation funnel to target audiences is *Fursan al-Tarjuma* (“Knights of Translation”), a supporter umbrella translation foundation formed in March 2023.⁶⁶ AI-enabled translation and text-to-speech functions can further reduce friction.⁶⁷ This use of AI is likely to produce compounding returns, with each language’s content translated at speed, potentially recruiting more sympathizers. This is relevant in regions with linguistic diversity where Islamic State and al-Qaeda branches operate, providing a way to reach new individuals to conduct acts of terrorism independently.

It is unclear to what extent AI-assisted content production has led to demonstrable increases in audience size, recruitment success, or pathways to violence. Nonetheless, various cases have already clearly shown that AI can facilitate, or itself be, a radicalization vector.⁶⁸ In sum, AI systems have lowered the cost of producing appealing, tailored, multilingual content, and even a modest improvement in appeal or a handful of additional translations could expand reach and recruit individuals to the movement, with an outsized effect if they commit violence.

Operational planning: from ideation to execution

Open-source analysis of digital ecosystems has shown that supporters are interested in using generative AI models for operational planning, including ideation, technical know-how, and attack execution.⁶⁹ Additionally, plots by Islamic State-inspired individuals who leveraged AI for operational questions have been noted globally. In April 2025, an eighteen-year-old inspired by the Islamic State was arrested in Vienna in connection with a plot and was found to possess ChatGPT logs about the production and storage of explosives.⁷⁰ In May 2025, two Bangladeshi-Italians inspired by the Islamic State were arrested in Palermo, Italy, for the glorification of terrorism and the threat of an imminent, concrete act of violence. One

63. Tech Against Terrorism, *Early Terrorist Experimentation with Generative Artificial Intelligence Services*, briefing (Tech Against Terrorism, November 2023), 5, <https://techagainstterrorism.org/hubfs/Tech%20Against%20Terrorism%20Briefing%20-%20Early%20terrorist%20experimentation%20with%20generative%20artificial%20intelligence%20services.pdf>.

64. Moustafa Ayad, “An ‘Alt-Jihad’ Is Rising on Social Media,” *Wired*, December 8, 2021, <https://www.wired.com/story/alt-jihad-rising-social-media/>.

65. Mona Thakkar and Anne Speckhard, *Caliphate AI: IS/ISKP Supporters Harness Generative AI for Propaganda Dissemination* (International Center for the Study of Violent Extremism, 2024), <https://icsve.org/caliphate-ai-is-iskp-supporters-harness-generative-ai-for-propaganda-dissemination>.

66. Lucas Webber and Daniele Garofalo, “Fursan al-Tarjuma Carries the Torch of Islamic State’s Media Jihad,” GNET, June 5, 2023, <https://gnet-research.org/2023/06/05/fursan-al-tarjuma-carries-the-torch-of-islamic-states-media-jihad/>.

67. Alessandro Bolpagni and Eleonora Ristuccia, “AI-Powered Translation: How AI Tools Could Shape a New Frontier of IS Propaganda Dissemination,” GNET, July 9, 2025, <https://gnet-research.org/2025/07/09/ai-powered-translation-how-ai-tools-could-shape-a-new-frontier-of-is-propaganda-dissemination/>.

68. Priyank Mathur et al., “The Radicalization (and Counter-Radicalization) Potential of Artificial Intelligence,” International Centre for Counter-Terrorism, May 1, 2024, <https://icct.nl/publication/radicalization-and-counter-radicalization-potential-artificial-intelligence>.

69. Clara Broekaert and Colin P. Clarke, “The Pandemonium Narrative and Its Limits.”

70. Austria Presse Agentur, “Wiener IS-Anhänger besprach Bombenbauen mit ChatGPT” [Viennese Islamic State supporter discussed bomb making with ChatGPT], *Salzburger Nachrichten*, August 31, 2025, <https://www.sn.at/politik/innenpolitik/wiener-is-anhaenger-besprach-bombenbauen-mit-chatgpt-art-613233>.

of the individuals had used a generative AI model to determine the best way to hit someone to paralyze them.⁷¹ In May 2026, a 27-year-old Tunisian man in Paris was found to have used ChatGPT to research how to make a bomb.⁷² In India, a member of the cell charged over the November 2025 Delhi Red Fort car bombing used YouTube and ChatGPT to research building rocket-type IEDs (but there is no public evidence whether this was used in the attack).⁷³ These instances indicate that lone actors increasingly seek guidance and technical know-how from generative AI models for operational planning, beyond ideating online on supporter forums. It is unclear how much uplift they experience and whether, in the above cases, the model complied with all the user requests. This is nonetheless credible: Tech Against Terrorism's counterterrorism AI benchmark shows that models, when processing a prompt that is framed as benign 'research', complied at high rates with malicious requests related to terrorism.⁷⁴ AI has also featured in directed plots. In November 2025, a failed medical doctor in India who was in contact with IS-K was arrested and had apparently used both Google and ChatGPT for instructions on how to produce ricin.⁷⁵

The use of AI for operational purposes is not limited to inspired and directed plots. Designated terrorist groups have adopted AI and institutionalized its use.⁷⁶ The two factions that emerged after Boko Haram's split in 2016, Islamic State West Africa Province (ISWAP) and Jama'atu Ahlis Sunna Lidda'awati wal-Jihad (JAS), appear to have established dedicated AI units that deploy frontier models such as ChatGPT, Grok, Claude, and DeepSeek. According to former Boko Haram fighters, foreign IS operatives trained ISWAP in person on such use and supplied them with laptops with VPNs and encryption software, as well as paid accounts through intermediaries.⁷⁷ ISWAP members also received advice from these operatives on prompting the models to receive answers to their requests. Operational uses of AI have included weapons identification and troubleshooting, IED design, drone weaponization, attack planning, force allocation, and operational security. This indicates that a substantial AI adoption campaign has been underway in ISWAP — and, given what appears to be the top-down involvement of foreign IS operatives, likely in other IS provinces as well. While this does not prove uplift, the apparent persistent and institutionalized nature of adoption suggests it is perceived as yielding significant benefits to the group. Official IS messaging on the operational deployment of AI, by contrast, remains practically non-existent; the June 2025 IS-K article illustrates this point. The observed operational uses of AI by IS and IS-inspired and directed plotters, however, indicate that generative AI is, at the very least, perceived as reducing friction in operational planning and execution.

Anticipated Exploitation of AI Systems

Based on current adoption trends, it is highly likely that AI systems will be further adopted to plan, facilitate, finance, incite, and execute acts of terrorism and violence. The horizon risks fall into two prongs identified in both PRC and U.S. documentation on terrorist use of AI: informational and operational exploitation, which can be categorized as sub-catastrophic misuse (lower risk, higher probability), and anticipatory CBRN concerns, which can be classified as catastrophic misuse (higher risk, lower probability). A third axis covers cross-cutting risks that span both.

Various experts have argued that generative AI primarily offers terrorists efficiency rather than a true transformation in capabilities and that many anticipated threats remain just that — hypothetical.⁷⁸ None-

71. Natalia Delfino, "Due giovani originari del Bangladesh arrestati per terrorismo a Palermo: 'Possibile una imminente concreta attivazione,'" *Secolo d'Italia*, May 9, 2025, <https://www.secoloditalia.it/2025/05/inneghiavano-sui-social-a-jihad-e-violenza-contra-i-miscredenti-due-giovani-originari-del-bangladesh-arrestati-per-terrorismo/>.

72. Jérémie Pham-Lê, "Man Arrested over Planned Jihadist Attack Targeting the Louvre," *Le Monde*, May 11, 2026, https://www.lemonde.fr/en/france/article/2026/05/11/man-arrested-over-planned-jihadist-attack-targeting-the-louvre_6753350_7.html.

73. "Delhi Blast Accused Used ChatGPT, YouTube To Make Bombs: Anti-Terror Agency," NDTV, May 24, 2026, <https://www.ndtv.com/india-news/delhi-red-fort-blast-news-ai-platform-misused-for-terror-engineering-in-red-fort-blast-anti-terror-agency-nia-11540357>.

74. Tech Against Terrorism, "Counter-Terrorism AI Benchmark," <https://www.ct-ai.org/>.

75. Satish Jha, "Hyderabad Ricin Terror Plotter Wanted to 'Separate South India from Rest of Country,'" *Deccan Herald*, November 20, 2025, <https://www.deccanherald.com/india/telangana/hyderabad-ricin-terror-plotter-wanted-to-separate-south-india-from-rest-of-country-3804094>.

76. Antonia Juelich, "'God has helped us, and so will AI': How the Terrorist Group Boko Haram Uses Frontier AI," *Cambridge Programme on AI Science and Policy*, July 2026, <https://casp.ac/reports/ai-enabled-terrorism>. The author conducted 57 interviews with 27 former members.

77. Antonia Juelich, "God has helped us, and so will AI," 34-35.

78. Andrew Glazzard, David McIlhatton, and Paul Martin, "Will Generative AI Fundamentally Change Terrorist Threats?" *CTC Sentinel* 19, no. 5 (May 2026), <https://ctc.westpoint.edu/will-generative-ai-fundamentally-change-terrorist-threats/>.

theless, this section shows that efficiencies gained can translate into compounding returns. What follows is a forecast of anticipated exploitation of AI systems, rather than established risk.

Axis 1: Informational and operational exploitation – Lower Risk, Higher Probability

In the next 12 months, the following adoption patterns are highly likely.

Further automation in the propaganda domain. Increased use of AI tools to produce, disseminate, and translate propaganda materials to expand reach and circumvent content takedowns on social media platforms as generative and agentic AI converge. Rapid reiteration based on feedback.

Bespoke targeting and recruitment. Further tailoring of propaganda materials to specific, parochial local grievances and connecting them to the larger message of Jihad. This AI risk was already anticipated in 2018: terrorists can target individuals with “the right message at precisely the right time to maximize persuasive potential.”⁷⁹

Doctrinal and operational guidance bots. The creation of chatbots to plan full phases of an attack, especially within the Islamic State supporter ecosystem, is a potential evolution for an organization that has long sought to reduce the friction of carrying out attacks on its behalf by producing and disseminating do-it-yourself (DIY) guides on all types of attacks. This can provide further uplift to lone radicalized individuals and can lead to improved execution of violence (e.g., more spectacular or more lethal attacks).

Anthropomorphic dependence on chatbots as a major threat vector. The PRC’s AI Safety Governance Frameworks 2.0 and 3.0 both identify “addiction and dependence on anthropomorphic interaction” as a risk without linking it to terrorism explicitly.⁸⁰

AI-enabled drone operations. The use of drones by terrorists will likely evolve with the adoption of AI, especially due to innovation spawned from the Russia-Ukraine War. AQ affiliate JNIM appears to have used open-source AI models to enhance its drone capabilities, but this is an inference based on observed capabilities rather than a confirmed method.⁸¹ In the case of Boko Haram, AI has similarly helped guide fighters by providing technical know-how, including designing explosive-release mechanisms.⁸²

AI-enabled cybercrime to fund and facilitate terrorism. Cybercriminals’ uptake of AI has outpaced that of terrorists, but signs have emerged of an increasing nexus between certain violent extremist subcultures and AI-enabled cybercrime.⁸³ AI-enabled cryptocurrency scams and tools could also finance terrorism.⁸⁴

Further institutionalization of AI in terrorist groups. Drone use by Islamic State of Iraq and al-Sham was initially ad hoc but was later formalized.⁸⁵ Similarly, as ISWAP’s use of AI suggests, further institutionalization of AI across operational tasks is likely to occur within IS and AQ affiliates.

Axis 2: Anticipatory CBRN concerns – Higher Risk, Lower Probability

Catastrophic CBRN risk. Frontier models may provide meaningful uplift for CBRN terrorism, as both Washington and Beijing fear. As in decades prior, capability rather than intent appears to be the current

79. Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Future of Humanity Institute, Centre for the Study of Existential Risk, Center for a New American Security, Electronic Frontier Foundation, and OpenAI, February 2018), <https://arxiv.org/abs/1802.07228>, 47.

80. AI Safety Governance Framework 3.0, 73, 85.

81. Niccola Milnes and Rida Lyammouri, *Countering JNIM’s Drone Proliferation in the Sahel* (Policy Center for the New South, July 2025), <https://www.policycenter.ma/publications/countering-jnims-drone-proliferation-sahel>.

82. Antonia Juelich, “God has helped us, and so will AI,” 51.

83. Yuri Neves and Emily Klein, “Innovation in AI-Enabled Harms: The Transference of AI Knowledge from Cybercriminals to Extremists,” GNET, June 8, 2026, <https://gnet-research.org/2026/06/08/innovation-in-ai-enabled-harms-the-transference-of-ai-knowledge-from-cybercriminals-to-extremists/>.

84. Daria Alexe, “Agentic Smurfing: How AI-Autonomous Micro-Laundering is Outpacing Traditional Terrorist Financing Detection,” GNET, January 28, 2026, <https://gnet-research.org/2026/01/28/agentic-smurfing-how-ai-autonomous-micro-laundering-is-outpacing-traditional-terrorist-financing-detection/>.

85. Don Ressler, Muhammad Al-Ubaydi, and Vera Mironova, “The Islamic State’s Drone Documents: Management, Acquisitions, and DIY Tradecraft,” Combating Terrorism Center at West Point, January 31, 2017, <https://ctc.westpoint.edu/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft/>.

operating constraint for various terrorist groups.⁸⁶ Even rudimentary experiments with chemical, biological, radiological, or nuclear plots can have immense, long-lasting impacts on communities, environments, and societal resilience.

Exploitation of screening gaps. Open-source, AI-powered protein design software can generate variants of amino acid sequences encoding sequences of concern (SOCs), some of which screening software used by nucleic acid synthesis providers has not detected.⁸⁷ Patches have since been distributed, but even with these mitigation measures, roughly 3 percent of variants likely to retain their function still evaded detection. Another study, using safe biological proxies, found that redesigned variants lost functionality—signaling limited near-term risk.⁸⁸

Generating better acquisition plans. Frontier labs have put safety measures in place, with some in-house assessments indicating that models produce more robust bioweapon acquisition plans than internet research alone. According to one 2025 OpenAI assessment, models are “on the cusp of being able to meaningfully help novices create known biological threats.”⁸⁹

Circumventing the tacit knowledge blocker through agentic AI. Automation may in the longer term erode an important obstacle to CBRN terrorism: tacit knowledge.⁹⁰ The practical skills needed for successful biological terrorism have appeared to be a more significant obstacle than knowing or being able to access recipes for terrorist actors. In the future, agentic systems may thus help by removing humans from some physical work with cloud laboratories — but this remains speculative at present.

Axis 3: Cross-cutting concerns

The open-weight models conundrum. Across all these outlined future risks, the safety concerns around open-source and open-weight models should be considered — especially as frontier labs that provide closed-source models continue to work on robust AI safety measures, which may push terrorists and other malicious actors to pivot to open-weight models.⁹¹ Locally run open-source and open-weight models improve operational security for terrorists by minimizing leakage, something the IS supporter ecosystem shows awareness of.⁹² Additionally, model ablation is cheap, and such models stripped of their refusal behavior are readily available for download from various open-source AI hubs.⁹³ The issue of open-weight models extends beyond generative AI to open-source robotics and computer vision projects, which can also be used in a terrorist attack.⁹⁴

Manipulation of deployed AI systems. AI models for civilian, commercial, and military purposes can be turned to terrorist purposes through various techniques, including prompt injection. For example, as counterterrorism intelligence workflows become more agentic and machine learning (ML) capabilities are increasingly embedded in intelligence functions, every document ingested can be corrupted by terrorists in hopes of disrupting the intelligence process. A better-known scenario is that of recommender systems of social media platforms which can be leveraged to surface relevant content by terrorist groups and their supporters.⁹⁵

86. Rueben Dass, “Jihadists’ Use and Pursuit of Weapons of Mass Destruction: A Comparative Study of Al-Qaeda and Islamic State’s Chemical, Biological, Radiological and Nuclear (CBRN) Weapons Programs,” *Studies in Conflict & Terrorism* 47, no. 5 (2024): 548, <https://doi.org/10.1080/1057610X.2021.1981203>; Antonia Juelich, “God has helped us, and so will AI,” 67.

87. Bruce J. Wittmann et al., “Strengthening Nucleic Acid Biosecurity Screening against Generative Protein Design Tools,” *Science* 390 (October 2, 2025): 82, <https://doi.org/10.1126/science.adu8578>.

88. Svetlana P. Ikononova et al., “Experimental Evaluation of AI-Driven Protein Design Risks Using Safe Biological Proxies,” *Biorxiv* (May 16, 2025), <https://doi.org/10.1101/2025.05.15.654077>.

89. “Deep Research System Card,” OpenAI, February 25, 2025, <https://cdn.openai.com/deep-research-system-card.pdf>.

90. On tacit knowledge and biological weapons: James Revill, Catherine Jefferson, Tacit knowledge and the biological weapons regime, *Science and Public Policy*, Volume 41, Issue 5, October 2014, Pages 597–610, <https://doi.org/10.1093/scipol/sct090>

91. Clara Broekaert, “Open-Weight AI Models and Terrorist Exploitation: A Preliminary Assessment,” *Militant Wire*, August 10, 2026, <https://www.militantwire.com/p/open-weight-ai-models-and-terrorist>.

92. Clara Broekaert and Colin P. Clarke, “The Pandemonium Narrative and Its Limits.”

93. Abliteration is a technique that modifies a model’s weights to suppress its tendency to refuse prompts. It specifically works by identifying the direction and/or the subspace in the model’s activation space that mediates refusal behavior and then removing the model’s ability to represent it.

94. Brian Fishman, “AI and the New Blueprint of Terrorism,” *War on the Rocks*, March 9, 2026, <https://warontherocks.com/ai-and-the-new-blueprint-of-terrorism/>.

95. Gilad Karo, Tom Divon, and Blake Hallinan, “The TikTok Caliphate: How Jihadist Supporters Exploit Algorithmic Recommendations and Evade Content Moderation,” *Social Media + Society* 12, no. 1 (2026): 20563051251412167, <https://doi.org/10.1177/20563051251412167>.

Cooperation Framework on Countering the Terrorist Misuse of AI

Three criteria should govern where cooperation between the PRC and the United States starts: the harm must be of high priority, the characterization of it must command high consensus, and the domain must carry low politicization. Terrorist misuse, when scoped within the bounds of joint Chinese and American counter terrorism interests, meets all three, as do child sexual abuse material and CBRN proliferation to non-state actors. As illustrated, few cases are as dire or consequential as the potential for terrorist organizations to harness AI for deadly purposes. Both the United States and China have an interest in preventing this from happening.

U.S. and Chinese labs lead the world in developing the most powerful AI models. One commonality among the risks posed by terrorist misuse of AI is that they are global threats, not bound by country borders or confined to a specific jurisdiction. No single state can tackle this security threat alone. This is why countries worldwide have developed and implemented numerous international counterterrorism cooperation frameworks. In the case of terrorist misuse of AI, for example, both the PRC and the U.S. are articulated targets. Take IS-K — a group that has a proven track record of high-tech capabilities — which has targeted both the U.S. and the PRC in propaganda and actual attacks carried out.

Guardrails

The most likely failure of a cooperation framework between the PRC and the United States would arise from misuse and its entanglement with other contentious issues in U.S.-PRC relations. Therefore, this framework should have clear limits from the outset. It shall not be based on any requirement related to disclosure of model capabilities, weights, training data, evaluation results, nor connected to any domestic terrorist designation practice. The latter point seeks to mitigate the fact that MPS and FBI cooperation is complicated because MPS implements Xinjiang's security policy. Moreover, people have raised alarms about counterintelligence exposure created by existing FBI-MPS cooperation.⁹⁶ To avoid risk exposure to the United States and to the PRC, the cooperative framework should be narrow and allow for little leeway to politicize definitions of, for example, terrorist propaganda and extremism. This is a clear barrier to prevent this framework from becoming a vehicle for CCP domestic policy in Xinjiang. All pillars of the cooperative framework should be considered and drafted in light of the following:

- The framework's scope is closed and relies on mutual recognition. The cooperation framework will only work with organizations listed in an agreed annex. This likely consists of Islamic State, al-Qaeda, and specific affiliates. ETIM would thus necessarily be excluded. This annex can only be expanded by written agreement of both parties to avoid the cooperative framework from becoming a vehicle to help with politicized designations.
- Discussions on designations cannot fall within this framework's scope. Neither party to the framework may condition its participation on specific designations once agreed. This framework will not serve as a battlefield for designations.
- No personally identifiable information (PII) is shared. No PII of U.S. people will be shared under this framework, including Chinese diaspora community members. This extends to any data from which members of this community could be identified, such as through derived or aggregated data.
- Redlines are agreed in advance. Exiting the cooperative framework is defined beforehand, based on the aforementioned safeguards.

The following pillars for a cooperation framework are ordered by dependency. Two of these pillars can be agreed upon quickly, while the other three will require an iterative process.

org/10.1177/20563051251412167.

96. Jana Winter, "Under Patel, FBI forges unprecedented law enforcement ties with China, Russia," Reuters, August 5, 2026, <https://www.reuters.com/world/china/under-patel-fbi-forges-unprecedented-law-enforcement-ties-with-china-russia-2026-08-05/>.

Pillar	First Phase	Earliest credible delivery
1. Working Group on Mitigating Terrorist Misuse of AI	Agreement in principle to stand up the group and name leads	6–12 months
2. Nucleic Acid Synthesis Screening	Joint endorsing of Joint endorsement of International Gene Synthesis Consortium (IGSC)-equivalent screening	6 months
3. Track II Dialogue	Annual third-party-convened dialogue	6 months
4. Parallel Taxonomies and Crosswalk	Agree to publish national taxonomies and joint crosswalk that maps counterparts	12–24 months
5. Incident Information Sharing Mechanism	Commitment to negotiate a reporting format and thresholds	12–24 months

Pillar 1: Working Group on Mitigating Terrorist Misuse of AI

As a gesture of commitment from both sides, establish a working group to mitigate terrorist misuse of AI as part of the government-to-government AI risk-reduction dialogue, led by Treasury Secretary Scott Bessent from the U.S. and by Vice Premier He Lifeng from the PRC. However, while officially under the government-to-government AI risk-reduction dialogue, given its clear counterterrorism and national security mandate, the working group on Mitigating Terrorist Misuse of AI would likely be most effective as part of the growing number of new law enforcement working groups led by the FBI and MPS. On the U.S. side, the National Counterterrorism Center (NCTC) will likely provide analytical support to the working group. On the PRC side, the Cyberspace Administration of China (CAC), the National Development and Reform Commission (NDRC), and the Ministry of Foreign Affairs (MFA) may possibly be included as needed for key aspects of the working group. For example, in regulating Chinese AI models to reduce misuse, the CAC will be critical.

The composition of the respective delegations to this working group should be settled before the first session. This way both Washington and Beijing can send technical, subject-matter expert staff, rather than political foreign policy officers, and ensure a smooth first meeting. Each side should appoint technical co-chairs.

One aspect of this working group that will require extra thought, design, and careful diplomacy is how to address open-source and open-weight models. Both capitals endorse open models and view their benefits from different competitive perspectives — Washington seeks to keep the U.S. AI stack relevant, while Beijing seeks to counter controls on chips and computing. The scope of cooperation on this issue is therefore narrow and fragile, though important, as open-weight models will likely feature in future misuse. The main shared interest is that neither country wants an open-weight model to provide meaningful uplift to a terrorist group or radicalized individual, and to face the backlash against open releases that would follow a mass casualty attack that was enabled by such a model.

In practice, as other analysts have argued, using risk dialogue to change how China's open releases of models work will most definitely be too contentious and open a Pandora's box of issues.⁹⁷ A realistic starting point could be to agree on tests to assess what an open-weight model can do after its refusal behavior is removed, for example, by ablation, with each side running the tests domestically. Anything beyond

97. Mark MacCarthy and Carl Schonander, "How the US and China can cooperate to reduce urgent AI risks," Brookings, July 14, 2026, <https://www.brookings.edu/articles/how-the-us-and-china-can-cooperate-to-reduce-urgent-ai-risks/>.

that is unlikely to stand the test of time, and of tension.⁹⁸

The working group's output should include a blueprint that specifies incident response, threat actor information sharing, and crisis communication. Existing AI safety frameworks do not specify what these would look like for terrorist misuse, making this a significant step forward if successfully delivered and made operable.

Pillar 2: CBRN Cooperation, Beginning with Nucleic Acid Synthesis Screening

CBRN is one of the most promising domains of cooperation with neither Washington nor Beijing in favor of non-state actors having access to these capabilities. Catastrophic proliferation to non-state actors, including terrorist groups, is a symmetric downside for both countries: neither Washington nor Beijing gains anything from those capabilities becoming widely accessible, and neither can contain the consequences within its own borders.

A CBRN cooperation agenda can include common capability and evaluation standards, standards around model access, sharing threats derived from uplift testing (without disclosing underlying evaluations), and continual monitoring, aligned where possible with NIST and The Center for AI Standards and Innovation (CAISI) work as well as with international standards. Nucleic acid synthesis screening is a logical starting point to commence cooperation, because voluntary standards and screening infrastructure already exist in both countries.

The U.S. and PRC do not require nucleic acid synthesis providers⁹⁹ to screen orders, though they provide most synthesis capacity.¹⁰⁰ As described above, both have identified risks related to uplift experienced in the CBRN domain and should thus naturally be an area where significant progress can be made. The most evident avenue for such cooperation is the International Gene Synthesis Consortium. This voluntary industry association has a screening protocol and already includes Chinese providers committed to screening “the complete DNA and translated amino acid sequences of every double-stranded gene order against IGSC’s comprehensive curated Regulated Pathogen Database.”¹⁰¹ A big step forward would be Beijing and Washington adopting this protocol as a baseline, using the working group to further promote these standards, and including more providers. In February 2026, Track II dialogue between the China Arms Control and Disarmament Association and Nuclear Threat Initiative already called on the governments to “elevate cooperation on preventing non-state actor misuse of modern bioscience and biotechnology as a shared priority.” They also encouraged pursuing mandatory nucleic acid synthesis and customer screening.¹⁰²

Pillar 3: Track II Dialogue to explore U.S.–PRC AI Risk Reduction of Terrorist Misuse

Building on existing Expert Exchanges and Track II Dialogues on AI and National Security, Washington and Beijing should encourage and support an annual Track II dialogue. The U.S.-China Track II Dialogue on Artificial Intelligence and National Security, convened by Brookings and Tsinghua University’s Center for International Security and Strategy since 2019, has already published analysis on addressing AI risks from non-state actors, including joint safety guidelines and threat actor information sharing, signaling a positive step in the right direction and something to continue building on. This dialogue has proven promising and realistic, “sustained by mutual interest, not mutual trust.”¹⁰³

The Track II Dialogue efforts have already produced technically grounded, jointly agreed-upon state-

98. For the U.S. side, Executive Order 14409 already provides a voluntary pre-release engagement framework between frontier developers and federal agencies for cyber capabilities.

99. There are some U.S. rules related to synthesis when federal funding is involved.

100. Nucleic acid synthesis providers are companies that primarily provide their services to research labs and biotechnology companies. These services typically consist of using automated systems to chemically synthesize the genetic sequence requested by the customer. Often there is a screening layer in place, in which the nucleic acid synthesis provider checks orders against certain databases to ensure that these do not pose a security risk. In the United States, some customer-side conditions related to screening exist for federally funded institutions.

101. International Gene Synthesis Consortium, <https://genesynthesisconsortium.org/#about/>

102. CACDA-NTI Joint Statement on Shared Priorities for Strengthened Biosecurity and Responsible AI-Biotechnology Innovation, February 18, 2026, <https://www.nti.org/analysis/articles/cacda-nti-joint-statement-on-shared-priorities-for-strengthened-biosecurity-and-responsible-ai-biotechnology-innovation/>.

103. R. David Edelman and Ryan Hass, “From Geneva: AI, security, and US-China dialogue.” Brookings, July 1, 2026, <https://www.brookings.edu/articles/from-geneva-ai-security-and-us-china-dialogue/>.

ments. The International Dialogues on AI Safety (IDAIS) London, attended by prominent scientists from both PRC and the West, recommended “states recognise the common threat posed by the proliferation of AI-enabled cyberattack and biological misuse,” assessing that “dual-use capabilities that were previously concentrated in states—or that required state-level resources to acquire—are fast becoming accessible to non-state actors, from terrorist groups to lone individuals.”¹⁰⁴ This is evidence of scientists being able to put their names under a shared characterization of the problem at hand: non-state misuse of AI. Similar work can thus be done on the particular misuses by terrorists and violent extremists.

The annual U.S.-China Track II Dialogue should bring together delegations consisting of government officials, technology leaders, researchers, and technical experts to explore U.S.-China AI risk reduction and misuse by terrorist actors. Each Track II Dialogue should be narrowly scoped to encourage solution-oriented policy exchange with the objective of identifying areas of convergence and developing practical options for risk reduction.

American and Chinese institutions should be designated as partners, tasked with maintaining year-round working groups to follow up on recommendations and sustain engagement among Track II Dialogue experts. The Track II Dialogue initiative should remain unofficial and nonbinding, with the understanding that findings will be communicated to relevant U.S. and PRC government stakeholders.

In the longer term, the Track II Dialogue could raise the participation of major labs in an incident-sharing mechanism (as per Pillar 5). Most known abuse of AI systems by non-state actors has come from threat intelligence reporting by labs. Encouraging Chinese labs to put out similar reporting as U.S. labs could be something raised in these fora.

Pillar 4: Parallel Threat Taxonomies and Crosswalk

Building upon already existing AI risk taxonomies, such as the Massachusetts Institute of Technology (MIT) AI Risk Repository, the United Nations Institute for Disarmament Research (UNIDIR) AI Risks Taxonomy, and AI threat taxonomies developed by U.S. and PRC government agencies, respectively, the United States and PRC should each establish a national Threat Taxonomy for the Terrorist Use of AI. After each side has done this, a crosswalk should be established. Such a crosswalk maps each U.S. category to its counterpart in the PRC’s taxonomy and shows when the categories do not have a counterpart.

The alignment in the crosswalk will likely be found in behavior-based concepts, and diverge at times where content is defined: At a minimum, both the PRC and the U.S.’s respective Threat Taxonomies should detail the threats posed by:

Terrorist Use of AI to Enhance Tactics, Techniques and Procedures (TTPs); including weaponry research, design, and procurement, reconnaissance, and other forms of operational, tactical, and logistical planning to carry out acts of violence.

Terrorist Use of AI for Catastrophic CBRN attacks; including accessing previously highly technical and scientific knowledge to act as a force multiplier in order to carry out chemical, biological, radiological, or nuclear attacks.

Terrorist Use of AI for Financing Purposes; including to launder money, circumvent anti-money laundering (AML) and other countering the financing of terrorism (CFT) rules and regulations, and automating financial fraud, extortion schemes, and other cybercrimes.

Terrorist Use of AI for Propaganda and Recruitment; including synthetic media generation, automated translation, and personalized recruitment tactics through bots and other online media.

Each Taxonomy should be updated on a set periodic basis to remain current with advancements in AI technology and terrorist exploitation. The crosswalk should be revised at such intervals as well. Inputs to update the crosswalk can be proposed and evaluated by the Working Group (Pillar 1), which also receives reports and input from the Incident Information Sharing mechanism (Pillar 5). Each national taxonomy should also record, for each case, the step on the observation-to-uplift ladder that it reached.

104. “IDAIS-London, 2026,” London, UK, April, 2026, <https://idaais.ai/dialogue/idaais-london/>; “Tsinghua experts and global AI leaders sign the IDAIS London Declaration,” Tsinghua University, <https://www.tsinghua.edu.cn/en/info/1245/14929.htm>

Pillar 5: Incident Information Sharing Mechanism

The U.S. and the PRC should establish a structured channel for incident reports. The channel should draw on existing military and law enforcement crisis management channels to establish a communications protocol for the timely exchange of information — not intelligence — related to incidents that rise to an established threshold in which terrorists use, attempt to use, or seek to acquire AI capabilities for terrorist or other violent purposes. The information-sharing mechanism should not be constructed as an intelligence-sharing framework, but rather should aim to help both sides provide early warning and enable coordination when both countries face a shared threat.

As one of the most important but sensitive pillars of this framework, it should be agreed upon beforehand what a report contains in a formulaic fashion, including the facts and data of an observed or attempted misuse of AI for the purpose of terrorism, the category of AI involved per the crosswalk established in Pillar 4, the organization to which the activity is attributed (if in annex) or a statement if attribution is not confirmed, and the technique used by the malicious actor.

The mechanism will thus be incident-driven and follow an established format to disclose, for example:

1. the nature of the threat;
2. the AI capabilities and misuse involved;
3. the relevant actor;
4. TTPs;
5. potential threat implications.

However, classified information, sources and methods, model capabilities, and other commercially sensitive technologies will not be disclosed. This includes model weights, training data, and training methods. Similarly, the incident sharing creates no obligation for either party to explain why the model behaved as it did.

Points of contact will be designated, and procedures will be established for reporting and notification, including for imminent or rapidly developing threats. The designated points of contact and communication procedures will also enable officials from both sides to seek clarification and coordinate appropriate mitigation measures as needed. Critically, this mechanism should be composed so that incident sharing can continue even if a political crisis suspends other forms of cooperation.

About the Authors

Mollie Saltskog is a Research Fellow at The Soufan Center, specializing in counterterrorism, national security policy, open-source intelligence (OSINT), and geopolitics. She has more than eight years of experience analyzing national security challenges and their implications for U.S. and international policy, with expertise spanning Salafi-jihadi terrorism, emerging technologies and counterterrorism, and Chinese foreign and national security policy. Her work focuses particularly on the intersection of counterterrorism and strategic competition, including opportunities and challenges for international cooperation to mitigate transnational security threats. Mollie has lived, studied, and worked in the People's Republic of China on multiple occasions over the past decade, most recently spending two years in Shanghai with the U.S. Department of State.

Clara Broekaert is a Research Analyst at The Soufan Center. At the Center, she specializes in international security and conflict with a focus on terrorism, emerging technology, and foreign interference. Clara has conducted investigations into terrorist groups, analyzing their organizational structures, online ecosystems, and operational tradecraft. She also conducts research on foreign interference and emerging technology in the context of conflict and interstate competition.

Acknowledgements

The authors thank Ali Wyne, Broderick James McDonald, and Chad Serena for their review and input. Any errors are our own.

The Soufan Center is a 501c3 non-profit organization



THE SOUFAN CENTER

Phone - +1 646-248-6486
Email - info@thesoufancenter.org
Website - www.thesoufancenter.org
156 W 56th Street
New York, NY 10019