

RESEARCH NOTE

Terrorist Exploitation of Artificial Intelligence

Joana Cook,* Graig Klein, and Bàrbara Molas

Volume XX, Issue 3
September 2026

ISSN: 2334-3745
DOI: 10.19165/JSMT2446

Abstract: On 7–8 November 2024, the International Centre for Counter-Terrorism (ICCT) and the Institute of Security & Global Affairs (ISGA) at Leiden University hosted a closed-door ‘blue-sky’ workshop in The Hague on the terrorist exploitation of artificial intelligence (AI), funded by the Netherlands’ National Coordinator for Security and Counter-Terrorism (NCTV). The workshop brought together 26 experts from academia, industry, law enforcement, computer science, and government across eleven countries to anticipate how terrorists and (violent) extremists may adapt to and exploit emerging AI technologies.

Using a ‘blue-sky’ approach, participants developed creative yet realistic scenarios to encourage proactive thinking about emerging threats and move beyond the traditionally reactive character of (counter-)terrorism studies. Across five thematic sessions, participants examined the potential exploitation of AI for operational purposes, including enhancing terrorist capabilities and facilitating weapons production; the misuse of decentralised and open-source AI systems to circumvent content moderation and access harmful information; and the lifecycle and trajectory of AI-generated extremist content online. Discussions also considered how emerging AI technologies could enable states to provide support to non-state actors, including terrorist and extremist groups and individuals, before exploring more speculative scenarios in which AI could operate as a fully independent entity.

Drawing together insights from these discussions, participants identified key themes and assessed how terrorists are most likely to adapt to AI-powered technologies. This event summary presents the workshop’s principal findings and session-specific insights, offering forward-looking perspectives relevant to scholars, practitioners, and policymakers working at the intersection of terrorism, counter-terrorism, and AI.

Keywords: AI, terrorism, weapons, generative AI, state sponsored terrorism, foresight

* Corresponding author: Joana Cook, Leiden University, email: j.l.i.cook@fgga.leidenuniv.nl

Introduction

Terrorists can identify and exploit emerging technologies for operational advantage. While sometimes uptake of new technologies can be slow and conservative to minimise introducing new risks and vulnerabilities, terrorists consistently demonstrate the ability to adapt, adopt, and innovate.¹ New technologies create opportunities to overcome operational constraints, expand organisational reach, and enhance tactical and strategic effectiveness. Artificial intelligence (AI) is the newest frontier for exploitation. With the rapidly evolving technological capabilities, increasing accessibility of commercial, open-source, and offline large language models (LLMs), generative image and video systems, and autonomous agents, AI presents unprecedented opportunities for terrorist and violent extremist exploitation.²

Although speculative and dramatic scenarios, like AI-directed terrorist campaigns, cannot be dismissed, they risk diverting attention from the more immediate ways AI is already lowering barriers to terrorist activity.³ In the near- to medium-term, AI is more likely to enhance existing terrorist capabilities than fundamentally transform the nature of terrorism.⁴

AI's principal significance lies not in creating entirely new forms of terrorism, but in acting as a force multiplier that amplifies existing capabilities while lowering technical, organisational and cognitive barriers. Rather than replacing human agency, AI "can improve the efficiency, accessibility and scale" of existing terrorist tools, tactics, and procedures (TTP).⁵ This distinction between technological transformation and technological amplification provides the analytical foundation for this research note.

The analysis presented here draws upon the principal findings of a multidisciplinary blue-sky workshop convened in The Hague, NL, in November 2024 hosted by the Institute of Security and Global Affairs (ISGA) at Leiden University and the International Centre for Counter-Terrorism (ICCT).⁶ Twenty-six specialists from academia, government, law enforcement, industry, and computer science participated in exploring plausible pathways through which terrorists can exploit AI. The aim was to identify emerging trends, challenge prevailing assumptions, and examine how technological developments influence future patterns of terrorist adaptation and activities.

Blue-sky exercises provide a structural method for examining plausible developments before they emerge as operational threats. The objective is not prediction, but anticipation by encouraging multidisciplinary dialogue identifying emerging patterns, conceptual gaps, and research priorities. Across the discussions, participants converged around one central observation: AI lowers the costs and barriers to action for terrorists and violent extremists (and potential recruits and radicalising individuals) while increasing the speed, scale, and efficiency with which existing TTPs can be adapted. Whether applied to operational planning, multilingual communication, intelligence analysis or cyber-enabled activity, AI was consistently viewed as an enabling capability rather than a substitute for human agency.

Building on these expert discussions, this research note examines terrorist exploitation of AI across operational, informational, and ecosystem dimensions before proposing a Force Multiplier Framework that synthesises these findings into four interconnected dimensions: cognitive, operational, communicative, and organisational.

Terrorist Exploitation of AI

Participants consistently emphasised that AI is not an end in itself, nor does it fundamentally alter the motivations driving terrorism.⁷ Rather, AI presents a rapidly evolving set of capabilities that terrorists can exploit across existing activities. The central question is therefore not what AI can do, but how terrorists can incorporate AI into existing TTP and upgrade their capabilities.

AI should be viewed within the broader history of technological adaptation rather than as an unprecedented development. From encrypted communications and cryptocurrencies to commercially available drones and social media platforms, terrorists have consistently appropriated emerging technologies to enhance recruitment, communication, financing, intelligence gathering, and attack planning. What distinguishes AI is not only its sophistication, but its broad applicability across almost every stage of terrorist activity. Unlike many previous technologies that served discrete operational purposes, AI can augment multiple activities at once.⁸ A recurring theme was that AI should primarily be understood as an enabling technology.

Participants shared concern that increasingly available and accessible commercial, open-source, and offline LLMs and AI systems lowers barriers to experimentation. While exploiting frontier capabilities still requires specialist knowledge, the democratisation of AI expands the pool of actors able to experiment with increasingly capable systems.

The discussions further highlighted the importance of distinguishing between opportunity and capability. The availability of AI does not automatically translate into operational success. Terrorists differ significantly in their resources, technical expertise, access to organisational resources and maturity, and strategic intent, all of which shape their desire and ability to exploit emerging technologies effectively.

Participants hedged against technologically deterministic narratives that portray AI as either a transformative solution or an existential threat. Instead, AI was consistently viewed as providing an opportunity for terrorists to increase speed, reduce costs, improve efficiency, and enable greater personalisation across existing methods of radicalisation, recruitment, and violence.

Finally, participants recognised that opportunities for terrorist exploitation will not emerge uniformly. Different individuals and organisations will pursue different pathways depending on their strategic objectives, technical capabilities, and operating environments. Some may prioritise operational applications such as planning, intelligence gathering, and cyber-enabled attacks, while others may focus on propaganda, recruitment, and influence operations. Likewise, state-supported groups or hybrid networks may be better positioned to exploit more advanced AI capabilities than smaller or less technically proficient individuals and organisations. Understanding these differences is essential for developing proportionate risk assessments and avoiding assumptions that technological advances will affect all terrorists in similar ways.

Taken together, the discussions suggest that AI is best understood as an enabling technology that expands opportunities for terrorist exploitation across multiple domains of activity. The following sections examine how those opportunities manifest operationally, within the information environment, and through broader AI ecosystems.

Operational Exploitation of AI

Workshop participants identified operational exploitation as one of the most credible and immediate pathways through which terrorists can benefit from AI. Rather than fundamentally changing how attacks are conceived or executed, or fully replace human decision-making, AI can be exploited to enhance the speed, efficiency, and effectiveness of multiple activities across the terrorist attack cycle. Ultimately, AI helps reduce the time, expertise, and resources required to coordinate, plan, and execute attacks.

Intelligence Collection, Reconnaissance, and Target Identification

Intelligence collection and reconnaissance were identified as two of the most immediate opportunities for terrorist exploitation of AI. Open-source intelligence (OSINT) already plays an important role in terrorist activities and AI significantly expands the speed and scale at which OSINT can be identified, collected, translated, and analysed. AI substantially reduces the cognitive burden associated with these tasks which thereby could improve the likelihood and reliability of target penetration and attack success. Advances in computer vision and image recognition algorithms will also improve reconnaissance by assisting and improving the identification of potential targets, security measures, and physical vulnerabilities from imagery and geospatial information.

Planning and Decision Support

Beyond improving intelligence collection, AI also creates opportunities to translate information into more effective operational planning. Increasingly capable LLMs function as interactive research assistants that can compare alternatives, synthesise technical information, and support decision-making. Rather than replacing human operational decision-making, AI enables terrorists to make better-informed decisions, just like it helps everyday civilians, by rapidly synthesising information from multiple sources or quickly identifying weaknesses or coordination gaps. For example, Boko Haram used AI to overcome physical security barriers and improve the likelihood of reaching their target via motorcycles jumping defensive trenches.⁹

Logistics, Cyber Operations, and Capability Enhancement

Workshop discussions highlighted the potential for AI to enhance logistics, communications planning, and resource management. Cyber-enabled activities featured prominently, with AI lowering barriers to coding assistance, vulnerability discovery, phishing and social engineering. Participants also discussed opportunities to optimise existing weapons and commercially available drones, as well as AI-assisted analysis of critical infrastructure vulnerabilities. AI-enabled simulation tools can support operational experimentation in virtual environments before real-world implementation. These discussions reinforced the conclusion that terrorists are more likely to exploit AI to enhance existing methods of violence than to replace them with entirely new approaches.

The workshop findings suggest that the operational significance of AI lies in enhancing activities already embedded within the terrorist attack cycle rather than introducing fundamentally new forms of terrorism. AI acts as a force multiplier by reducing technical and cognitive barriers while augmenting human decision-making. But operational exploitation is only one dimension. The workshop devoted equal attention to the ways in which generative AI is transforming the information environment, creating new possibilities for propaganda, recruitment, influence and radicalisation.

AI and the Information Environment

Participants emphasised that the most pronounced terrorist exploitations of AI are in propaganda production and contested public discourse in the broader information environment. While terrorists have long exploited digital platforms for propaganda, recruitment, and strategic communication, advances in (generative-) AI create new opportunities to increase the speed, scale, sophistication, and personalisation of these activities. It is not simply another propaganda tool, rather, it fundamentally enhances how content is produced and enables catering information and propaganda to target specific audiences by adapting content to different cultures, context, and audience vulnerabilities.

Propaganda Production and Content Generation

One of the clearest findings from the workshop was that (generative-) AI substantially lowers the barriers for producing high-quality propaganda. Historically, creating persuasive multilingual content, professional graphics, or convincing videos required time, technical expertise, and organisational resources. Now, AI assists with image generation and video synthesis tools which enables the production of dynamic and 'Hollywood'-style material that previously would have required specialist capabilities.

AI substantially lowers the barriers for mass-production of propaganda and content. And, using AI's multi-lingual translation capabilities, adapting narratives and content to different contexts is easier. Terrorists can exploit AI for rapidly producing tailored content that engages audiences across linguistic and geographical boundaries. AI accelerates existing propaganda strategies and reduces the time and effort required to develop new material.

Participants also noted that (generative-) AI systems can be combined to produce integrated propaganda campaigns incorporating text, imagery, audio, and video. Multimodal content may prove more persuasive and memorable than individual media formats alone, which increases the risks from a lengthier content lifecycle and likelihood that online content is downloaded into the offline world.

The workshop also highlighted that AI-generated content may become increasingly difficult to distinguish from authentic material. Improvements in text generation, synthetic imagery, cloned voices, and AI-assisted video production create opportunities for terrorists to produce persuasive content that appears credible and professional.

Recruitment, Radicalisation, and Audience Engagement

Participants also explored how AI can reshape recruitment by enabling personalised and adaptive engagement with potential supporters. LLMs and conversational AI systems are increasingly capable of sustaining prolonged interactions, responding to individual questions and adapting communication styles to particular audiences. Participants identified various scenarios that included the use of AI (chat)bots to do harm, especially through the potential to shape discourses in closed environments. Participants explored scenarios in which AI chatbots outnumber human users in closed online communities. The chatbots would always be online and available to answer questions, and therefore could reinforce extremist narratives, shape group norms, and amplify disinformation and extremist content. The more they interact with specific individuals, the more likely they can adapt and tailor their messaging and content to that individual. Chatbot-to-chatbot communication (i.e. chatbots responding to other chatbots instead of only to human input) could create a constant extremist loop, reducing opportunities for moderation or intervention.

But it is not just the technology that is a concern. The platform users, i.e., people, also pose a challenge in this new environment. People could also become desensitised to increasingly aggressive messaging that shapes online discussions. And users' psychological or mental health could make them more vulnerable to manipulation by AI tools that contain harmful content and intent. Participants developed a potential scenario in which decentralised platforms are used to identify and target vulnerable individuals for recruitment or exploitation.

Importantly, workshop participants cautioned against assuming that AI itself radicalises individuals and emphasised that AI creates opportunities to enhance existing recruitment and engagement strategies by making communication more responsive, scalable, and tailored to individual preferences.

Information Integrity and Trust

One of the most significant workshop discussions emphasised that the proliferation of AI-generated content may fundamentally alter the broader information environment in which governments, law enforcement agencies, journalists, and researchers operate.¹⁰ For example, advances in (generative-) AI images, audio, and video increase opportunities to manipulate information, impersonate individuals, and undermine confidence in authentic content. Participants discussed how synthetic media could be incorporated into influence campaigns designed to exaggerate the impact of attacks, manipulate media reporting, or exploit rapidly evolving crises.

As AI-generated material becomes increasingly commonplace, distinguishing authentic information from manipulated or fabricated content is likely to become progressively more difficult. Yet, participants highlighted that AI-driven information overload may itself become a strategic challenge, complicating verification, attribution, and online threat detection.

This portion of the workshop demonstrated that AI's significance within the information environment extends well beyond propaganda production. By reshaping communication, influence, credibility, and audience engagement, AI expands opportunities for terrorist exploitation while simultaneously complicating attribution, verification, and online threat detection. Consensus was reached that understanding terrorist exploitation of AI requires examining individual technologies *and* the broader information environment. This served as a bridge for considering how states could shape future pathways for terrorist exploitation of AI, which we describe in the following section.

AI Ecosystems and State(-Supported) Terrorism

Participants widely agreed that terrorist exploitation of AI will depend on both technological advancements and the ecosystem through which AI capabilities are developed, transferred, and accessed. While open-source models, decentralised AI, and commercial innovation continue lowering barriers to entry, participants stressed that the most sophisticated AI capabilities are likely to remain concentrated among states and major technology companies. Understanding future terrorist exploitation of AI therefore requires examining the role of states, technology companies, and hybrid threat networks.

A recurring theme throughout the workshop was that most contemporary terrorists groups, or individuals, are unlikely to independently develop advanced AI-enabled capabilities. Many of the more sophisticated applications discussed, including autonomous weapons, advanced

surveillance systems, AI-enhanced intelligence analysis, and complex cyber capabilities, remain technically demanding, resource intensive, and dependent upon specialised expertise. Participants agreed that a significant risk is how sophisticated technologies developed by states or companies could become accessible through proxy relationships, hybrid networks, or (in-) direct state support.

State Actors as Capability Multipliers

Rather than transferring sophisticated AI systems outright, participants suggested that states would be more likely to provide AI-enabled analysis, outputs, or products to proxy groups or aligned non-state actors. This concern was illustrated using contemporary examples of states, including Iran, employing AI-enabled surveillance, facial recognition, and digital targeting capabilities against political opponents and activists, and the potential for sharing this information.¹¹ Other scenarios explored states sharing outputs from vulnerability detection models to maximise non-state actors' attacks. And that states could co-attack through cyber operations to overload the target's systems and stretch its response and countermeasures thin.

Participants emphasised that private military companies and proxy organisations (e.g. Wagner Group/Africa Corps) help transfer AI-enabled capabilities from conflict zones and against civilian populations.¹² Threats from these processes extend outside conflict zones as foreign fighters observe, learn, and practice battlefield operations in Ukraine and Gaza, for example, and export these lessons when they return home or travel to new conflicts.¹³

This reflects a broader workshop conclusion that future terrorist exploitation of AI may be driven as much by external enablers as by terrorist innovation itself. An important question about the role of state actors and their capabilities is their willingness and capacity to share them with non-state actors (NSAs) through the crime-terror nexus.¹⁴

State-Crime-Terror Nexus

Participants also highlighted the increasingly blurred boundaries between states, organised crime, and non-state armed groups. AI capabilities may diffuse through these hybrid networks rather than via direct state sponsorship. Examples discussed included organised criminal groups facilitating access to technologies through illicit markets and the potential transfer of AI-enabled capabilities through existing crime-terror relationships.¹⁵

Such indirect pathways may prove more attractive to states seeking to preserve plausible deniability while expanding the operational capabilities of aligned actors. The diffusion of AI capabilities through such networks represents an important evolution of the crime-terror nexus. AI introduces a new strategic resource that can be exchanged, transferred, or jointly exploited within existing criminal and extremist networks.

Information Warfare and AI-Enabled Intelligence

The workshop underscored the growing importance of AI within information warfare. State actors increasingly employ AI to amplify propaganda, generate persuasive disinformation, manipulate online discourse, and shape public opinion at an unprecedented scale that can degrade public trust and obscure attribution.

Participants also discussed how AI-assisted processing of large datasets offers governments unprecedented opportunities to identify security vulnerabilities, analyse border crossings, optimise logistics, detect weaknesses in critical infrastructure, and support cyber operations. Rather than transferring AI models themselves, states may selectively share intelligence products generated through AI systems, enabling proxy actors to conduct more effective attacks while reducing the technical expertise required to execute them.

Governance, Data, and Future Risk

Finally, participants expressed concern about the governance of data itself as AI becomes increasingly embedded within state institutions. AI increasingly enables governments to integrate vast repositories of personal, biometric, financial, and behavioural data. While these capabilities can support legitimate governance, social services, taxation, and security functions, participants highlighted the risks posed by political change, evolving regulatory frameworks, deteriorating international relations, tech and AI industry leaders obtaining leading roles in governments, or corrupt leaders selling access to or information from these repositories.

The workshop suggests that future terrorist exploitation of AI will be shaped by the broader strategic ecosystem in which states, private industry, organised crime, proxy organisations, and decentralised AI communities collectively influence the accessibility, diffusion, and application of AI capabilities. The greatest risks therefore may emerge from the convergence of technology access, hybrid conflict, state support, and criminal networks, rather than from independent terrorist innovations.

AI as an Independent Entity and Security Risk

Societal implications of AI integration

The pursuit of artificial general intelligence (AGI) and artificial super intelligence (ASI) is expected to continue, although technological barriers and uncertainty around their feasibility remain. In the meantime, AI is likely to become increasingly authoritative and persuasive, potentially affecting individual autonomy and concentrating power among technology developers. Human decisions around training data and algorithms will remain a key source of risk. Particular concerns exist around AI adoption without sufficient safeguards, accountability, or digital literacy. AI's societal and environmental impacts could also generate anti-tech movements, polarisation, or attacks on AI-linked infrastructure.

Human oversight versus autonomous systems

The integration of AI into critical infrastructure, medical systems, traffic control, and other interconnected networks is set to advance, but this also brings risks of possible exploitation or attacks. Linking previously separate systems could create unforeseen interactions and cascading failures, while increasingly interconnected smart cities may make emergency shutdowns highly disruptive. Such disruption could be either driven by extremist or terrorist actors or also exploited by them. Maintaining effective safeguards and "emergency breaks" will therefore be important, although participants considered the possibility of complete loss of human control unlikely in the near term.

AI as an uncontrolled entity

Participants generally dismissed the risk of AI itself becoming an independent entity and security threat (in contrast to the concept paper produced before the workshop, which highlighted several AI leaders voicing such concerns). They stressed the need for a human in the loop to make the process and technology function. There was also general agreement that the crucial threat, or fear, is not AI as an uncontrollable entity, but rather the motivation or trustworthiness of the human in the loop. In other words, concerns were not about the technology; rather, they were about the people who understand and operate the technology and how they use it and the threats they may pose. Participants proposed scenarios in which AI system or platform employees with access to user data become targeted by terrorists in blackmail or extortion efforts. There is also risk that disgruntled or ideologically motivated employees seek extremist or terrorist actors for information sharing. The fallout from these scenarios intensifies with increasingly interconnected systems and users relying on AI systems for health and psychological care. Through the sale or transfer of user data, terrorists may be able to identify vulnerable individual for AI-enabled personalised radicalisation and recruitment. Another scenario is that AI-generated personalities become a substitute for human leadership – a possibility seemingly reflected in a January 2026 case by Sepehr Saryazdi who planned to firebomb an Australia Day event in the pursuit of a ‘cybernetics’ government.¹⁶

A Force Multiplier Framework for Understanding Terrorist Exploitation of AI

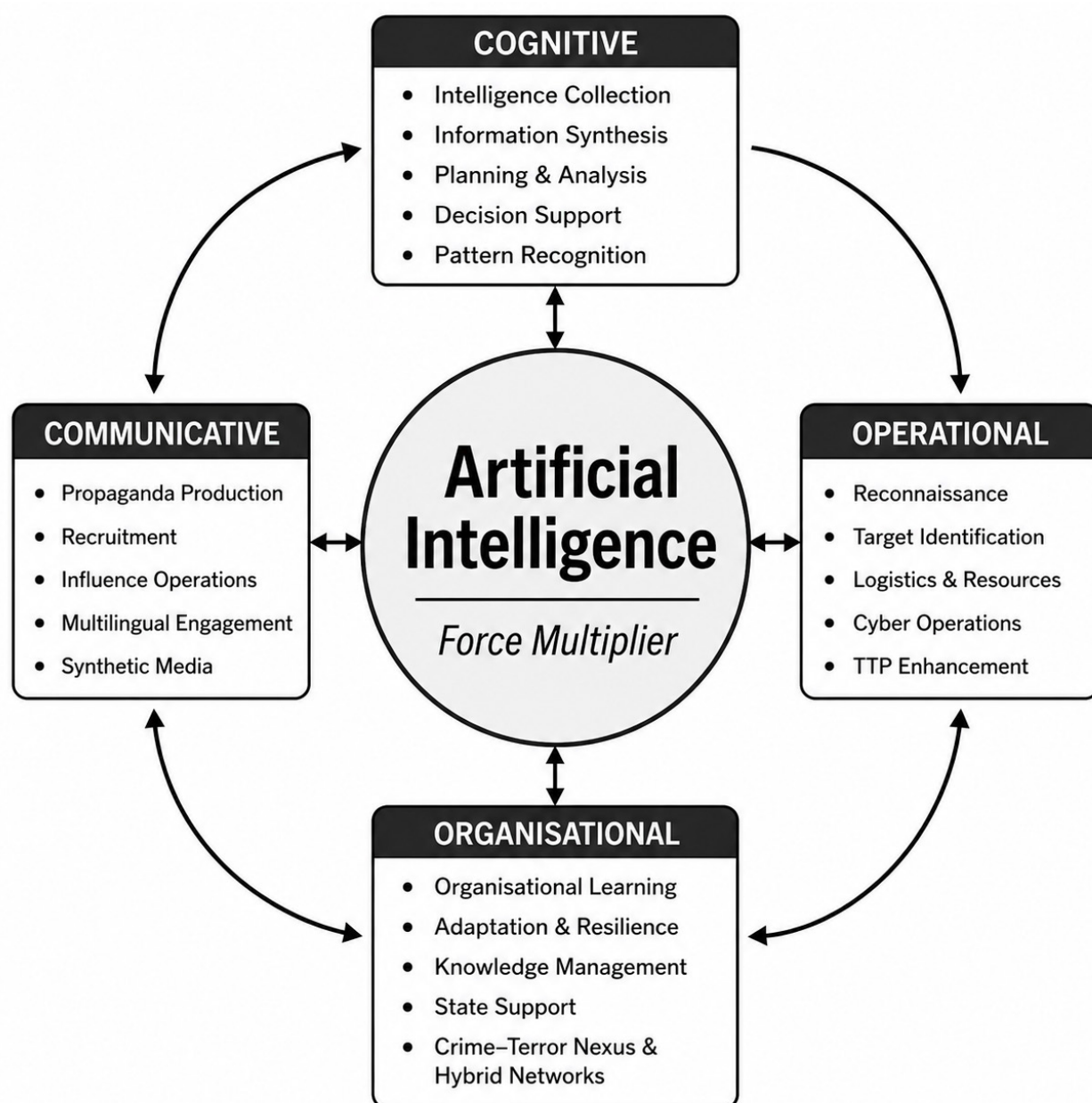
The multidisciplinary workshop examined diverse pathways through which terrorists can exploit AI. Across discussions spanning operational planning, propaganda, cyber capabilities, state support, and emerging AI ecosystems, one consistent observation emerged: AI is an enabling technology that enhances existing terrorist TTPs by reducing barriers to entry, accelerating planning, aiding decision-making, and increasing efficiency.

Synthesising these discussions produces the Force Multiplier Framework, which is a structured means for understanding how AI can be simultaneously exploited across multiple dimensions of terrorist activity. The framework conceptualises AI as an enabling capability across interconnected cognitive, operational, communicative, and organisational dimensions. Importantly, the framework does not imply that AI replaces human agency or fundamentally alters the motivations underlying terrorism. Instead, as workshop participants consistently emphasised, AI augments terrorist decision-making by increasing the efficiency, accessibility, and scalability of their existing TTPs and functions as a force multiplier. The framework is an analytical heuristic rather than a predictive model.

Cognitive Dimension

AI functions as a cognitive force multiplier by expanding the capacity of terrorists to acquire, synthesise, and exploit information while reducing the expertise and time traditionally required for intelligence gathering and operational planning.

Figure 1: illustrates how AI acts as a force multiplier across terrorist activities.



Operational Dimension

AI enhances existing operational capabilities by improving reconnaissance, logistics, target identification, cyber activity, and resource management. AI strengthens existing TTPs rather than introduce fundamentally new forms of violence.

Communicative Dimension

AI expands opportunities for propaganda production, multilingual engagement, recruitment, and influence by enabling increasingly sophisticated, appealing, and dynamic content while tailoring narratives to specific audiences and rapidly adapting messaging in response to changing events.

Organisational Dimension

AI strengthens organisational structures through which terrorist capabilities are acquired, shared, and refined. The workshop demonstrated that AI exploitation is increasingly affected by the wider ecosystems involving states, proxy organisations, organised crime, and decentralised AI communities.

Integrating the Framework

The value of the Force Multiplier Framework lies in recognising that these four dimensions are mutually reinforcing rather than independent. Improvements in one dimension likely generate opportunities across the others, producing cumulative effects that exceed the contribution of any individual AI capability. The framework provides researchers, practitioners, and policymakers with a practical means of assessing terrorist exploitation of AI as an interconnected system rather than a collection of isolated technological adaptations.

Conclusion and Recommendations

AI is evolving at a pace that challenges conventional approaches to understanding technological change and its implications for terrorism. Public debate frequently oscillates between exaggerated (as workshop participants concluded) doomsday expectations of AI-enabled terrorism and optimistic assumptions that existing safeguards will prevent malicious use. The multidisciplinary blue-sky workshop moved beyond these narratives by examining credible pathways through which terrorists can exploit AI over the short to medium term.

A consistent finding from the workshop is that AI is best understood as a force multiplier enabling technology rather than a discrete terrorist capability. Its significance lies in expanding opportunities to enhance existing terrorist TTPs, rather than fundamentally or systematically changing the motivations underlying terrorism or replacing human agency. Across operational planning, intelligence collection, propaganda, recruitment, cyber activities, organisational learning, and state-enabled pathways, participants repeatedly identified AI as a force multiplier that reduces barriers to entry, improves efficiency, and expands opportunities for exploitation. The challenge for researchers and practitioners is anticipating and understanding how terrorists can exploit AI in their pursuit of “perfecting” recruitment, radicalisation, and violence.

The workshop demonstrated that future terrorist exploitation of AI cannot be understood in isolation from the broader technological ecosystem. Open-source AI, commercial innovation, decentralised development, organised crime, proxy organisations, and state actors all influence the accessibility, diffusion, and application of AI capabilities. As these ecosystems continue to evolve, opportunities for terrorist exploitation are likely to emerge through an increasingly complex hybrid threat environment and state-crime-terror nexus.

Building on these findings, this research note proposes a Force Multiplier Framework that synthesises the workshop’s principal insights into four interconnected dimensions: cognitive, operational, communicative, and organisational. The framework provides a practical analytical tool that assists in systematically assessing how new technology (in this case AI) creates opportunities for terrorist exploitation across multiple domains simultaneously.

The workshop also demonstrates the value of multidisciplinary horizon-scanning and bluesky exercises for identifying emerging threats before they become operational realities. Bringing together expertise from terrorism studies, artificial intelligence, cyber security, law

enforcement and policing, intelligence, industry, and government enabled participants to assess terrorist exploitation of AI from multiple complementary perspectives that would be difficult to achieve otherwise. Continued collaboration is essential for refining threat assessments, validating emerging trends, and developing evidence-based approaches to countering terrorist exploitation of AI.

AI will continue to evolve, as will the opportunities for terrorist exploitation. Anticipating developments requires moving beyond technological determinism and reactive policymaking towards a more systematic understanding of how AI intersects with terrorist adaptation and innovation and evolving technological ecosystems. By synthesising the workshop findings and proposing the Force Multiplier Framework, this research note contributes to, and finds a foundation for, research into terrorist exploitation of AI, and countering it.

Joana Cook is an assistant professor at the Institute of Security and Global Affairs (ISGA) at Leiden University. Her research primarily focuses on rehabilitation and reintegration of terrorist-affiliated families, terrorist governance, and AI and terrorism. Her forthcoming book "Extreme Childhoods: Growing up in Families Affiliated with Violent Extremism and Terrorism" (co-authored with Dr Lynn Schneider) will be published by Columbia University Press in 2027.

Graig R. Klein is an assistant professor at the Institute of Security and Global Affairs (ISGA) at Leiden University. His research explores the instrumentality of political violence, primarily terrorism and protests, and how dissident-government interactions inform tactical and strategic evolution in conflict processes, international security, and national security. He leads the European Research Council (ERC) funded project Terrorist Group Adaptation & Lessons for Counterterrorism (ERC, TERGAP, 101116436).

Bàrbara Molas is a senior analyst with RAND's Defence, Security, and Justice team. Her work focuses on security-related research for policy development. She obtained her PhD at York University (2021, Toronto), and has since worked as an analyst of emerging threats for the United Nations Office for Counter-Terrorism and the International Centre for Counter-Terrorism, in addition to supporting law enforcement counterterrorism efforts in the UK and the EU.

Acknowledgements: The authors would like to thank the following for their support and assistance in the organization of the event: Dyon van Velzen, Rebecca Visser, Nina Prillwitz, and Antonio Ballesta.

Declaration of generative AI and AI-assisted technologies: The authors conceptualised and wrote the research note based directly off of the workshop. ChatGPT was used to check grammar and prompted to test the logical consistency of the research note. The authors designed Figure 1 through prompting and directly guiding ChatGPT.

Endnotes

- 1 Jackson, B. A. (2001). Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption. *Studies in Conflict & Terrorism* 24(3): 183-213. Dolnik, A. (2007). Understanding Terrorist Innovation: Technology, tactics and global trends. New York: Routledge. Cronin, A. K. (2020). Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists. Oxford: Oxford University Press. Silke, A., and Filippidou, A. (2020). What drives terrorist innovation? Lessons from Black September and Munich 1972. *Security Journal* 33: 210-27. Byman, D. (2026). Artificial Intelligence and the Future of Terrorism. *Center for Strategic & International Studies*. Lubrano, M. (2024). Choosing what (not) to do next: A preliminary theoretical framework on strategic innovation in terrorist organizations. *Dynamics of Asymmetric Conflict* 17(1): 1-22.
- 2 Glazzard, A., McIlhatton, D., and Martin, P. (2026). Will Generative AI Fundamentally Change Terrorist Threats? *CTC Sentinel* 19(5): 25-31. Cook, J., Klein, G. R., and Molas, B. (2024). Terrorist Exploitation of AI: A Concept Note. International Centre for Counter-Terrorism. Nelu, C. (2024). Exploitation of Generative AI by Terrorist Groups. International Centre for Counter-Terrorism.
- 3 Pfaff, C. A. (2025). Introduction: Terrorism and Artificial Intelligence. In *The Weaponization of Artificial Intelligence the Next Stage of Terrorism and Warfare*, Ed. C. Anthony Pfaff. pp. 7-22.
- 4 Kapsokoli, E. (2026). AI as an Enabler of Jihadist Terrorism. *International Journal of Intelligence and Counterintelligence* 39(3): 756-73.
- 5 See endnote 2 above.
- 6 Funding for the workshop was provided by the Netherlands' National Coordinator for Security and Counter-Terrorism (NCTV). There are no conflicts of interest and workshop hosts had full freedom to design and implement the proceedings. All discussion, analysis, and implications included in the research note are solely the authors' perspectives and do not represent the opinion, preference, or conclusions of NCTV (or Dutch government).
- 7 AI is one element of anti-tech terrorism, but not the sole driving force. The growth and predominant role in many countries is a defining factor for many anti-tech extremists. To date, pro-AI views or ideology have contributed to one planned terrorist attack in Australia.
- 8 Cao, J., Yao, J., Sun, S., Song, Z., and Zhang, F. (2025). Not all forms of artificial intelligence are perceived equal: AI functions and work outcomes. *Journal of Open Innovation: Technology, Market, and Complexity* 11(2): 1-17.
- 9 Juelich, A. (2026). "God had helped us, and so will AI": How the terrorist group Boko Haram Uses Frontier AI. Cambridge Programme on AI Science & Policy. University of Cambridge. p.53
- 10 Vosoughi, S., Roy, D., and Aral, S. (2018). The spread of true and false news online. *Science* 359: 1146-51.
- 11 Mahapatra, S. (2021). Digital Surveillance and the Threat to Civil Liberties in India. German Institute for Global and Area Studies: Focus Asia (<https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india>). George, R. (2023). The AI Assault on Women: What Iran's Tech Enabled Morality Laws Indicate for Women's Rights Movements. Council on Foreign Relations: Technology and Innovation (<https://www.cfr.org/articles/ai-assault-women-what-irans-tech-enabled-morality-laws-indicate-womens-rights-movements>). Goodfriend, S. (2023). Algorithmic State Violence: Automated Surveillance and Palestinian Dispossession in Hebron's Old City. *International Journal of Middle East Studies* 55(3): 461-78. Frenkel, S., and Krolik, A. (2026). How ICE Already Knows Who Minneapolis Protesters Are. *New York Times*, January 20, 2026
- 12 Mapping a Surge of Disinformation in Africa (2024). Africa Center for Strategic Studies (<https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-in-africa/>).
- 13 de Deus Pereira, J. (2025). From Drones to Data: Private Contractors and Cyber Mercenaries. Royal United Services Institute (RUSI) (<https://www.rusi.org/explore-our-research/publications/commentary/drones-data-private-contractors-and-cyber-mercenaries>).
- 14 Makarenko, T. (2004). The Crime-Terror Continuum: Tracing the Interplay Between Transnational

Organised Crime and Terrorism. *Global Crime* 6(1): 129-45.

- 15 Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal* 38(29): 1-23.
- 16 Australian Associated Press, "Queensland PhD candidate accused of plotting to firebomb Australia Day event wanted AI-driven society, court hears," *The Guardian*, 22 January 2026. <https://www.theguardian.com/australia-news/2026/jan/22/queensland-phd-candidate-accused-plotting-firebomb-australia-day-event-ntwnfb>"

About

Perspectives on Terrorism

Established in 2007, *Perspectives on Terrorism* (PT) is a quarterly, peer-reviewed, and open-access academic journal. PT is a publication of the International Centre for Counter-Terrorism (ICCT), in partnership with the Institute of Security and Global Affairs (ISGA) at Leiden University, and the Handa Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews.

Copyright and Licensing

Perspectives on Terrorism publications are published in open access format and distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License, which permits non-commercial reuse, distribution, and reproduction in any medium, provided the original work is properly cited, the source referenced, and is not altered, transformed, or built upon in any way. Alteration or commercial use requires explicit prior authorisation from the International Centre for Counter-Terrorism and all author(s).

© 2023 ICCT

Contact

E: pt.editor@icct.nl

W: pt.icct.nl

