מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

The Use of Artificial Intelligence and Advanced Technologies by Terrorist Organizations

Gabi Siboni
Simon Tsipsis

מכון ירושלים לאסטרטגיה ולביטחון
The Jerusalem Institute
for Strategy and Security

The Use of Artificial Intelligence and Advanced Technologies by Terrorist Organizations

Gabi Siboni
Simon Tsipsis

October 2025

The Use of Artificial Intelligence and Advanced Technologies by Terrorist Organizations

1. Introduction

Cyber capabilities and artificial intelligence have become central components of how terrorist and guerrilla organizations operate today. These groups rely on such tools to adapt to the challenges posed by the advanced technologies employed by state security and law enforcement, expand their operational reach, inflict greater damage, and reduce costs, resource requirements, and direct physical contact with security forces that could endanger them. Internet-based technologies—such as social networks, online discussion platforms, content channels, digital currencies, and hacking tools—enable terrorist organizations to disseminate propaganda, recruit supporters and fighters, raise funds and donations, and maintain anonymity, making them harder to detect and apprehend. Digitization has improved the management of critical infrastructure but has also increased its vulnerability to exploitation by hostile groups.

Cyber tools and artificial intelligence also allow terrorist and guerrilla organizations to conduct warfare more efficiently and lower their operational costs. One of the most significant advantages is the ability to radicalize large numbers of supporters worldwide through cyber means—an achievement that far surpasses what was possible in the past. The sowing of fear and the undermining of governance, which are central objectives of terrorism, represent another dimension enabled by cyber capabilities as a method of contemporary warfare.

Fundraising and financing terrorism are also significant outcomes made possible by a wide range of online platforms that enable near-unlimited fundraising, recruiting and independence from state sponsors (such as states that support and/or finance terrorism), thereby allowing for greater ideological, political, and geographic freedom of action. Engagement with cyber tools and artificial intelligence also raises the level of specialization and expertise among terrorist and guerrilla operatives. In turn, this creates a greater degree of parity between fighters in asymmetric organizations and the security forces of states and authorities confronting them.

Terrorist organizations, guerrilla and rebel groups are not the only actors to have adopted artificial intelligence and cyber capabilities. A convergence is underway among these groups and transnational organized crime. What began during the Cold War as an overlap between drug trafficking and revolutionary movements in Latin America—where drug trafficking provided funding for insurgents and guerrilla organizations supplied weapons

to narco-traffickers—has evolved into a unified anti-government struggle in which both spheres share digital knowledge and capabilities. As a result, drug cartels in Latin America are adopting cyber and artificial intelligence capabilities in their confrontations with local security forces. The far right has likewise adopted these tools in its efforts to undermine adversary governments.

2. Advanced Technologies in Use by Terrorist Organizations

2.1 Military Research and Development in the Service of Terrorist and Guerrilla Groups

Throughout history, military research and development (R&D) has significantly shaped non-state actors, including terrorist and guerrilla groups. This influence has flowed through technology diffusion, black-market procurement, and the adaptation of open-source innovations and unclassified developments, often via captured equipment, reverse engineering, or commercial offshoots of military technology.

Military R&D is primarily driven by state actors such as the United States, the Soviet Union (and later Russia), China, and other countries. It focuses on weapons, methods of warfare, cyber systems, and intelligence, including artificial intelligence. Research and development in these domains can leak and spread—whether inadvertently or deliberately—to unauthorized actors through multiple pathways.

Surplus or stolen military weapons and equipment from wars and conflicts worldwide reach the black market, arming groups across the Middle East, Africa, and Latin America. Guerrilla methods developed in twentieth-century conflicts (for example, by Mao Zedong or Che Guevara) which included "hit-and-run" ambushes and psychological operations today are combined with the uptake of military technological R&D outputs and dual-use technologies, such as drones or explosive-detection capabilities. Military research and development outcomes and products have also become accessible through commercial markets or via the leakage of open-source code (intelligence work conducted through OSINT—open-source intelligence).

In addition, groups may also receive support from rival states, granting them access to military R&D outputs—like for example, during Cold War proxy wars. This dynamic was evident among states that supported and financed terrorism and state-sponsored terrorist activity, such as Libya under Muammar Gaddafi, Syria under Bashar and Hafez Assad, and Iraq under Saddam Hussein. During the Cold War, some groups and organizations, including terrorist and guerrilla groups, obtained advanced military developments from Russia, North Korea, Cuba, and China through close military cooperation, a pattern that, in all likelihood, persists today.

Guerrilla groups, which often fight for political and ideological objectives, differ from terrorist organizations in scale and purpose: guerrillas typically target military forces, whereas terrorist actors focus on civilians for maximum publicity and to sow fear. Both, however, exploit asymmetries in the use of military research and development. This distinction is flexible, as reflected in ongoing debates over how states label and classify adversaries for political reasons.[1]

2.2 Examples of the Diffusion of Military Technologies

One striking example is the iconic firearms and small arms such as the AK-47 that emerged from Soviet R&D in the 1940s' and was mass-produced, copied, and distributed worldwide. Their reliability made them the weapon of choice for guerrilla groups in Vietnam, Afghanistan, and Latin America, including organizations such as Colombia's FARC, Vietcong, Mujaheddin and others, for decades. Terrorist organizations in the Middle East similarly adopted a wide range of AK-47 variants through smuggling networks.

Explosives, improvised explosive devices, and military-grade munitions derived from ammunition R&D (such as U.S. programs during World War II and subsequent conflicts) have been repurposed by insurgent groups worldwide. In Iraq and Afghanistan, organizations such as al-Qaeda and the Taliban produced IEDs from unexploded ordnance or commercial fertilizer, modifying these materials to produce anti-vehicle mines. This pattern reflects guerrilla tactics that emphasize the use of low-cost weapons adapted for advanced military purposes.[2]

Drones and unmanned systems originally developed within U.S. military R&D frameworks—such as DARPA programs beginning in the early 2000s—have made their way into the hands of terrorist actors. Commercial drones were weaponized by groups such as ISIS for reconnaissance and bombing missions in Syria and Iraq. Looking ahead, the adaptation of advanced features, such as drone swarms or AI-enabled targeting, represents a growing risk. Reports from conflict zones also indicate that some groups are acquiring military-grade drones through smuggling channels.[3]

Cyber tools and electronic-warfare capabilities originating in state-level research and development, such as hacking software or signal jammers, have been used by non-state groups for break-in cyber operations, propaganda, disruption, and intelligence collection. Hezbollah in Lebanon, for example, has employed electronic warfare influenced by

[2] Guerilla Warfare & Law Enforcement: Combating the 21st Century Terrorist Cell within the U.S." Journal of Strategic Security 2 (4): 39–52. https://digitalcommons.usf. edu/cgi/viewcontent.cgi?article=1066&context=jss.
[3] Thomas G. Pledger. 2021. "The Role of Drones in Future Terrorist Attacks." The Association of the United States Army 137 (Land Warfare Paper). https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

Iranian military technology, including the jamming of Israeli drones.[4] The organization has claimed and demonstrated successes in downing Israeli surveillance UAVs, including Hermes 450, Hermes 900, and Skylark models, using surface-to-air missiles (SAMs).

These interception capabilities rely on sophisticated air-defense systems acquired from and adapted by foreign sources such as Iran and Syria, requiring substantial R&D integration to be effective against advanced Israeli drones. Hezbollah operatives have also dismantled captured drones to reverse-engineer their components, thereby enhancing their capabilities through military R&D processes.[5] Cyberattacks conducted by groups such as Anonymous or by state-backed hackers further illustrate how exposed methods proliferate.[6]

Advanced surveillance technologies and artificial intelligence may reach terrorist and guerrilla organizations through military cooperation and exports. Israeli military R&D products in the field of AI-based systems, tested in combat, have been exported worldwide and have, at times, been adopted by non-state actors through leaks or reverse engineering. Guerrilla groups also use commercial adaptations of military biological sensors (biosensors) or predictive technologies for intrusion and penetration activities.[7]

The non-conventional domain has not been immune to these dynamics as well. The question of whether asymmetric groups and organizations can gain access to biological and chemical tools remains pertinent. Historical research and development in biological weapons—for example, U.S. programs in the mid-twentieth century—has inspired limited terrorist use, such as the 1995 sarin attack carried out by Aum Shinrikyo in Japan, by drawing on non-classified knowledge of its production. Concerns are also growing over the potential manipulation of genes or the misuse of virus-based sensors originating in military laboratories.[8]

2.3 Interim Summary

Terrorist organizations have fused guerrilla tactics with technologies derived from military R&D to offset the advantages of superior adversaries. This dynamic has, in turn, driven countervailing R&D efforts, including U.S. military initiatives in counter-drone defenses

[4] Maya Gebeily, and Laila Bassam. 2024. "How Hezbollah Used Pagers and Couriers to Counter Israel's High Tech Surveillance." Reuters, June 9, 2024. https://www.reuters.com/world/middle-east/pagers-drones-how-hezbollah-aims-counter-israels-high- tech-surveillance-2024-07-09.

[5] "Hezbollah Shoots Down Israeli Drone with Surface-to-Air Missiles." Foundation for Defense of Democracies. February 26, 2024. https://www.fdd.org/analysis/2024/02/26/hezbollah-shoots-down-israeli-drone-with-surface-to-air- missiles

[6] Terry Gross. 2021. "U.S. Cyber Weapons Were Leaked — And Are Now Being Used Against Us, Reporter Says." NPR. February 10, 2021. https://www.npr.org/2021/02/10/966254916/u-s-cyber-weapons-were-leaked-and-are-now-being-used-against-us-reporter-says.

[7] @grimeywun in X. 2025. "AI Tools Deployed on Palestinians." X. X. https://x.com/grimeywun/status/1968027043590967613?referrer=grok-com.

[8] "Hyperspectral Reporters for Long-Distance and Wide- Area Detection of Gene Expression in Living Bacteria." Nature Biotechnology, August.

and deepening its research in behavioral prediction. At the same time, the spread of weapons and military technologies raises ethical concerns, as systems designed for protection can also violate privacy and perpetuate cycles of violence.

Conspiracy theorists claim that agencies such as the Central Intelligence Agency deliberately develop tools that end up in the hands of adversaries for geopolitical reasons; these claims, however, rely on little more than declassified CIA programs, such as the MKUltra behavioral experiments,[9] conducted by the CIA in the early 1950s.[10] Overall, while military research and development confers strategic advantages on states, its unintended diffusion highlights the challenges of arms control in a globalized world.

3. Cyber Warfare by Terrorist Organizations

Terrorist and guerrilla organizations are increasingly integrating cyber warfare into their asymmetric warfare doctrines, leveraging digital tools to amplify their impact while minimizing direct physical risk and reducing costs in resources and manpower. This approach enables non-state actors to strike states, infrastructure, and civilian populations worldwide, often within hybrid warfare frameworks that combine online activity with traditional kinetic activity tactics in insurgency and terrorism campaigns.

3.1 Primary Methods of Cyber Warfare Used by Terrorist Organizations

Terrorist groups use social media, websites, and online forums for propaganda campaigns and disinformation operations aimed at instilling extremist ideologies, spreading false narratives, and conducting psychological operations designed to radicalize individuals, sow fear, and undermine public trust in government institutions. Violent extremist organizations, for example, exploit platforms such as X and YouTube to reach broad audiences and frame their actions as legitimate in search for support.[11] This method is particularly effective for terrorist and guerrilla movements in protracted conflicts, where online narratives can mobilize support and demoralize adversaries.

Cyber tools enable direct outreach to supportive communities and potential recruits through chat rooms, encrypted applications, and targeted online content. Terrorist groups publish recruitment materials, including operational guides and training manuals, and circulate calls to action to attract and instruct supporters. These efforts often focus on vulnerable demographic groups such as youth,[12] the unemployed, homeless, and

[9] Robert Brown Asprey. 2025. "Guerrilla Warfare." Britannica, August. https://www.britannica.com/topic/guerrilla-warfare. Also in L'America in X. 2025. "U.S. Government Mind Control & Behavioral Experiments (1920s–1970s)." X. X. https://x.com/MFTXAC/status/196 7745798692643204?referrer=grok-com.

[10] U.S. Government Printing Office. 1977. Project MKUProject MKULTRA, the CIA's Program of Research in Behavioral Modification. https://books.google.co.il/books?id=TEqhqtrF3XEC&pg=PA70&redir_esc=y#v=onepage&q&f=false.

[11] Norwich University. n.d. "Information Warfare and Terrorism: How Extremist Organizations Exploit Modern Platforms." Accessed September 8, 2025. https://online.norwich.edu/online/about/resource-library/info-warfare-terrorism.

[12] Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf

individuals with criminal backgrounds. Guerrilla movements employ similar methods to build activist networks and coordinate operations.

Cyber capabilities also facilitate intelligence collection and data mining from open sources. Open-source information from the internet—including public databases, news outlets, and social media—is gathered to identify targets, vulnerabilities, and operational intelligence. This collection can include reconnaissance of critical infrastructure such as power plants or transportation systems without the need for any on-site physical presence, for example, through the use of mapping services that provide up-to-date imagery of nearly any location worldwide.[13]

Online systems enable the transfer of donations, fundraising, and resource acquisition through websites, decentralized cryptocurrencies, or charitable networks, thereby sustaining terrorist and guerrilla activity. Some organizations provide bank details or use chat rooms to solicit donations and collect funds from supporters around the world. Online donations through various means of internet communication also allow contributors to remain anonymous.[14]

Encrypted communications and decentralized online network structures—used for recruitment, fundraising, propaganda, and related activities—help maintain loose undetected connections among active terrorist cells while enabling real-time planning and cooperation across national borders. Such coordination is critical to guerrilla warfare, where dispersed units must synchronize attacks and share tactics.[15]

Terrorist and guerrilla organizations conduct cyberattacks and disruption operations, including hacking government systems, launching distributed denial-of-service (DDoS) attacks, and targeting critical infrastructure such as hospitals, power grids, and financial networks, including pension funds, to inflict economic damage and generate fear. State-sponsored terrorist actors or proxies, such as those linked to Iran today (and linked to Libya in past), have intensified these methods to heighten geopolitical tensions.[16] Guerrilla forces operating in active war zones, such as Syria or Ukraine, also utilize electronic warfare to disrupt adversary communications and support their ground operations.[17]

---

[13] Andre Slonopas. 2024. "What Is Cyber Warfare? Various Strategies for Preventing It." American Public University. April 16, 2024. https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare. Also in Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

[14] Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf

[15] Cleveresq in X. 2024. "Hybrid Warfare Is a Good Description of What Russia Is Doing, Has Done, and Continues to Do." X. X. https://x.com/cleveresq/status/1788173986079113600?referrer=grok-com. Also in Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

[16] Andre Slonopas. 2024. "What Is Cyber Warfare? Various Strategies for Preventing It." American Public University. April 16, 2024. https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare.

[17] InfoSiftWeekly in X. 2024. "Cyber Attacks - HIGH Threat Level." X. X. https://x.com/InfoSiftWeekly/status/1865724584437108759?referrer=grok-com.

DarkNet websites and forums enable the covert sharing of operational knowledge and host manuals covering tactics ranging from constructing improvised explosive devices to executing cyber operations, facilitating knowledge transfer among organizational branches and cells. This tool effectively renders sophisticated and specialized expertise widely accessible to terrorist and guerrilla non-state actors.[18]

These methods are often part of a broader integrated warfare concept, in which cyber elements complement physical operations.[19] Groups such as the Islamic State, Al-Qaeda, Hamas, and various rebel factions in ongoing conflicts (against Western interests for example in Syria, Iraq and Afghanistan) illustrate this evolution, adapting to the digital environment to achieve broader objectives.[20] At the same time, countermeasures by governments, including enhanced monitoring and international cooperation, continue to challenge these efforts.[21]

4. The Use of Artificial Intelligence by Terrorist Organizations

Terrorist and guerrilla groups are incorporating artificial intelligence (AI) into their psychological warfare strategies, which seek to manipulate perceptions, emotions, and behavior to undermine adversaries, recruit supporters, or spread fear. Such use often focuses on amplifying propaganda efforts, disseminating disinformation, and enabling large-scale recruitment; it should be noted that much of the documented activity in these domains remains experimental, ad hoc, and unsophisticated. The following section outlines key ways in which these practices have been observed or analyzed, drawing on reporting related to groups such as the Islamic State, Hezbollah, and various other extremist networks.

4.1 The Use of Artificial Intelligence for Psychological Warfare

Artificial intelligence tools, particularly those based on large language models (LLMs) or image and video generators, enable the rapid generation of propaganda and disinformation, including customized content, designed to elicit strong emotional responses such as fear, anger or solidarity.[22]

---

[18] Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

[19] Kyle.Moon in X. 2025. "I Have a Feeling This Is the Beginning of Hybrid Warfare by USA on Mexico. Analogous to Russo-Georgian Conflict 2008-2009." X. X. https://x.com/GanseKyle/status/1892951048807141778?referrer=grok-com. Also in Cleveresq in X. 2024. "Hybrid Warfare Is a Good Description of What Russia Is Doing, Has Done, and Continues to Do." X. X. https://x.com/ cleveresq/status/1788173986079113600?referrer=grok-com.

[20] Gabriel Weimann. 2024. "How Modern Terrorism Uses the Internet." http://usip.org/sites/default/files/sr116.pdf.

[21] OSCE. n.d. "Countering the Use of the Internet for Terrorist Purposes." Organization for Security and Cooperation in Europe. Accessed September 8, 2025. https://www.osce.org/secretariat/107810.

[22] Large language models (LLMs) are a subset of machine learning known as deep learning. They use algorithms that operate on very large datasets to identify complex patterns. At a fundamental level, LLMs learn to respond to user prompts with contextually relevant content written in human language—that is, using the vocabulary and syntax people employ in ordinary conversation. In other words, LLMs constitute an advanced subcategory of artificial intelligence focused on understanding, predicting, and generating human-like text. LLMs are a critical component of AI capability, making them powerful tools for a wide range of natural-language processing tasks, including search, translation and text summarization, question answering, and the creation of new content, including text, images, music, and software code. See: "What Is a Large Language Model?", SAP, July 2024.

These groups use AI to generate deepfakes—realistic videos and articles depicting fabricated atrocities, glorifying fighters, or demonizing the enemy. For example, AI-generated images of alleged war crimes can be circulated on social media to provoke outrage or boost morale among supporters. This capability significantly enhances the effectiveness of propaganda efforts.

Rather than relying on manual editing, AI automates the process, enabling multilingual content tailored to specific demographic groups, such as vulnerable youth in conflict zones, Third World, developing countries, or other high-risk areas. The objective is to undermine trust in official sources, generate confusion, and polarize public opinion.[23]

Groups also employ AI for targeted recruitment and radicalization. AI algorithms help identify and engage potential recruits by analyzing online behavior, social media interactions, and publicly available data. Chatbots[24] or AI-driven messaging systems simulate human conversation to build rapport, answer ideological questions, and guide individuals toward extremist views. These tools can operate continuously, adapt responses based on user sentiment, and deepen engagement, thereby enabling the recruitment of a far larger numbers of supporters and fighters than in the past.[25]

AI-driven sentiment analysis scans forums, comments, and posts to identify individuals displaying signs of frustration or anger and then delivers tailored propaganda. While this approach mirrors commercial marketing techniques, it is weaponized for ideological persuasion and often leads to online radicalization that spills over into real-world actions, such as lone-actor terrorist attacks.[26]

In psychological operations, AI enhances efforts to instill fear and terror without direct physical violence by focusing on digital disruption. Automated Bots flood social media platforms with coordinated disinformation and propaganda campaigns, such as false reports of ongoing attacks or exaggerated claims of strength, in order to create panic and force security services to divert resources.[27]

---

[23] Jim Stewartson, Antifascist in X. 2024. "The Failure to Recognize the Power of Psychological Warfare on Civilians May End up Being *the* Fatal Error." X. X. https://x.com/jimstewartson/status/1846392462266478840?re

[24] A chatbot is a computer program that simulates and processes human conversation (in writing or speech), allowing people to interact with digital devices as if they were communicating with a real person. Chatbots can be simple—such as basic programs that respond to a straightforward query with a single-line answer—or sophisticated, such as digital assistants that learn and evolve to provide increasing levels of personalization as they collect and process information. See: "What Is a Chatbot?", Oracle, https://www.oracle.com/il/chatbots/what-is-a-chatbot/.

[25] Lidia Bernd. n.d. "AI-Enabled Deception: The New Arena of Counterterrorism." Georgetown University, no. Georgetown Security Studies Review. Accessed September 19, 2025. https://gssr.georgetown.edu/the-forum/topics/technology/ai-enabled- deception-the-new-arena-of-counterterrorism.

[26] Maverick News Agency in X. 2025. "The Most Concerning Version Is an 'Untethered' AI Is Doing It through Social Platforms." X. X. https://x.com/mavnewsagency/status/1966917963346571693?referrer=grok-co

[27] Austin Coombs. 2024. "Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment." Modern War Institute, October. https://mwi.westpoint.edu/persuade-change-and-influence-with-ai-leveraging-artificial-intelligence-in-the-information-environment.

Some groups are experimenting with AI for predictive modeling of public reactions, simulating how particular messages might spread virally to maximize psychological impact. These experiments also include the use of AI to fabricate documents or audio recordings that sow distrust within enemy ranks, including among civilian populations.[28]

4.1.1 Challenges and Limitations

While artificial intelligence offers advantages in speed and scale, its adoption by these groups is constrained by the need for access to advanced technology, technical expertise, and supporting infrastructure. Most groups rely on publicly available tools rather than customized systems. At the same time, countermeasures such as content moderation and AI detection are being developed by authorities to address the use of artificial intelligence by terrorist and organized crime groups. Reports indicate that state actors and counterterrorism efforts are increasingly focused on monitoring and disrupting the use of these tools to maintain a degree of control and oversight and to prevent their further diffusion.[29]

Overall, artificial intelligence functions as a force multiplier for psychological warfare by enabling more efficient, targeted, and deceptive operations, but it remains part of a broader toolkit that also includes traditional methods such as leaflet distribution, propaganda in mosques (in the context of radical Islam), and online broadcasts.

4.2 Terrorism and Artificial Intelligence in the Middle East

Terrorist and guerrilla organizations in the Middle East, including groups such as the Islamic State (ISIS), Al-Qaeda affiliates, Hezbollah, and Hamas, have begun experimenting with AI technologies.

This adoption is largely driven by access to general-purpose AI tools such as ChatGPT, which allow these groups to enhance their operations without requiring advanced technical expertise.

While the use of AI remains at an early stage and is not yet operationally relevant for physical attacks, it advances and amplifies existing practices such as propaganda dissemination and recruitment. Reports by counterterrorism experts, research institutes, and media outlets indicate that these groups are adapting AI to overcome constraints, produce digital multimedia content, and explore applications such as future cyber

[28] The Chronology in X. 2025. "From CIA, ISI Learnt Many Techniques of Psychological Warfare Which CIA Was Using to Train Mujahedeen." X. X. https://x.com/TheChronology__/status/1938559139879563542?referrer=grok-com.
[29] Clarisa Nelu. 2024. "Exploitation of Generative AI by Terrorist Groups." International Centre for Counter-Terrorism (ICCT). June 10, 2024. https://icct.nl/publication/exploitation-generative-ai-terrorist-groups. Also in UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.p

operations and technologies. At the same time, much of the available information derives from Western and international sources, which may be biased in their assessment of the threats posed by Islamist groups. In contrast, relatively little information exists regarding the use of AI by state actors, particularly state security forces and intelligence services.[30]

4.2.1 Reported Cases

The most extensively documented application of AI by these organizations is in propaganda and content creation. Generative AI enables the rapid production of text, images, video, and audio that mimic professional media, helping groups evade automated detection on social platforms. For example, ISIS supporters have reportedly used tools such as ChatGPT to produce "news bulletins," converting written propaganda into audio segments or fabricated broadcasts about attacks in regions such as Africa and the Middle East.[31]

Groups linked to Al-Qaeda have published guides on using AI chatbots and announced online workshops to train followers in these technologies.[32] Such use facilitates the creation of "emotive content" designed to motivate supporters, including AI-generated videos depicting U.S. presidents singing ISIS war songs or manipulative images circulated within extremist networks.[33]

AI is also leveraged for recruitment and radicalization. By generating persuasive, high-impact narratives, these tools help tailor messages to specific communities, including fundraising campaigns that employ compelling language—for example, portraying ISIS as struggling with "corrupt and oppressive governments."[34] In 2023, ISIS circulated a guide on the secure use of generative AI, emphasizing its role in evading censorship and disseminating extremist messaging.[35]

Some evidence points to "operational improvements," such as the use of AI for website development, creating apps, or basic planning. Terrorist actors have experimented with

[30] The Soufan Center. 2024. "Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment E orts." October 3, 2024. https://thesoufancenter.org/intelbrief-2024-october-3.
[31] Makuch, ben. 2025. "They're Fighting Dirty. We're Fighting Back." The Guardian, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence. Also in Cathrin Schaer. 2024. "How Extremist Groups like 'Islamic State' Are Using AI." DW, October 7, 2024. https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398.
[32] Cathrin Schaer. 2024. "How Extremist Groups like 'Islamic State' Are Using AI." DW, October 7, 2024. https://www.dw.com/en/ how-extremist-groups-like-islamic-state-are-using-ai/a-69609398.
[33] Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." Combating Terrorism Center 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation.
[34] Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." Combating Terrorism Center 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation. Also in Lidia Bernd. 2024. "AI-Enabled Deception: The New Arena of Counterterrorism." Georgetown Security Studies Review, no. Cyber&Artificial Intelligence, Terrorism&Transnational Threats (May). https://georgetownsecuritystudiesreview.org/2024/05/03/ai-enabled-deception-the-new-arena-of-counterterrorism.
[35] INTELBRIEF. 2024. "Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment E orts." October 3, 2024. https://thesoufancenter.org/intelbrief-2024-october-3.

advanced programming language models (such as LLMs) to generate instructions for activities such as disinformation campaigns or fundraising, often employing indirect prompts to bypass AI safeguards.[36] Regional groups, including those associated with violent extremist organizations, have shared more than 5,000 AI-generated content items online, primarily to amplify propaganda rather than to enable direct attacks.[37]

Guerrilla organizations, such as those operating in Syria or Yemen (for example, the Houthis), have shown limited adoption of AI. Nevertheless, broader regional trends suggest comparable experimentation in asymmetric warfare, including the integration of AI with drones for targeting purposes, although this remains speculative and is not yet well substantiated in open sources.[38]

4.2.2 Potential Risks and Future Implications

Artificial intelligence may enable more sophisticated threats, including cyberattacks, autonomous weapons operation, and enhanced planning for fraud, recruitment, propaganda, and financing. For example, it could support the development of ransomware, distributed denial-of-service (DDoS) attacks, or even designs for chemical or biological weapons, although current applications remain largely confined to scaling existing methods and to research and development by terrorist organizations with limited access to advanced capabilities.[39]

Terrorist groups could use AI for recruitment through Chatbots or for orchestrating complex attacks, as illustrated in hypothetical scenarios where AI is combined with drone technology to produce "killer robots."[40] Reports by the United Nations highlight the "malicious use" of artificial intelligence for terrorist purposes, underscoring particular risks in the Middle East, where groups such as the Islamic State have a track record of adopting emerging and advanced technologies.[41]

---

[36] Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." Combating Terrorism Center 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation.

[37] Tech Against Terrorism. n.d. "Terrorist Use of Generative AI ." Tech Against Terrorism. Accessed September 1, 2025. https://techagainstterrorism.org/gen-ai.

[38] Jacob Ware. 2019. "Terrorist Groups, Artificial Intelligence, and Killer Drones." War On The Rocks. September 24, 2019. https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones. Also in Vision of Humanity. 2023. Preventing Terrorists from Using Emerging Technologies." Vision of Humanity, September. https://www.visionofhumanity.org/ preventing-terrorists-from-using-emerging-technologies.

[39] Clarisa Nelu. 2024. "Exploitation of Generative AI by Terrorist Groups." International Centre for Counter-Terrorism (ICCT). June 10, 2024. https://icct.nl/publication/exploitation-generative-ai-terrorist-groups. Also in UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

[40] Jacob Ware. 2019. "Terrorist Groups, Artificial Intelligence, and Killer Drones." War On The Rocks. September 24, 2019. https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones. Also in Anthony C. Pfaf. 2025. "The Weaponization of Artificial Intelligence the Next Stage of Terrorism and Warfare." Ankara. https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf.

[41] UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

At the same time, some analyses downplay the immediacy of these risks, arguing that artificial intelligence supplements existing threats rather than transforming them, and that "real-world" attacks related to propaganda and recruitment remain heavily dependent on geopolitical factors such as the conflict in Gaza.[42] Stakeholder outlets and research bodies such as the Institute for Strategic Dialogue (ISD) and the Combating Terrorism Center (CTC) emphasize that vulnerabilities stem more from a decline in resilience to online extremism than from artificial intelligence itself.[43]

4.2.3 Countermeasures and the Broader Context

International efforts, including NATO's focus on counterterrorism technologies and initiatives led by the United Nations, aim to contain these risks through intelligence sharing, training, and policy responses.[44] Technology platforms are being urged to strengthen content moderation through AI-enabled tools (AI-based cybersecurity), such as semantic detection, to counter evasion techniques.[45] Reports from diverse sources, including U.S. research institutes and European media outlets, aggregate assessments and perspectives, though they often prioritize threats posed by non-state actors over state uses of artificial intelligence.[46]

In conclusion, while artificial intelligence is enhancing and accelerating the ability of terrorist and guerrilla groups in the Middle East to expand digital operations, its current impact is evolutionary rather than revolutionary and is concentrated primarily in the realm of information warfare. Ongoing monitoring by global institutions is essential in addressing these growing risks.

4.3 The Use of Artificial Intelligence by Drug Cartels in Latin America

Mexican drug cartels—most notably the Jalisco New Generation Cartel (CJNG) and the Sinaloa Cartel—are increasingly adopting artificial intelligence (AI) to enhance their criminal operations. What follows is an overview based on currently available information.

[42] Cathrin Schaer. 2024. "How Extremist Groups like 'Islamic State' Are Using AI." DW, October 7, 2024. https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398. Also in David Wells. 2024. "The Next Paradigm-Shattering Threat? Right-Sizing the Potential Impacts of Generative AI on Terrorism." Middle East Institute. March 18, 2024. https://mei.edu/publications/next-paradigm-shattering-threat-right-sizing-potential-impacts-generative-ai-terrorism

[43] Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." The Guardian, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence. Also in Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." Combating Terrorism Center 17 (1). https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation

[44] NATO. 2025. "Countering Terrorism." Nato.Int. August 6, 2025. https://www.nato.int/cps/en/natohq/topics_77646.htm

[45] Tech Against Terrorism. n.d. "Terrorist Use of Generative AI." Tech Against Terrorism. Accessed September 1, 2025. https://techagainstterrorism.org/gen-ai.

[46] Susan Sim, Eric Hartunian, and Paul J. Milas. 2024. "Emerging Technologies and Terrorism: An American Perspective." Strategic Studies Institute USAWC Press (April). https://press.armywarcollege.edu/monographs/967. Also in Asha Hemrajani. 2024. "The Use of AI in Terrorism." RSIS, no. 124 (August). https://rsis.edu.sg/wp-content/uploads/2024/08/CO24124.pdf

4.3.1 Financial Fraud and Cybercrime

Cartels such as CJNG use artificial intelligence, including large language models (LLMs), to carry out sophisticated fraud campaigns and more advanced forms of financial fraud. This includes the creation of phishing emails, deep impersonation, and automated fraud schemes that mimic legitimate communications to deceive victims (such as fake stock-trading platforms that imitate real trading activity). Artificial intelligence helps cartels create personalized messages to trick individuals into sharing information, providing personal data such as passwords, or disclosing sensitive credentials.[47]

Artificial intelligence is also used to obscure the origins of illicit funds and facilitate large-scale money laundering. The cartels employ AI-based analysis to identify patterns in financial data, enabling them to launder money through decentralized currencies or complex networks of shell companies. This capability allows them to evade detection by authorities.[48]

4.3.2 Human Trafficking and Recruitment

According to reports, the CJNG cartel utilizes artificial intelligence to expand its human trafficking operations and lure individuals into illegal activities under the guise of legitimate job offers. AI tools assist in automating recruitment processes, including coercion and deception, while targeting vulnerable populations via social media platforms.[49]

Cartels exploit social media and leverage AI-based facial recognition and data analysis to identify and recruit drug traffickers, for example truck drivers to transport and deliver drug loads without their knowledge of the cargo, by using platforms such as Facebook. For example, a federal investigation used AI-based facial recognition to identify a recruiter after a year of inactivity, illustrating how cartels exploit these platforms for recruitment.[50]

4.3.3 Drone-Based Warfare and Surveillance

The CJNG cartel was a pioneer in using armed AI-enabled drones for both surveillance and attacks. These drones, equipped with sensors and cameras, are utilized to monitor rival cartels, track drug shipments, and even deliver explosives and weapons in conflicts

[47] AI incident database. n.d. "Incident 725: Cartels Reportedly Using AI to Expand Operations into Financial Fraud and Human Tra cking." Accessed August 31, 2025. https://incidentdatabase.ai/cite/725.
[48] AP news. 2022. "Mexican Cartels Turn to Bitcoin, Internet, e-Commerce." March 10, 2022. https://apnews.com/article/business-caribbean-mexico-crime-drug-cartels-1bb5ebf84fbf71baf6a845648bad4990. Also in Robert Muggah, and Misha Glenny. 2025. "The Coming Golden Age of Crime." FP. February 17, 2025. https://foreignpolicy.com/2025/02/17/drug-cartels-organized-crime- mafia-cybercrime-money-laundering-corruption-smuggling.
[49] AI incident database. n.d. "Incident 725: Cartels Reportedly Using AI to Expand Operations into Financial Fraud and Human Tra cking." Accessed August 31, 2025. https://incidentdatabase.ai/cite/725.
[50] Clearview AI. n.d. "Uncovering Members of an International Drug Smuggling Network." Clearview AI. Accessed August 31, 2025. https://www.clearview.ai/success-stories/uncovering-members-of-an-international-drug-smuggling-network

such as those in Michoacán,[51] where gangs equipped drones with C4 explosives and metal pellets, turning them into "flying improvised explosive devices."[52]

Several drug cartels in Mexico operate laboratories where they produce fentanyl, a synthetic drug produced in some countries as an opioid that has legitimate medical uses in anesthesia and pain management but is widely trafficked illicitly and is a major driver of overdose deaths in the United States. Under the Trump administration, the CIA deployed AI-enabled drones to surveil cartel fentanyl laboratories in Mexico, identify chemical emissions, and monitor laboratory activity in real-time. Beyond the counterintelligence aspect, it is necessary to consider the possibility that cartels may use similar AI-driven drone technology to protect their operations.[53]

4.3.4 Drug Trafficking and Logistics Enabled by Artificial Intelligence

Predictive Analytics and Machine Learning are increasingly used to analyze large datasets—such as shipping records—to optimize smuggling routes and evade law enforcement. For example, drug cartels employ these tools to identify trade patterns likely to attract regulatory or law enforcement scrutiny, such as chemical shipments from China to Mexico, and to adjust sourcing and logistics accordingly, increasing the efficiency and resilience of the synthetic drug production pipeline, including for fentanyl and methamphetamine. [54]

Artificial intelligence is also used in developing new and increasingly sophisticated smuggling methods, such as optimizing the construction of tunnel networks or coordinating drug shipments by drones across the U.S.–Mexico border.[55]

4.3.5 Challenges and Countermeasures

U.S. agencies such as the DEA and the Department of the Treasury address the use of artificial intelligence by cartels through their own AI-driven tools, including geospatial analytics, to map trafficking networks and predict cartel movements.[56] To counter the use of drones by drug cartels, authorities are examining and developing counter-drone

[51] Wikipedia, The Free Encyclopedia. n.d. "Operation Michoacán." Accessed August 31, 2025. https://en.wikipedia.org/wiki/Operation_Michoac%C3%A1n
[52] HOZINT. 2021. "Mexico | The Use of Weaponized Consumer Drones by Drug Cartels." Hozint.Com. October 26, 2021. https://www.hozint.com/2021/10/mexico-the-use-of-weaponized-consumer-drones-by-drug-cartels. Also in Gabriel Mondragón Toledo. 2023. "NarcoDrones Have Become a Growing Scare Tactic in Mexico's Drug Wars." INKSTICK. November 7, 2023. https://inkstickmedia.com/narcodrones-have-become-a-growing-scare-tactic-in-mexicos-drug-wars
[53] Jon Michael Raasch. 2025. "Trump Secretly Sends CIA Drones into Mexico to Spy on Drug Cartel Labs." Daily Mail, February 18, 2025. https://www.dailymail.co.uk/news/article-14409511/amp/trump-cia-drones-mexico-spy-drug-cartels.html
[54] 3GIMBALS. 2025. "Data-Driven Intelligence for Combating Drug Cartels." 3gimbals.Com. January 30, 2025. https://3gimbals.com/insights/data-driven-intelligence-drug-tracking.
[55] Albert Stepanyan. n.d. "Southern Border: Cartels, Wagner, and Drone Warfare." SCYLLA. Accessed August 31, 2025. https://www.scylla. ai/southern-border-cartels-wagner-and-drone-warfare.
[56] 3GIMBALS. 2025. "Data-Driven Intelligence for Combating Drug Cartels." 3gimbals.Com. January 30, 2025. https://3gimbals.com/insights/data-driven-intelligence-drug-tracking.

technologies, including AI-based countermeasures such as radio-frequency jammers and drone detection systems.[57]

Legislative gaps pose a significant obstacle for law enforcement agencies and local security forces. Mexico lags considerably in dedicated artificial intelligence legislation, leaving vulnerabilities in regulating cartel use of these technologies. Mexico's National Artificial Intelligence Alliance (ANIA) seeks to address these gaps, but progress in this area remains slow.[58]

4.3.6 Future Implications and Global Trends

Interpol notes that the CJNG cartel and other cartels are part of a global trend in which organized crime groups across Europe, Asia, and Africa are adopting artificial intelligence for fraud, human trafficking, and other crimes.[59] Others point to a socioeconomic dimension as well: while cartels use artificial intelligence to expand their operational reach, some argue that their activities generate local economic benefits, such as employment and infrastructure—albeit at the cost of violence and corruption.[60] These processes can also be assumed to apply to terrorist organizations in general, particularly in the Middle East.

4.3.7 Interim Summary

Even if U.S. and Mexican authorities somewhat exaggerate the severity of cartel use of artificial intelligence—at times to justify military responses and cross-border actions, such as designating cartels as terrorist organizations—the domain remains challenging and may also serve as a model for terrorist actors. Scholars such as Oswaldo Zavala argue that cartel power is often overstated and frequently relies on state messaging, suggesting that the use of artificial intelligence may be less autonomous and more closely intertwined with networks of corruption.[61] This interim summary reflects the complex and evolving role of artificial intelligence in cartel operations, balancing recognition of potential risks with skepticism regarding the scale of their capabilities and the motivations underlying official narratives.

[57] Gabriel Mondragón Toledo. 2023. "NarcoDrones Have Become a Growing Scare Tactic in Mexico's Drug Wars." INKSTICK. November 7, 2023. https://inkstickmedia.com/narcodrones-have-become-a-growing-scare-tactic-in-mexicos-drug-wars.
[58] Latisha Harry. 2024. "Digital Surveillance and the Specter of AI in Mexico." Advox Global Voices. February 20, 2024. https://advox. globalvoices.org/2024/02/20/digital-surveillance-and-the-specter-of-ai-in-mexico.
[59] AI incident database. n.d. "Incident 725: Cartels Reportedly Using AI to Expand Operations into Financial Fraud and Human Trafficking." Accessed August 31, 2025. https://incidentdatabase.ai/cite/725.
[60] Tommy E. Murphy, and Martín A. Rossi. 2020. "Following the Poppy Trail: Origins and Consequences of Mexican Drug Cartels." Journal of Development Economics 143 (102433). https://www.sciencedirect.com/science/article/abs/pii/S0304387819303098.
[61] Kate Linthicum. 2024. "Are Mexican Drug Cartels as Powerful as People Think?" Los Angeles Times, August 28, 2024. https://www. latimes.com/world-nation/story/2024-08-28/are-mexican-drug-cartels-as-powerful-as-people-think.

5. Terror Financing

Terrorist organizations and guerrilla groups utilize artificial intelligence in financing and fundraising efforts. While artificial intelligence does not fundamentally create new categories of threats, it amplifies existing ones by improving efficiency, scalability, and evasion tactics. The following is a general overview of reported methods, based on analyses by counterterrorism experts, international organizations, and media reporting. These uses often overlap with propaganda, recruitment, and cyber-based activities, but the focus here is on financial aspects.

5.1 Propaganda and Donor Recruitment

Groups such as the Islamic State (ISIS) use AI-based creative tools to produce personalized multimedia content, including images, audio, and videos that enhance visibility and attract supporters and donors. This indirectly facilitates fundraising by strengthening outreach on social media and encrypted channels and encouraging donations through heightened emotional appeals or calls to action.[62] Right-wing extremists use artificial intelligence similarly for graphics and disinformation, thereby expanding their supporter networks and increasing voluntary donations.

5.2 Deepfakes and Impersonation

AI-enabled deepfakes, particularly audio versions, enable impersonation fraud in which voices are cloned to deceive individuals into transferring funds or disclosing financial information. Cyber-fraud experts have identified this as a potential risk for terrorist financing, based on documented cases of voice cloning used in broader fraud schemes that could be adapted to illicit financial scams.[63] These technologies lower barriers for less sophisticated groups and facilitate large-scale fraud.

5.3 Cybercrime and Ransomware Attacks

Terrorist actors leverage artificial intelligence to plan and conduct cyberattacks, including deploying ransomware that generates revenue through extortion. Artificial intelligence facilitates the automation of data collection, analysis, and victim profiling, enabling even low-skilled operatives to target organizations and/or individuals for fraud and financial extraction.

[62] Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." The Guardian, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence. Also in UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www. un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

[63] UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www. un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

These methods include fraud operations in which artificial intelligence processes stolen data or generates fictitious identities to facilitate extortion and the movement of funds, including transfers via banks, applications, or decentralized currencies.[64] Reports highlight this as part of a broader trend in which terrorist organizations and transnational organized crime use artificial intelligence to generate revenue through digital fraud.

5.4 Decentralized Currencies

Artificial intelligence tools analyze market data and enable automated trading in decentralized currencies, providing means for speculation and anonymous revenue generation. This approach builds on the traditional use of decentralized currencies by terrorists to finance operations, with artificial intelligence potentially assisting in digital wallet theft, obfuscation of transactions, or optimization of processes for money laundering or fundraising without direct donor involvement[65] and without exposing identities.

5.5 Crowdfunding

Terrorists exploit crowdfunding platforms, even when these are not specifically AI-driven, by promoting campaigns through social media and virtual assets. Artificial intelligence amplifies these efforts by generating automated campaign content or deploying Chatbots to interact with donors, making such misuse harder to detect within large volumes of legitimate activity. Risks include fragmented payments and the anonymous cross-border transfer of funds.[66]

Counterterrorism agencies note that these AI applications intersect with challenges such as weakened oversight and rapid access to technology, which may accelerate and amplify threats. However, systematic adoption varies by group, with technologically capable organizations such as ISIS leading experimentation and the digital race. Efforts to address the phenomenon include enhanced detection systems and international cooperation on the governance and oversight of artificial intelligence.[67]

---

[64] Threat Intelligence Report: August 2025. 2025. "Detecting and Countering Misuse of AI: August 2025." ANTHROP\C. August 27, 2025. https://www.anthropic.com/news/detecting-countering-misuse-aug-2025. Also in Gabriel Weimann, Alexander T. Pack, and Et.Al. 2024. "Generating Terror: The Risks of Generative AI Exploitation." Combating Terrorism Center 17 (1). https://ctc.westpoint.edu/ generating-terror-the-risks-of-generative-ai-exploitation

[65] UNICRI and UNCCT. 2021. "Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes." https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

[65] FATF. 2023. "Crowdfunding for Terrorism Financing." FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf. Also in Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." The Guardian, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial- intelligence

[67] FATF. 2023. "Crowdfunding for Terrorism Financing." FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf. Also in Makuch, ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." The Guardian, June 8, 2025. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial- intelligence.

In summary, terrorist organizations, guerrilla groups, and insurgents use artificial intelligence to finance their activities through AI-based deception, fraud, and digital scams, including identity theft, financial theft, and credit card fraud. It cannot be ruled out that current global fraud schemes involving imitation platforms for international stock trading will intensify. Such frauds have already exacted a heavy toll on victims worldwide, and it remains unclear who precisely is behind them or what their origins are. It is possible that they are linked to global organized crime, drug cartels, insurgent groups, and transnational terrorist organizations.[68]

6. Conclusion

Terrorist and guerrilla organizations are often able to gain access to military research and development outputs. With the end of the Cold War, the global arms market, particularly the technological segment, became largely unregulated. Vast quantities of weapons, primarily from Warsaw Pact stockpiles and post-Soviet regions, flooded the black market. Arms dealers traded with virtually any buyer, including criminal organizations, insurgent groups, terrorist organizations, guerrilla movements, and drug cartels. Additionally, the collapse of regimes worldwide—especially in the Middle East following the dissolution of the Soviet Union and the Arab Spring—led to the widespread proliferation of weapons and their transfer into the hands of terrorist and guerrilla organizations across the region.

Hamas and Palestinian Islamic Jihad received large quantities of weapons originating from Iran, North Korea, and other countries, enabling them to expand their military capabilities and evolve into heavily armed guerrilla organizations. Alongside weapon systems, terrorist organizations also obtained military R&D outputs developed by major powers such as Russia, China, India, and North Korea, as regimes that later collapsed had maintained long-standing military cooperation with these states during the Cold War. As a result, military research and development outputs of sovereign states ultimately reached terrorist and guerrilla organizations.

These capabilities encompass a wide range of weapons systems, including rockets, advanced anti-tank missiles, automatic firearms, sophisticated explosives, and anti-personnel and anti-armor mines and charges, as well as drones and unmanned aerial vehicles. At the same time, there is a need to assess how far the pursuit of non-conventional—or "dirty"—weapons has progressed, including biological and chemical agents.

[68] Task Force to Investigate Terrorism Financing. 2016. "Trading with the Enemy: Trade-Based Money Laundering Is the Growth Industry in Terror Finance." https://www.govinfo.gov/content/pkg/CHRG-114hhrg23565/html/CHRG-114hhrg23565.htm. Also in Harry Freeborough. 2024. "Online Investment Scams: Inside a Fake Trading Platform." March 13, 2024. https://www.netcraft.com/blog/inside- a-fake-trading-platform.

Some state-origin military R&D products reach terrorist and guerrilla organizations in ready-to-use form, while others are obtained through reverse engineering carried out by specialists and engineers working on their behalf.[69] Since the collapse of the Soviet bloc, a pattern has emerged in which former military R&D experts from socialist-bloc states have been recruited or employed by terrorist and criminal networks. The development of combat robotics by multiple states suggests that similar pathways of diffusion may emerge in the future, allowing such technologies to migrate to asymmetric and non-state actors as well.

In the cyber domain, military research and development based on cyber capabilities began to emerge only in the early 2000s and has, to date, diffused to terrorist organizations to a more limited extent. Nonetheless, these organizations have independently acquired—and continue to enhance—cyber capabilities. This has been achieved by recruiting specialists who are motivated either by substantial financial compensation[70] and/or ideological commitment, and by accessing the open market for artificial intelligence tools, developing custom-made applications and malware 'in-house', executing cyberattacks, and utilizing contracted hacker groups.

Terrorist organizations use cyber and artificial intelligence capabilities to instill fear and confusion among local populations and to undermine state authorities by disrupting critical infrastructure, communication networks, media systems, and propaganda channels, as well as disseminating disinformation. They also use these capabilities to recruit supporters and fighters, raise funds to finance operations—including extensive reliance on decentralized currencies—and obtain strategic and tactical intelligence from open sources, including for planning and executing attacks.

Artificial intelligence is becoming an integral component of the operational ecosystem of asymmetric actors. Its use is wide-ranging and spans all core elements of asymmetric warfare. These organizations deploy AI-generated content primarily for recruitment, propaganda, and financing, as well as for instilling fear and undermining governance. In doing so, they indirectly achieve a significant strategic effect: generating international pressure on governments with which they are in conflict. For example, pressure on the Israeli government by the world community is amplified through the mobilization of pressure on global political leaders.

[69] Cordesman, A H. 2016. "The Road to Hell in Iraq and Syria." CSIS Center for Strategic and International Studies, no. October 6, 2016. https://www.csis.org/analysis/road-hell-iraq-and-syria?block1.
[70] US. Department of State. 2019. "Country Reports on Terrorism 2019." https://www.state.gov/reports/country-reports-on-terrorism-2019.

In addition, artificial intelligence enables extensive process automation, significantly reducing the time and resources required for asymmetric warfare activities. It facilitates encrypted coordination among terrorist cells, organizations, and networks worldwide; advanced analytical and predictive capabilities—including forecasting counter-responses by government security forces; machine learning; the production of deepfakes; psychological warfare; deception; and financial fraud. These systemic challenges underscore the need for a comprehensive and integrated approach to countering organized terrorism and conducting effective counter-warfare.

October 2025

The Jerusalem Institute for Strategy and Security
16 Abba Eban St, Jerusalem
www.jiss.org.il
info@jiss.org.il

Conlonel (Res.), Prof. Gabi Siboni is CEO of the Jerusalem Institute for Strategy and Security. He was director of the military and strategic affairs program, and the cyber research program, of the Institute for National Security Studies (INSS) from 2006-2020, where he founded academic journals on these matters. He serves as a senior consultant to the IDF and other Israeli security organizations and the security industry. He holds a B.Sc. and M.Sc. in engineering from Tel Aviv University and a Ph.D. in Geographic Information Systems (GIS) from Ben-Gurion University.

Dr. Simon Tsipis holds a Ph.D. in Political Science and International Relations from the University of Bonn and an M.A. in Political Science and National Security from Tel Aviv University. His areas of expertise include terrorism, cybersecurity, post-Soviet politics, and European and Eurasian affairs.

www.jiss.org.il