EXECUTIVE SUMMARY

"God has helped us, and so will AI": How the Terrorist Group Boko Haram Uses Frontier AI

Antonia Juelich
Cambridge Programme on AI Science & Policy, University of Cambridge

In 2025 and 2026, I conducted 57 in-person interviews with 27 former members of Boko Haram in northeast Nigeria, including mid-ranking commanders and technical specialists, to ask whether and how the group uses AI. Based on their accounts, this study presents the first on-the-ground evidence of AI use by an active terrorist organization. The findings establish that the group uses leading AI systems to plan attacks, design explosive devices, service and troubleshoot weapons, and improve operational security, and that this know-how is spreading through transnational jihadist networks, with Islamic State operatives delivering in-person AI training and remote support. These interviews describe activity from 2023 through 2024, with the most recent accounts extending into mid-2025. Terrorist use of AI is likely even more widespread now. It is thus a present and growing reality, and has advanced more systematically and across a wider range of activities than prior analysis has recognized.

AI is used to assist in combat and day-to-day operations, and adoption of AI by terrorist groups has been significantly underestimated. Previous assessments relying on online content concluded that use of AI by jihadist supporters has been slow and focused mainly on propaganda. In contrast, this study finds that both factions of Boko Haram — the Islamic State West Africa Province (ISWAP) and Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād (JAS) — have used multiple leading AI systems, including ChatGPT, Claude, Gemini, Grok, Meta AI, and DeepSeek, for every stage of military activity, from mission preparation through execution to post-mission review. Former members describe AI as a go-to problem-solver, with one former ISWAP commander saying: "You type in the question or use your voice and it [AI] gives you a detailed answer, like 'How can I build a bomb?' and then it

tells you how. It is like a human robot! We used it a lot." Reported use cases include weapons troubleshooting and design of explosive devices, tactical and strategic planning, operational security, and logistics. For example, when defensive trenches became an obstacle to ISWAP's assaults, commanders used AI to work out how to jump the trenches by motorcycle, allowing them to breach fortified bases. Terrorist adoption of AI has thus been significantly underestimated in both scope and character.

AI training has been delivered through transnational jihadist networks. Neither faction arrived at AI use independently. Islamic State operatives delivered in-person training and online assistance to ISWAP across multiple locations: "The white guys came and taught us," one former commander recalled. "They assembled the top people in a room and used a projector to show how it works on a big screen." They supplied laptops with VPNs and encryption software, set up accounts and managed paid subscriptions, and advised daily on prompting techniques and bypassing platform restrictions. Respondents consistently identified the Islamic State as "the real source" behind these efforts. Because ISIS disseminates technical capabilities across its provinces and runs them as an integrated global network, similar training has likely reached other affiliates. JAS received parallel training through separate networks, indicating diffusion beyond any single group.

Boko Haram has set up dedicated AI teams. Both ISWAP and JAS have established multiple AI units staffed by personnel drawn from senior operational and technical roles, such as bomb-makers, gun specialists, and engineers, who "don't go to war. Their role is to disseminate information." These units query the models to generate guidance that feeds into daily operations, manage accounts across multiple providers, and conduct internal training that cascades knowledge down the command hierarchy. Because the groups worry about privacy and internal security, access is governed by rank-based policies that concentrate use among trusted, trained personnel. "We are not allowed to access the computers. [...] They are the masters. They do the analysis with the AI and give us the strategies to implement," said a respondent about the AI units that sit "directly under the leadership." That a resource-constrained group assigns senior technical talent to this, rather than to combat, further signals how much it values AI.

AI has led to perceived capability improvements. "The steps it gave us to solve problems were so helpful," explained a participant. According to former members,

they learned to conduct better-coordinated attacks using smaller units and to build more powerful bombs, reducing casualties within their own ranks. “Trial and error can kill you. AI gives you accuracy.” Some reported that AI advised on payload weight and release-mechanism design that assisted ISWAP’s weaponization of drones. These perceptions and revealed preferences indicate uplift, though it is important to note that it cannot be conclusively determined. But the perception itself matters, since the belief that AI improves performance drives institutional investment and potentially the pursuit of higher-risk capabilities.

Adoption has spread, and safeguards did not prevent misuse. Within roughly two years of ChatGPT’s release, both factions progressed from initial exposure to dedicated units and integration into operational routines, and use has likely expanded further since the period studied. Some of what the group asked of AI is dual-use or general knowledge, such as vehicle repair or logistics advice. This still confers operational benefits, but obtaining it is no safeguard failure. Other requests, such as explosives design and attack planning, are what safeguards should block. Here the groups described restrictions as manageable rather than prohibitive. As one commander put it, “boys that have received extensive training [...] bypass the restrictions. They say they need it for a movie or something like that.” They used jailbreaking techniques taught by foreign operatives, and because they keep accounts across multiple providers, a single refusal or suspension rarely mattered. Whether more recent safeguard updates present greater obstacles is not known, but throughout 2024, restrictions did not appear to prevent misuse.

Expressed enthusiasm for AI, combined with openness to mass-casualty weapons, warrants attention as models advance. Interviewees voiced strong enthusiasm for AI, as captured in the statement “God has helped us, and so will AI.” Moreover, some did not categorically reject weapons of mass destruction, specifically chemical and biological weapons, and a few accounts pointed to rudimentary experimentation with chemical agents. Neither faction shows chemical, biological, radiological, or nuclear (CBRN) capability, and their documented AI use remains conventional. But an actor eager to adopt AI, and willing to contemplate mass-casualty weapons, is precisely the kind for whom safeguards matter, even more so as models grow more capable.

Significant uncertainties remain. First, the study relies on self-reported accounts that may be subject to over- or underreporting. I triangulated across respondents and

cross-referenced with secondary sources wherever possible, though this was not always achievable given the sensitivity of the topic and the difficulty of accessing this population. Second, the findings document AI adoption and institutionalization, and members described AI as improving operational efficiency, but they do not conclusively establish whether AI provided uplift, or whether it enabled attacks that would otherwise not have been possible. Third, participants were former and not active members, and most were mid-ranking rather than top leadership, so the most recent developments, the highest-level decisions about AI, and the most sensitive applications may not be captured. Fourth, as a case study, the findings cannot be directly generalized to other organizations, though their implications do not depend on generalization.

The vulnerabilities are structural and not actor-specific. Boko Haram is not exceptional in its resources or sophistication, and although a transnational network accelerated and systematized its AI use, such a network is not a precondition. The tools are publicly available, and the barriers to reaching the uses documented here are low enough that a motivated group could plausibly arrive at them independently. A single well-documented case is therefore sufficient for treating this as a present security problem. It requires AI developers to assess whether current safety architectures are adequate against organized adversaries rather than isolated users; policymakers to treat terrorist adoption of AI as a current national security concern; and the intelligence community and law enforcement to monitor and disrupt the evolving threat. It also requires them to work together, developing shared methods, information-sharing channels, and joint responses. This study raises the question of whether those efforts currently exist at the scale the problem warrants.