Automated Recruitment: Artificial Intelligence, ISKP, and Extremist Radicalisation

GNET > Insights > Automated Recruitment: Artificial Intelligence, ISKP, and Extremist Radicalisation

By Fabrizio Minniti
11th April 2025
In Insights

Introduction

The role of artificial intelligence in terrorist recruitment has grown exponentially, which has had a significant impact on the way extremist groups interact with vulnerable individuals online. Recent advances in generative artificial intelligence, deepfake technology and autonomous chatbots have made it much easier for terrorist organisations to amplify their propaganda, personalise radicalisation efforts and circumvent counter-terrorism monitoring. These developments present a direct challenge to digital platforms, intelligence, and policymakers, as AI enables extremist content to spread with greater speed, sophistication and resilience against traditional countermeasures.

This Insight examines the current landscape of AI-enhanced terrorist recruitment, focusing on the ways groups like Islamic State Khorasan Province (ISKP) have integrated AI into their radicalisation strategies. The piece explores the latest AI-driven threats, analysing how extremist groups exploit technology to automate recruitment and improve their ideological dissemination. It also suggests counter-terrorism responses, highlighting AI-based detection mechanisms, algorithmic counter-narratives and proactive monitoring efforts. By providing a comprehensive overview of these trends, this Insight aims to offer practical solutions for policymakers, security operators and technology companies seeking to prevent the terrorist exploitation of AI-based tools.

The Current Landscape of AI in Terrorist Recruitment

AI has enhanced how terrorists exploit social media. AI models can analyse how users interact with content, allowing extremists to adapt and target potential recruits. Using data-driven insights from social media behaviour to customise propaganda in real time makes AI-assisted radicalisation significantly more effective than traditional methods. IS is doing exactly this, having published a guide on "how to securely use generative AI" in 2023.

Unlike human recruiters, AI-based chatbots can operate continuously across multiple platforms, engaging in conversations that mimic human interactions. Designed to tailor radicalisation pathways, AI chatbots analyse behavioural triggers and adapt their responses

based on an individual's ideological inclinations and vulnerabilities. The danger of passive recruitment with the malign use of AI is extreme.

Case Study: ISKP and AI-Driven Recruitment

The transnational jihadist group known as ISKP, which was formed in 2015 in Afghanistan and Pakistan, has developed a sophisticated understanding of modern cyber warfare and digital influence. The group has actively used AI to expand its recruitment base, circumvent security monitoring, and maintain ideological cohesion despite territorial losses. Following the Taliban's return to power in Afghanistan in 2021, ISKP has increasingly relied on AI-based radicalisation tools to differentiate itself from other extremist organisations. AI now plays a crucial role in ISKP's media strategy, propaganda campaigns and recruitment processes, enabling the group to remain highly active despite intensified counter-terrorism efforts.

ISKP is using AI to amplify and tailor its propaganda and to improve on traditional radicalisation methods, particularly for recruitment and psychological warfare.

Timeline of AI Propaganda Adoption Following Attacks

Date	Event	Description
2023	ISKP AI Training	ISKP explored online AI training courses for its propagandists (Munasireen)
22 March 2024	Crocus City Hall Attack (Moscow)	Following the attack claimed by IS, an IS supporter circulated AI-generated video news bulletins about the Moscow attack
17 May 2024	Bamiyan Attack	ISKP launched an AI-generated propaganda bulletin featuring a local-looking anchor to claim responsibility
21 May 2024	Kandahar Bombing	Second AI video appeared announcing the Kandahar bombing claim via "Khurasan Television" with a Western-dressed anchor

Figure 1: An April 2024 AI-generated news bulletin following the group's attack on Crocus City Hall in Moscow presented the event as a significant victory. Source linked.

ISKP's propaganda strategy is characterised by a keen understanding of the regional landscape, meticulously tailored to exploit existing socio-political tensions and ongoing conflicts. This involves a conscious effort to tap into local grievances and frame its narrative in a way that resonates with specific populations. A critical component of this approach is the extensive use of local languages, including Pashto, Tajik, and Uzbek, enabling ISKP to directly communicate with and influence diverse target audiences within the region. This multilingual capability underscores a sophisticated understanding of its target demographics and a deliberate effort to connect with various ethnic and national groups by addressing their unique concerns and cultural contexts.

After the Kabul Airport bombing in August 2021, ISKP intensified its propaganda activities, strategically targeting disillusioned Taliban members affected by internal divisions and contentious diplomatic negotiations. The group's narratives portrayed the peace agreements with the Taliban as a betrayal of Sunni Muslims globally, with the aim of exploiting the rifts within the Taliban and recruiting defectors disillusioned with the perceived ideological compromises.

Similarly, after the deadly attack on a Shia mosque in Kunduz in October 2021, ISKP leveraged existing sectarian tensions through carefully crafted propaganda. The group positioned itself as a defender of Sunni interests, framing acts of violence against Shia communities as justified religious retaliation, thus exploiting deep sectarian divisions to attract further support.

The ISKP's propaganda is centrally managed by its media wing, the Al-Azaim Foundation, which demonstrates a significant awareness of regional sensitivities through multilingual content suitable for different audiences. The ISKP actively promotes 'media jihad', encouraging supporters to spread propaganda, often using the graphic content of attacks to project strength and legitimacy.

This foundation is responsible for producing and disseminating a wide range of multilingual content, including magazines, videos, and online bulletins, targeting diverse audiences both within and outside Afghanistan. The prominent role of the Al-Azaim Foundation and its collaborative efforts underscore ISKP's organisational commitment to maintaining a centralised and extensive propaganda network, maximising its ability to disseminate its ideology and influence potential recruits.

ISKP's adoption of AI in its propaganda efforts is not an isolated incident but part of a growing trend within the broader Islamic State network. It signifies a dangerously proactive approach to harnessing emerging technologies for its strategic objectives.

AI-Generated News Bulletin: Attack on Crocus City Hall

In the aftermath of the Moscow attack, ISKP disseminated an AI-generated news bulletin, heralding a notable paradigm shift in the manner by which extremist groups are leveraging AI to shape narratives. This development stands in stark contrast to the conventional terrorist propaganda videos, which frequently rely on footage of substandard quality and amateur recordings.

Al-Qaeda's early video propaganda (of the late 1990s and early 2000s) reflected the technological limitations of the time, prioritising the message over the higher production values seen in later groups like the Islamic State. The AI-generated news programme, in contrast, boasted a high level of sophistication in its visual appeal, closely resembling conventional media broadcasts. The news programme featured an AI-generated news anchor designed to resemble a real journalist.

Figure 2: The image contains text in Pashto and English, specifically showing "کې داعش ډلې په وسله وال" in Pashto, which translates to "ISIS group in armed" and the English text "Khurasan TV" repeated twice, indicating a news outlet associated with ISKP.

This AI-generated avatar, facilitated by sophisticated deepfake technology, delivered written propaganda messages in a neutral and professional tone, thereby rendering the content authentic and credible. The AI-generated anchor read propaganda statements that reinforced ISKP's ideological objectives, describing the attack as symbolic of the weakening of Russia's security infrastructure.

The bulletin also incorporated deepfake-enhanced images, which manipulated footage of the attack to exaggerate the level of destruction and chaos. The AI altered the original footage to create the illusion of a much larger explosion and a higher death toll than was actually reported, furthering the group's propaganda goals. The bulletin also incorporated fabricated speeches from Russian political figures, falsely suggesting that the Russian government was on the verge of collapse. The incorporation of synthetic voices and deepfake-enhanced images ensured that ISKP's message reached a wide and highly engaged audience.

A notable shift occurred after the Bamiyan attack on 17 May 2024, when ISKP released an AI-generated propaganda bulletin, a 52-second Pashto-language video featuring an AI anchor resembling local residents, disseminated via official channels, including Al-Azaim Media. Khurasan Television followed this with another AI-driven segment on 21 May 2024, featuring an AI anchor in Western attire to claim responsibility for the Kandahar bombing.

In addition to AI-generated news content, ISKP has explored other innovative propaganda methods, including animated content targeting children and online AI training courses for its media activists, initiated as early as 2023.

ISKP's sophisticated propaganda efforts, centrally coordinated through the Al-Azaim Foundation, leverage multilingual media to engage diverse audiences effectively. Its strategic integration of on-ground actions with advanced digital technologies—including the pioneering use of AI-generated propaganda—highlights ISKP's adaptability and underscores the persistent threat the group poses to regional and global security.

The evolution of ISKP's recruitment strategy reveals a disturbing sophistication. This may result in the seamless translation of their propaganda, not just into static text, but into dynamic videos, tailored to resonate with diverse linguistic communities. It is a strategic deployment of AI, breaking down language barriers and extending its reach into the very heart of potential recruitment pools: Russian-speaking enclaves, the Pashto-speaking regions, and even the digital spaces frequented by European sympathisers.

ISKP's multilingual outreach is merely a precursor to its deeper strategy: exploiting social media algorithms to amplify extremist propaganda. AI enhances this process by refining audience segmentation, ensuring extremist materials are not just accessible but precisely targeted. This algorithmic precision fosters a self-reinforcing cycle of exposure and ideological entrenchment, accelerating radicalisation.

ISKP strategically employs keywords, hashtags, and engagement mechanisms to optimize content visibility. AI further refines this approach by profiling users based on digital behaviour, tailoring narratives and optimising content delivery. This AI-driven targeting amplifies the risk of online radicalization, underscoring the need for advanced countermeasures in digital counterterrorism.

Conclusion

Countering ISKP's AI-driven propaganda necessitates a strategic, multifaceted approach that transcends technological innovation. In partnership with governments and researchers, the tech industry must lead efforts to develop AI-driven detection systems, content authentication technologies, and multimodal analysis tools to disrupt extremist narratives. However, practical challenges must be acknowledged, including ISKP's adversarial tactics, AI's difficulty in interpreting nuanced content, and the risk of false positives.

Implementing AI-based countermeasures effectively requires balancing privacy protections with security measures. Expanding surveillance without adequate safeguards raises ethical concerns, while AI-generated counter-narratives risk losing credibility among vulnerable individuals if not carefully crafted. Additionally, resource constraints, fragmented industry responses, and legal barriers hinder seamless coordination and information-sharing, complicating efforts to create a unified defense.

To address these challenges practically, technology companies should prioritise the development of scalable and responsible AI solutions that transparently and actively mitigate unintended biases. This can be achieved by implementing regular audits of AI algorithms, ensuring diverse and representative data sets, and fostering open dialogue with civil society organizations to address ethical concerns. Furthermore, governments and international bodies can facilitate cross-sector collaboration by establishing clear legal frameworks that balance privacy rights with the need for effective counter-propaganda measures. To effectively counter ISKP's AI-driven propaganda, policymakers and tech companies must collaborate on proactive countermeasures that limit extremist reach while protecting fundamental digital rights. This requires a sustained, multifaceted effort that combines technological ability with a deep understanding of the socio-political contexts that fuel radicalisation.