UNIVERSITY OF CAMBRIDGE | CASP Cambridge Programme on AI Science & Policy

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

Antonia Juelich

July 2026

Frontier AI Working Paper Series No. 1/2026
Cambridge Programme on AI Science & Policy
University of Cambridge

CONTENTS

ABSTRACT

How are terrorist groups using AI? Semi-structured interviews with 27 former Boko Haram members conducted in northeast Nigeria in 2025 and 2026 reveal unprecedented detail about AI-assisted terrorist activity primarily through 2024. This report finds that both factions of Boko Haram use frontier AI, including ChatGPT, Claude, Gemini, Grok, Meta AI, and DeepSeek, to assist in combat and day-to-day operations. This AI use is institutionalized through specialized units and internal training. It has aided in attack planning, weapons troubleshooting, and the design of explosive devices, as users have successfully circumvented some safeguards. This know-how was transferred through transnational jihadist networks, with Islamic State operatives delivering in-person training. Respondents expressed strong enthusiasm for AI and, in some cases, openness to mass-casualty weapons, though documented use remains conventional. Terrorist adoption of AI has thus advanced further and more systematically than prior analysis has recognized, making it a present and growing reality that warrants attention from policymakers, security communities, and AI developers.

EXECUTIVE SUMMARY

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.

INTRODUCTION

In a hotel room in northeast Nigeria, I sat across from a man who had spent years fighting for one of the world's deadliest jihadist insurgencies. I opened my laptop, typed in the web address of a leading AI company's chatbot, and turned the screen around to face him. "Was this one of the systems you used?" He nodded. "What did you do with it?" I asked. "You type in the question, or use your voice, and it gives you a detailed answer, like 'How can I build a bomb?', and then it tells you how," explained a former Boko Haram commander.[1] "It is like a human robot. We used it a lot," he added. In 2025 and 2026, I interviewed 27 former members of Boko Haram in northeast Nigeria about whether and how the group uses AI. Over many hours, they described who had introduced them to AI, what they used it for, how they circumvented its safeguards, and why they benefitted from it.

Research on AI misuse risk has centered on testing what models can do, but we have limited knowledge on what threat actors are actually doing. Benchmark testing demonstrates how fast model capabilities are advancing across domains (Epoch AI 2026; UK AI Security Institute 2025). Researchers stress-test models to map how those capabilities could be weaponized and whether safeguards prevent such misuse (Mouton et al. 2024; Weimann et al. 2024; Hong et al. 2026), while risk assessments and expert forecasts estimate the severity and likelihood of AI-enabled attacks (Halstead and Righetti 2025; van der Merwe 2025; Righetti 2025; Williams et al. 2025). To counter misuse, developers deploy layered mitigations, from safety training and content filtering to usage monitoring and account-level enforcement. Even so, some AI developers acknowledge that their latest models are capable enough to be misused

[1] Interview with ISWAP Commander-7, 2025.

for the development or acquisition of chemical, biological, radiological, and nuclear (CBRN) weapons (Anthropic 2025a; OpenAI 2025), and that in light of unprecedented cyber capabilities, the misuse risk is too high to publicly release them (Anthropic 2026).

There is emerging evidence of misuse by different actors. AI labs have reported that their systems are employed for cybercrime, fraud operations, and cyber espionage by government-backed actors and cybercriminals (Anthropic 2025c, 2025b; Google Threat Intelligence Group 2025a, 2025b). There are also documented cases of individuals consulting Large Language Models (LLMs) to plan violent attacks, including the Cybertruck bombing in Las Vegas (Catalini 2025), the Palm Springs fertility clinic attack (Palmer 2025; United States District Court for the Central District of California 2025), and mass school shootings (BBC News 2026; G. Wells 2026a). In one recent case, a medical consultant arrested in India over an alleged Islamic State plot had reportedly consulted ChatGPT and AI-powered search while attempting to produce the lethal toxin ricin (Jha 2025). Jihadist supporters have also used AI to generate online propaganda (Stalinsky 2025; Humphrys 2024; Tech Against Terrorism 2023). However, whether terrorist organizations, which tend to possess the resources and networks to carry out more lethal attacks than lone actors (Alakoc 2017; Phillips 2017), are adopting AI remains largely unknown.[2]

To address this gap, I conducted a total of 57 semi-structured interviews with 27 former Boko Haram members. Drawing on the cases of the Islamic State West Africa

[2] A literature review concluded that the existing scholarship "relies primarily on speculative and theoretical arguments" and identified the absence of empirical research on terrorists' actual AI use as its most significant weakness (Houser and Dong 2025, 7, 17). The Generative AI Terrorism Risk Assessment Act, which passed the House in 2025 and would require the Department of Homeland Security to conduct annual assessments of incidents in which foreign terrorist organizations have used or attempted to use generative AI (U.S. House of Representatives 2025), is itself a recognition that the evidence base for such assessments does not yet exist.

Province (ISWAP) and Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād (JAS), jointly known as Boko Haram, this study provides the first on-the-ground investigation of AI use by active terrorist organizations. The interviews were carried out over several weeks in 2025 and 2026, covering AI adoption pathways, current use cases, and perceptions of AI's potential and constraints, alongside questions about other technologies and operational procedures to contextualize AI within broader patterns of technology adoption.

Based on these interviews, the study finds that AI use by both factions extends well beyond propaganda into the operational core of insurgent warfare. Both factions have employed frontier AI as a problem-solving tool across the full spectrum of terrorist activities, including to plan attacks, design explosive devices, service and troubleshoot weapons, and improve operational security. Members were trained in AI by Islamic State operatives, built dedicated AI units, and embedded the technology in their organizational routines. This adoption and institutionalization happened within roughly two years of ChatGPT's release, inside resource-constrained groups under military pressure, and existing safeguards did not prevent it. Taken together, the findings suggest that terrorist use of AI has been faster, more advanced, and more systematic than prior analysis has recognized — and that the conditions enabling it are not unique to this case.

Respondents described engagement with AI as having begun in 2023 and, because they had left the group at different points, most in 2024 and one in mid-2025, their accounts cover that period rather than the time of the interviews. This research method offers unique access to internal organizational processes but relies on self-reported accounts that may over- or understate, or be incomplete. To mitigate this, rapport was built over multiple meetings to encourage candid engagement, and accounts were triangulated across respondents and cross-referenced with secondary

sources wherever possible. Because the sensitivity of the topic and the difficulty of accessing this population meant the accuracy of individual accounts could not always be independently verified, throughout this study I state broadly corroborated patterns as fact and attribute narrower claims explicitly to interviewees. At the same time, the data's value lies in its access to members' own perceptions and representations of their groups' engagement with AI, which even chat logs and platform-level data cannot capture and which questions of veracity do not diminish.

How severe the risk actually is remains unclear, and the use cases documented here are not existential threats. But that a group such as Boko Haram has recognized the value of AI, built institutional capacity around it, and found safeguards manageable suggests that the barriers to AI adoption are lower than is often presumed, and that adoption is unlikely to be the primary constraint on terrorist use of AI. If current and future models provide meaningful capability uplift, and safeguards can be overcome, at least some militant groups are likely to be willing and already positioned to exploit them. The specific policy implications are beyond the scope of this paper, which instead provides empirical evidence of terrorist adoption of AI and aims to prompt governments, intelligence communities, and AI developers to assess what actions are warranted.

This study proceeds as follows. The next section describes the risk of AI misuse by terrorist organizations, reviewing uplift mechanisms and potential domains of misuse. The section that follows synthesizes the current evidence and gaps in understanding terrorist AI adoption, situating the contributions made by this research. The methodology section details the research design and methods that enabled access to this sensitive data and hard-to-reach population, followed by some brief background information on the case of Boko Haram. The empirical sections then examine AI adoption, the organization of AI access and expertise within

institutional structures, AI use cases, attitudes toward weapons of mass destruction (WMD), and uplift and optimism regarding future use of AI, before concluding with final observations and implications.

THE RISK OF AI MISUSE BY TERRORIST GROUPS

AI could alter the threat landscape by uplifting threat actors' capabilities. Uplift is "an improvement in capabilities or outcomes that can be achieved with a given level of resources" (Rose et al. 2024, 12). If terrorist operations require fewer people, less expertise, less time, and/or less funding, the effects could include:

- An expanded actor pool: due to lowered barriers to entry, a greater number of actors have the capability to conduct terrorist operations.
- Increased speed and frequency of attacks: terrorist operations can be planned and executed at higher frequency and on faster timelines.
- Increased scale, complexity, and sophistication: terrorist operations can be conducted at greater scale, with more complex multi-domain coordination, and using more technically advanced methods than previously possible.
- Improved precision: terrorist operations can more accurately achieve intended strategic objectives, such as through improved target selection, method optimization, and timing. This could enable actors to develop end-to-end attack plans that advance their goals more effectively.
- Improved operational security: threat actors can better evade detection, reduce vulnerability to counterterrorism measures, and maintain operational continuity.

Beyond resource efficiency, uplift may additionally:

- Raise the ceiling of harm: AI may enable fundamentally new capabilities and attack vectors that reach levels of impact that would be impossible without AI, such as personalized algorithmic radicalization at scale (Janjeva et al.

2024), novel biological agents beyond natural or current scientific capability (AIxBio Global Forum 2025), cyberattacks based on autonomous discovery and exploitation of software vulnerabilities (Anthropic 2026), or attacks exploiting vulnerabilities in AI systems themselves (Brundage et al. 2018).

In other words, the risk is that AI serves as a force multiplier, lowering barriers to entry for potential attackers, enhancing the capabilities of threat actors, and enabling novel attack vectors that were not previously possible, thereby expanding existing threats or introducing new ones. While AI's uplift effects are relevant across the full spectrum of threat actors, the extent and nature of benefits depend on an actor's existing expertise and resources, which can vary considerably among organized groups, small cells, and lone actors. In that regard, it also matters that uplift can be nonlinear. Terrorist capability often hinges on crossing specific performance thresholds, and AI may supply just enough assistance to push actors past a boundary that previously constrained them. Even individually modest gains can then produce qualitative shifts in what an actor can achieve, and because actors begin from different levels, the same assistance can be decisive for one and marginal for another.

LLMs could assist terrorist groups across the full spectrum of activities, from recruitment and coordination to attack execution (UNOCT and UNICRI 2021; Weimann 2025; Weimann et al. 2024; Ackerman 2023; Lakomy 2023; Brundage et al. 2018; Janjeva et al. 2024; Pfaff et al. 2025). This entails both technical and operational support in key areas, including:

- Propaganda, radicalization & recruitment
- Organizational management & coordination
- Training & skill development
- Financial operations
- Logistics & procurement

- Intelligence & reconnaissance
- Operational security
- Cyber capabilities
- Weapons & physical attack capabilities

These categories complement and reinforce each other. For example, the use of AI may simultaneously enable recruitment networks to find operatives with aviation knowledge, accelerate intelligence gathering on airport security protocols, streamline procurement of drone components, and secure communication among actors who are involved. These parallel improvements across the "end-to-end 'AI attack chain'" (Janjeva et al. 2024, 26) enable complex operations, such as coordinated multi-site drone attacks, that would be impossible with any single enhancement alone. Moreover, the level of risk is not intrinsic to specific categories. Applications that appear low-risk in isolation (e.g., management, logistics, operational security) may serve as crucial enablers for high-impact operations.

Whether any of these potential effects materialize, however, is unclear. Evidence on uplift is domain-specific, mixed, and constantly evolving alongside AI capabilities, safeguards, and user proficiency. In the biological domain, the early evidence was reassuring but is increasingly contested. For example, multiple randomized controlled trials found no statistically significant uplift in biological threat capabilities. Teams developing attack plans showed similar viability regardless of whether they had LLM access or internet-only use (Mouton et al. 2024), participants completing threat creation tasks demonstrated only small, non-significant improvements with GPT-4 (OpenAI 2024), and a further study found that models gave novices only modest help with complex laboratory procedures (Hong et al. 2026). However, model capability has risen sharply as measured by the Virology Capabilities Test, showing that the strongest model outperformed 94 percent of

expert virologists even within their own specializations (Götting et al. 2025). On top of that, safeguards remain uneven, with refusal rates for high-risk biological prompts varying widely across deployed models (Marshall, et al. 2026). Even the most robust defenses can be broken by automated jailbreaking on biological-misuse questions, although still only with substantial expertise and resources (Davies et al. 2026).

Recent reporting shows that AI-enabled bioterrorism is a serious threat, as chatbots have been shown to be able to help design, assemble, and disperse biological agents (*The Economist* 2026a; *The Economist* 2026b; Dance 2026), while Anthropic co-founder and CEO Dario Amodei anticipates a significant near-term jump in biological capability that would heighten it further (Thornhill 2026). Regarding other domains, quantitative risk modeling has already pointed to systematic uplift in cyber attack efficacy and speed (Barrett et al. 2025). Since then, frontier models have been withheld from public release over their cyber capabilities (Anthropic 2026; OpenAI 2026). When it comes to extremist propaganda, an expert assessment found that LLMs can generate credible extremist prose (Baele et al. 2025), while an older red-teaming study found an overall 50 percent success rate across five platforms when prompting for a range of harmful outputs, including dis-/misinformation, polarizing content, and recruitment support, both with and without jailbreaks (Weimann et al. 2024). Ultimately, whether capabilities demonstrated in controlled settings with ordinary people translate to genuine advantages for adversaries operating in real-world conditions depends on whether AI capabilities are actually adopted by terrorist groups, whether they are in fact helpful, and whether defensive measures adapt quickly enough to counteract relevant gains.

EVIDENCE & GAPS IN UNDERSTANDING TERRORIST AI ADOPTION

AI misuse by malicious actors has already been documented. Since late 2024, multiple violent attacks have involved perpetrators consulting LLMs. The perpetrators of the Las Vegas Cybertruck bombing used ChatGPT to calculate explosive quantities and research procurement methods, described by authorities as the first confirmed case of ChatGPT assisting bomb construction on U.S. soil (Catalini 2025). The perpetrator of the New Orleans Bourbon Street attack, which killed 14 people and injured 57, used Meta's AI-enabled smart glasses in the planning process to conduct reconnaissance (A. Bacon 2025; Sarnoff 2025). Other cases include the Palm Springs bombing in May 2025, in which the attacker sought information about "explosives, diesel, gasoline mixtures and detonation velocity" (Palmer 2025); a planned attack in Vienna where an Islamic State supporter used chatbots to inquire about bombmaking and joining ISIS affiliates in West Africa (Vienna Online 2025); a school stabbing in Finland where the perpetrator used AI to draft his manifesto and structure attack logistics (Gustavsson and Asp 2025; Solea 2025); and a mass shooting in Canada where the shooter's ChatGPT conversations had flagged OpenAI's monitoring systems months before the attack (G. Wells 2026b). The AI Incident Database (2026) has recorded 283 cases of "malicious actors and misuse," representing 28.6 percent of all reported incidents.[3] Among those are also cases that AI companies have documented. Their threat intelligence reports focus primarily on LLMs being employed for cybercrime, fraud, and cyber espionage by

[3] The "malicious actors and misuse" category consists of three subcategories: "Fraud, scams, and targeted manipulation" (193 incidents), "Disinformation, surveillance, and influence at scale" (84 incidents), and "Cyberattacks, weapon development or use, and mass harm" (six incidents).

government-backed threat actors and criminal organizations (Anthropic 2025c, 2025b; Google Threat Intelligence Group 2025a, 2025b).

However, whether and how terrorist organizations — which tend to possess levels of resources and networks that enable more lethal attacks than lone wolves (Alakoc 2017; Phillips 2017) — are adopting AI remains largely unknown. A literature review found that the limited scholarship on the topic of AI misuse by terrorist organizations "relies primarily on speculative and theoretical arguments" about potential future use (Houser and Dong 2025, 7).[4] The authors therefore note that "one of the most significant weaknesses of the existing literature is the lack of empirical work focused on terrorists' AI use" (Houser and Dong 2025, 17).[5] Beyond academia, the lack of evidence and understanding of the national security threat posed by terrorist groups using AI has informed the Generative AI Terrorism Risk Assessment Act, which seeks to require the U.S. Department of Homeland Security to "take steps to recognize, assess, and address such threat" to the United States through an annual analysis of incidents in which a foreign terrorist organization or individual has used or attempted to use generative AI for terrorist activity (U.S. House of Representatives 2025).

Some initial empirical evidence has emerged from analyses of online content and propaganda materials (Humphrys 2024; Criezis 2024; Stalinsky 2025). Specifically, the BBC has analyzed jihadist experimentation with AI based on official and unofficial Islamic State and al-Qaeda propaganda released in 2024 on Telegram, Rocket.Chat,

[4] Of 1,138 identified records, only 28 fulfilled the inclusion criteria, most importantly whether they actually address the issue of AI-enabled terrorism (Houser and Dong 2025, 5). Of the 28, only two were based on empirical work: one qualitative experiment using ChatGPT (Lakomy 2023), and a survey of national security experts (UNOCT and UNICRI 2021).

[5] While the conclusion still holds, limiting the analysis to academic articles and government reports misses relevant work considering that "the evolution of AI is rapid and that scholarly literature might lag behind the current state-of-the-art at the time of publication," as the authors themselves admit (Houser and Dong 2025, 6).

X, and Facebook (Humphrys 2024). The analysis shows that AI has mostly been used to generate and translate jihadist propaganda by unofficial jihadist media groups and individual content creators. Examples include AI-generated news broadcasts, with synthetic presenters reading Islamic State attack claims taken from the group's Telegram channels and its weekly newsletter *al-Naba*, and images and videos depicting militants at global landmarks. ISIS supporters and sympathizers have been especially active in spreading AI-generated propaganda. To leverage AI efficiently and securely, a guide was published by a pro-ISIS tech support group entitled "How to protect your privacy when using [the AI content generator]" (Tech Against Terrorism 2023). Another "Guide to AI Tools and Their Dangers," published in April 2025 in English and Arabic by the Qimam Electronic Foundation (QEF), a pro-ISIS media house, stated that information security risks "must be carefully managed" (Marzuk and Green 2025). Similarly, two pro-al-Qaeda media outlets jointly published a technical guide on how to use ChatGPT for propaganda in February 2024, but the group's supporters have overall exhibited less AI engagement so far compared with ISIS supporters (Humphrys 2024). In a comprehensive analysis of online chats and propaganda materials, Stalinsky (2025) also found jihadist supporters using AI to expand their propaganda, recruitment, and operation.

Moving beyond the use of AI for propaganda, a pro-ISIS outlet emphasized the importance of AI for the future of jihad, stating that it "isn't just a technology, it's becoming a force that shapes war." Hence, "[f]or every individual, regardless of their field of expertise, grasping the nuances of AI has become indispensable," one author states. Another author writing in the same publication gives concrete examples by suggesting that AI tools could serve as "digital advisors" or "research assistants" (Makuch 2025). Such statements echo those posted on ISIS-operated servers on Rocket.Chat as early as December 6, 2022, when a user explained how he had used ChatGPT for advice on supporting the caliphate (Stalinsky 2023). He shared

ChatGPT's responses, which covered detailed steps for identifying and mobilizing a "core group of supporters," developing a "political program and ideology," gaining support from "the Muslim community," taking "control of territory," establishing "institutions and government structures," and promoting and defending the caliphate. The user concluded that the model is "smarter than most activists," and others who tested Perplexity agreed that AI could assist in the global jihad (Stalinsky 2023). However, as noted by Broekaert & Clarke (2026), "[s]o far, AI use within the Islamic State ecosystem appears to cluster around low-hanging applications: generative propaganda imagery and anasheed, automated translation, basic operational ideation, and exploratory discussions about coding, drones, and cyber activity. There is not yet any proof of whether the speculative uses of AI that Islamic State supporters mention in online forums have materialized in actual attacks."

Online conversations also reveal concerns and controversies over AI adoption (Humphrys 2024). In addition to worries about information security, there have been debates over whether AI-generated images and voices violate Islamic prohibitions on pictorial and audio representations of humans. For example, the presenter's face in an AI-generated news bulletin was blurred in response to criticism that showing animated human faces was forbidden (*haram*), though concerns persisted about depicting animated beings at all. Text-to-speech tools have generated additional controversy, with users arguing that they should not be used because they are based on the voices of "infidels" and mispronounce Arabic words commonly used in jihadist messaging. Mockery by al-Qaeda-affiliated groups also appears to have led the Islamic State Khorasan Province (ISKP) to withdraw statements embracing and promoting the use of AI (Al-Lami and Humphrys 2025), although the group has since returned to encouraging the use of AI among supporters for assisting with religious campaigns and preaching in its magazine "Voice of Khorasan" (Boycott-Owen 2026).

Despite these insights, it remains largely unknown if or to what extent terrorist organizations are actually leveraging AI. First, the presented evidence covers jihadist supporters and sympathizers as well as pro-ISIS, though noninstitutional, media houses active on online platforms — not terrorist groups and their official organizational entities. News reporting and blog posts regularly conflate terrorist organizations with their online supporters, wrongly attributing AI-generated content produced by sympathizers in online forums to the groups themselves.[6] Analysts who distinguish between these actors have in fact noted the "relatively slow rate of adoption" (D. Wells 2025) by terrorist groups and concluded that there is a surprising reluctance to embrace AI among official jihadist media outlets, with uptake "not yet proved as widespread as might be expected" (Humphrys 2024).

Second, whether due to data availability or implicit assumptions about terrorist priorities, existing research on AI and terrorism is skewed toward online propaganda and recruitment. But even when posted by official media teams, it captures only one type of use, and one that is intended to be seen. While AI-generated propaganda may signal broader adoption, its absence does not establish that groups are not drawing on AI for other purposes. They might still seek operational and tactical support, such as for bombmaking, cyber capabilities, or attack planning, all of which is less likely to be presented online. Beyond empirical blind spots, anchoring analysis to propaganda also creates conceptual blind spots when thinking about high-risk use cases. For instance, Adam Hadley of Tech Against Terrorism concluded from analyzing terrorist and violent extremist online content that "[f]uture risks include terrorists leveraging AI for rapid application and website development, though fundamentally, generative AI amplifies threats posed by existing technologies rather

[6] ISKP might be an exception here as it released AI-generated news bulletins to claim attacks in March and May 2024 via its semiofficial propaganda wing Al-Azaim Media and has reportedly been "looking for recruits internally within the IS Jihadist ecosystem to train in artificial intelligence" (Firdous 2024).

than creating entirely new threat categories" (Makuch 2025). It is unclear how such predictions follow from evidence limited to online content and propaganda, particularly for a technology whose misuse risks range from large-scale explosive attack to CBRN weapons development, and that are considered serious enough by governments and AI developers to warrant dedicated capability assessments and safety frameworks.

RESEARCH DESIGN & METHODS

To address the lack of empirical evidence on how terrorist groups are using AI, this study employs a fieldwork-driven case study of Boko Haram, examining both the Islamic State West Africa Province (ISWAP) and Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād (JAS) faction.[7] Field research directly engaging with militants has been essential in conflict studies for explaining violent outcomes in ways external observation cannot capture (Wood 2003; Weinstein 2007; Fujii 2011; Mampilly 2011; Cohen 2016), and understanding how terrorist groups adopt and weaponize new technologies benefits from qualitative insights into internal organizational processes, such as leadership preferences, resource constraints, and decision-making (Ackerman 2016, 2023; Tishler 2018; Dolnik 2007), as detailed case studies have demonstrated (Danzig et al. 2012; Mowatt-Larssen 2010; Santhana Dass 2021). If and how actual adversaries are choosing to use AI not only matters for assessing and addressing immediate risks but for informing threat models, identifying vulnerabilities in model safeguards, and establishing a baseline for tracking how terrorist use of AI evolves over time.

The case selection followed several considerations. First, Boko Haram follows a Salafi-jihadist ideology combining maximalist political objectives with millenarian elements (Kassim 2015; McCants 2015; Thurston 2016, 24; Zenn 2020). Although ideological beliefs in armed groups are neither static nor uniformly held among members (Leader Maynard 2019; Parkinson 2021), at the organizational level this orientation leads to fewer internal constraints on pursuing capabilities that could cause large-scale harm. This makes it more likely that the group would consider the

[7] Throughout this report, Boko Haram is used as an umbrella term for ISWAP and JAS.

full spectrum of AI applications, including the most dangerous ones from which other groups might refrain.[8] Second, as detailed below, both factions have demonstrated remarkable resilience over more than a decade of sustained military pressure, with ISWAP distinguished by the deliberate integration of new technologies into its operations (Samuel 2023), and JAS by rapid tactical reinvention (Vasseur et al. 2022). Together, ideological motivation and a track record of technological and tactical adaptation make Boko Haram a strong candidate for AI experimentation. Third, research conditions and access made this type of study feasible. High defection rates have created opportunities to interview former commanders with recent operational knowledge (Maclean and Alfa 2021; Adebayo 2025), while relative stability in certain urban locations makes fieldwork in an active conflict zone possible. Importantly, my previous doctoral research in northeast Nigeria with former Boko Haram members provided the groundwork for this study (Juelich 2024, 2026). It enabled me to draw on established contacts and networks, as well as contextual understanding of the conflict and security dynamics essential for safely accessing this population.

Data collection occurred over two rounds in 2025 and 2026 in northeast Nigeria, specifically in Borno state and Adamawa state.[9] I carried out 57 semi-structured interviews with a total of 27 former members of ISWAP and JAS, the majority of whom previously held commanding and/or specialized technical positions within either or both factions.[10] Each interview lasted approximately 90 minutes, with an interpreter present. I obtained informed consent and ensured participant protection

[8] Research has shown that jihadist groups, particularly those with apocalyptic beliefs, demonstrate higher lethality than other terrorist organizations, killing more people per attack and exhibiting higher kill-wound ratios (Levy 2019). In fact, the Islamic State, operating as a decentralized network of affiliates, continues to be the deadliest terrorist organization globally (Institute for Economics & Peace 2025).

[9] For a detailed description, see the Appendix "Fieldwork Methods and Practices."

[10] For a breakdown of participants, see the Appendix "List of Interviewees."

by anonymizing all data and refraining from recording names. Any information that could potentially identify participants was altered to protect their safety.

The two rounds of data collection differed in sampling emphasis. The first round was more exploratory, and while I prioritized former members with commanding authority, it became clear that a subset of participants, predominantly women in lower-ranking leadership roles (*amiras*), lower-ranking male commanders (*amirs*), and rank-and-file combatants, tended not to have knowledge of the group's AI use. Recognizing this, I adjusted the sampling strategy in the second round to more deliberately target mid- to senior-level commanders and technical specialists likely to have direct or indirect exposure to AI-related activities, which reduced the proportion of participants without knowledge of AI use significantly. Of the 27 participants, 12 had no knowledge of their faction's use of AI, reflecting the rank-based access restrictions described in this research. The remaining 15 participants (seven from JAS and eight from ISWAP) were knowledgeable about AI use, providing the accounts that form the empirical basis of the findings below. Participants without knowledge of AI use nonetheless contributed meaningfully to the study, providing detailed accounts of the group's broader approach to technology adoption, organizational dynamics, and operational practices that contextualize and corroborate the AI-specific findings reported by other participants.

Data analysis employed thematic coding to identify patterns across three primary domains aligned with the research questions. First, I analyzed patterns of technological adaptation. Within that category, I examined innovation processes, skill acquisition and training procedures, and responses to operational challenges and constraints. This captured how the groups learned about and implemented new technologies and tactics more generally. Second, I coded for AI adoption specifically across the following dimensions: awareness, exposure, and access to LLMs; training,

skill acquisition, and institutionalization; and use cases during participants' membership. Third, I examined attitudes toward innovation, AI, and different types of violence and weapons. Finally, I searched for signs of convergence and differences across these domains between ISWAP and JAS. While both factions are represented throughout the empirical sections, ISWAP members are quoted more frequently than JAS members, reflecting the greater depth of AI-specific knowledge among them, which could be indicative of the more formalized and centralized nature of AI integration within ISWAP relative to JAS.

Interpreting qualitative data, especially from former armed group members, requires careful consideration (Fujii 2010; Brounéus 2011). Respondents may overstate their group's capabilities and their own roles within it. Conversely, they may understate or conceal sensitive operational information due to security concerns or fear of legal repercussions. Aside from deliberate misrepresentation, respondents may also unintentionally distort accounts through selective memory or retrospective rationalization. While these limitations apply to qualitative research generally, controlling for accuracy is much more difficult in conflict zones where "access to informants is restricted and one has to depend on whom one can get close to" (Helbardt et al. 2010, 258).

I attempted to mitigate these risks through the following measures. First, I triangulated accounts across respondents for accuracy and cross-referenced findings with secondary sources where possible. To do so, I established several independent entry points to interviewees, accessing participants across different communities in different states through separate community contact persons. This meant that respondents recruited through different channels could serve as an independent check on one another, reducing the risk that a single gatekeeper shaped or filtered the accounts I received. Second, I met with most respondents multiple times, which

allowed trust to develop over the course of the interview process and created opportunities to revisit accounts that seemed inconsistent or incomplete. Third, I benefitted greatly from the rapport and connections my research assistant had established with participants prior to and during fieldwork, which facilitated candid engagement that would have been difficult to achieve through cold access. Fourth, because the study turned on a specific and unfamiliar technology, care was taken to convey the concept of AI accurately across languages. The research assistant rendered key terms in both Hausa and Kanuri and, more importantly, rather than relying on a single translated label, we walked participants through the distinction between AI tools and computers or the internet more generally. I also tested some participants with a standard search-engine page on my laptop — instead of an LLM web interface — to see whether they would recognize that it was not the AI tool. They did, and when asked how the AI tool would be used, their responses reflected the basic process of prompting. Fifth, rather than asking about AI upfront, I began by tracing participants' conflict experiences and the group's broader approach to technology and innovation, allowing the topic to come up in the context of an individual's specific role. This reduced the risk of respondents calibrating their answers to what they expected I wanted to hear.

Some participants refused to answer certain questions, visibly circumvented them, or said they did not know, which lent greater credibility to the information they did provide. At the same time, not all data collected here makes claims to factual accuracy in the same way. Respondents' perceptions of AI's capabilities and their group's engagement with it are analytically valuable in their own right. How members talk about AI reveals something about organizational culture, priorities, and disposition toward a technology that is indicative of how adoption may develop over time and that neither platform-level data nor external observation could capture. Finally, beyond the matter of veracity, all of these methodological choices

reflect broader principles for conducting ethical and rigorous fieldwork with conflict-affected populations (Thaler et al. 2024; Fujii 2012; Cheng and Day 2024; Wood 2006).

There are several limitations to the study's methodology. For security reasons, I interviewed only defectors who had left at least several months prior, not active members. Given that AI capabilities are advancing rapidly, the research therefore does not capture the most recent developments.[11] Additionally, I interviewed former commanders with direct technical responsibilities, and those closely working with them, but not individuals who held top leadership positions at the highest organizational levels where decisions about AI appear to be made. Finally, as a case study, findings cannot be directly generalized to other terrorist organizations. However, Boko Haram is broadly representative of the type of armed group that drives contemporary conflicts and terrorism in that it is an Islamic extremist group fighting a protracted insurgency (Rustad 2025; Institute for Economics & Peace 2025). Africa has experienced a particularly sharp increase in Salafi-jihadist violence over the last two decades (Faleg and Mustasilta 2021), becoming the new frontier of global jihad (Raineri 2022; T. Bacon and Warner 2021; Thomas 2025) and epicenter of terrorism (Institute for Economics & Peace 2025). Findings from this case may therefore have relevance well beyond the Lake Chad Basin, especially given both factions' integration into global jihadist networks.

[11] However, the sample includes one participant who could speak to the use of AI until mid-2025.

THE CASE

Boko Haram, which emerged in northeastern Nigeria in the early 2000s and was first led by Mohammed Yusuf, advocates for the implementation of strict Islamic law and rejects Western education and institutions. Following a violent government crackdown and Yusuf's death in police custody in 2009, the movement turned into a jihadist insurgency under the leadership of Abubakar Shekau. The conflict has killed approximately 43,000 people, displaced about 3.1 million, and left more than 4 million severely food-insecure across the Lake Chad Basin region spanning Nigeria, Niger, Chad, and Cameroon (UN OCHA 2025; Council on Foreign Relations 2023).[12]

In 2015, Boko Haram pledged allegiance to the Islamic State, becoming the Islamic State West Africa Province (ISWAP, also referred to as ISIS-WA and IS-WA). However, ideological and tactical disagreements within the leadership led to a split in 2016. ISWAP, led initially by Habib Yusuf al-Barnawi, emphasized targeting government forces and infrastructure while reducing civilian casualties to build popular support. The original faction, known as Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād (JAS), remained under Shekau's leadership until his death in 2021 following an ISWAP offensive, which further escalated the interfactional conflict that continues to the present day (Foucher 2024; International Crisis Group 2024).

[12] Scholars have analyzed the conflict's origins, drivers, and trajectory, including in terms of its ideological and historical roots in the region's tradition of Islamic reformism (Abubakar 2017; Loimeier 2011; Last 2014; Walker 2016), contemporary intra-Muslim and intra-religious dissent (Mustapha and Bunza 2014; Mustapha and Ehrhardt 2018), the escalating dynamics with Nigerian security forces and civilian self-defense groups (Comolli 2015; Thurston 2018; Smith 2015), internal factionalization and external ties to global jihadist networks (Kassim 2018; Mahmoud 2018; Zenn 2020), and socioeconomic and political drivers of recruitment (Meagher and Hassan 2020; Mustapha 2014).

Boko Haram has been characterized as among the most adaptable violent non-state actors, with a high capacity for innovation and rapid responses to changing operational environments (Vasseur et al. 2022). ISWAP has exhibited a certain degree of organizational sophistication. It has built governance structures and taxation systems in territory it controls (International Crisis Group 2024); adapted commercially available technologies for military purposes, ranging from establishing satellite internet access in remote areas of the Lake Chad Basin to weaponizing drones (Samuel 2023); and has emerged as a key node in the Islamic State's global network (Zenn 2020) with "the ability to carry out complex attacks outside its conventional areas of operation" (UN Security Council 2024, 9).

Both factions have been designated by international bodies due to their associations with the global terrorist networks of al-Qaeda and the Islamic State (UN Security Council 2020), and recent U.S. missile strikes and troop deployment appear to have been at least partially a response to the growing regional threat of a jihadist corridor connecting the Sahel with the Lake Chad Basin region (The Soufan Center 2026; Samuel 2026a). Together, these dynamics point to Boko Haram not merely having survived but continuing to evolve in capabilities and reach.

THE FINDINGS

AI Adoption

Boko Haram uses multiple frontier AI systems. To identify the providers, participants were shown sheets displaying the logos of six AI chatbots in randomized order — OpenAI's ChatGPT, Anthropic's Claude, Google DeepMind's Gemini, xAI's Grok, Meta AI, and DeepSeek — and asked which they had used themselves or seen used. Those who could recognize logos identified varying combinations of AI systems as having been used, with all six identified across participants collectively. Because computer access is restricted by rank, not all participants who were aware of their group's AI use had seen which platforms were used. Exposure varied by camp, which means that junior members were present when commanders used the tools in some places, while access was more tightly controlled in others (discussed below).[13] Among the few participants who could speak to it, ChatGPT was named as the chatbot that was adopted first.[14] This is in line with its earlier market release and

[13] The logo-identification exercise was introduced only in the second round of data collection, and I treat it as secondary to the credibility of interviewees' accounts. Among the second-round interviewees with knowledge of their faction's AI use, five recognized specific logos (four from ISWAP, one from JAS) and seven did not. The latter included four Lake Chad ISWAP commanders who described the especially strict access controls in their camps. I read their candor about not having been in a position to see the interface as a marker of their reliability rather than a limitation, particularly as the information they did provide was detailed, internally coherent, corroborated across accounts, and confined to what they could plausibly have observed or been told. First-round interviewees were not shown the logo sheets, but I informally showed the ChatGPT logo alone to several who knew about AI use, of whom two JAS members and one ISWAP member (the latter also interviewed in the second round) recognized it. Because this informal exposure was not conducted systematically, I report it separately rather than folding it into the figures above.

[14] Of the participants who expressed a view, four identified ChatGPT as the first adopted and most heavily used (ISWAP Commander-5, ISWAP Commander-7, ISWAP Commander-17 and JAS Commander-3, 2026), and one named Gemini (ISWAP Commander-24, 2026), while the remainder could not speak to the sequencing or intensity of use.

status as the world's most widely used LLM, but specific reasons for system preference and variation in use by purpose could not be systematically determined from participant accounts.

When asked who had introduced them to AI, former ISWAP members unanimously stated that they had received external assistance from "the foreigners."[15] "The white guys came and taught us," a former ISWAP *munzir* (mid-ranking commander) said, further clarifying that he was referring to operatives from Libya, France, and Arab countries with a lighter complexion than their own.[16, 17] "The real source is ISIS,"[18] he added, while a former *naqib* (a rank below *munzir*) similarly stated that "[t]he key players are Arabs who are in charge of all of this AI."[19] Without being able to determine the precise origins, interviewees mentioned that ISIS-linked trainers who visited their camps, and others who provided assistance from abroad, were part of its global network from countries such as Algeria, Libya, Mali, Niger, Somalia, Sudan, Iraq, and Afghanistan.[20] Although it was not always clear whether all such references were specific to AI assistance or to external support more broadly, Iraq and Libya were most frequently cited in connection with AI training specifically.[21]

---

[15] Interviews with ISWAP Commander-7, ISWAP Fighter-20, ISWAP Commander-21, ISWAP Commander-22, ISWAP Commander-23, ISWAP Commander-24, 2026.
[16] Interview with ISWAP Commander-7, 2025.
[17] In ascending order of seniority, the relevant ranks run *amir* (village head) → *naqib* (lieutenant) → *munzir* (captain) → *qaid* (major) → *fiya* (senior commander) → *jaysh* (army commander) → *wali* (provincial head). Within ISWAP, "a *munzir* commands about 100 men, and a *qaid* about 400" (Foucher 2024, 16). JAS uses broadly the same ranks but is less formalized and is ultimately headed by an *imam*. For a detailed organizational mapping of ISWAP and JAS as of July 2024, see Foucher (2024).
[18] Interview with ISWAP Commander-7, 2026.
[19] Interview with ISWAP Commander-22, 2026.
[20] Interviews with ISWAP Commander-5, ISWAP Commander-7, 2025; ISWAP Fighter-20, ISWAP Commander-21, ISWAP Commander-22, 2026.
[21] Interviews with ISWAP Commander-7, ISWAP Fighter-20, ISWAP Commander-21, 2026.

While ChatGPT was discussed among ISWAP's religious leaders as early as 2022, especially in terms of "how it affects our beliefs, and how we can Islamize it rather than letting it modernize us,"[22] the foreign operatives initiated its uptake during a series of visits that interviewees dated to around 2023, continuing in 2024 and 2025.[23] The scale and duration of these visits seemingly varied across ISWAP's different strongholds in Borno state. Participant accounts describe groups of up to 20 trainers, with stays ranging from brief visits to several months depending on where they were based, though only a very small number within each group were specifically focused on AI instruction. "Among the foreigners [who came to the Lake Chad islands], one was highly trained. He studied in Russia. [...] He understands technology and knows a lot about AI. He was the main AI trainer," explained a former war strategist.[24] Some ISWAP commanders themselves also regularly travel for training purposes, making trips to Libya and Mali.[25] Taken together, these accounts suggest a pattern of repeated, sustained AI training across multiple locations and years, rather than a single event.

These efforts are part of a long-standing trajectory of Islamic State assistance to Boko Haram that dates back to Shekau's pledge of allegiance in 2015 (Zenn 2020; Mahmoud 2018; Bukarti 2022), and a more recent ramping up of support to the Lake Chad Basin and the Sahel, potentially laying the foundations for an African "caliphate," as reporting in the Islamic State's official weekly Arabic-language newsletter *al-Naba* indicates (Samuel 2025).[26] According to findings by Samuel (2025),

[22] Interview with ISWAP Commander-5, 2026.
[23] Precise dating is difficult to establish. Timelines were reconstructed from interview accounts anchored to events respondents could reliably place, such as when they left the group. Notably, individuals who departed as early as 2023 reported exposure to AI, suggesting uptake began around that time, and possibly earlier.
[24] Interview with ISWAP Commander-24, 2026.
[25] Interviews with ISWAP Commander-7, ISWAP Commander-22, 2026.
[26] As mentioned above, the transition of jihadist activity from the Middle East toward Africa has been ongoing for a decade (Hansen 2022; T. Bacon and Warner 2021; Raineri 2022).

the Islamic State deployed seven instructors to ISWAP in 2024 to provide specialized training, including on drone operations, the assembly of vehicle-borne improvised explosive devices (VBIEDs), electronic device hacking, and advanced combat tactics.[27] The AI training fits neatly within these intensified knowledge-transfer efforts, building on a history of financial and operational support.[28] In fact, some interviewees recognized the names of two trainers identified in Samuel's reporting (2025), stating that they had supported ISWAP with AI but were "not the main guys."[29] According to the *munzir*, the technical support generally provided by the Islamic State has played an outsized role in the group's success, even more than the material assistance: "They teach us how to use guns and other technologies that we would otherwise not have been able to use," he said.[30] Another confirmed that "[t]here were a lot of Arabs from Afghanistan and Iraq that lectured us. That is the main reason why we excel."[31] AI assistance appears to be the latest chapter in this exchange.

To understand the implications of this knowledge transfer for AI diffusion and skill development, it is important to consider the Islamic State's internal structure. Unlike al-Qaeda's decentralized branches, the Islamic State's provinces (*wilayas*) form an integrated global network, organized under the General Directorate of Provinces (GDP), that ties the provinces to the Islamic State's central organization (Hamming

[27] Two of them have appeared in Islamic State's propaganda videos in 2024 and have been identified as Abu Ishaq al-Maqdisi and Abu Juwayriya al-Maghribi (Samuel 2025).
[28] Since Boko Haram pledged allegiance, the Islamic State has provided remote military advice, sent Arab trainers to Nigeria to conduct courses on strategy and tactics, and invited ISWAP associates to meet with Islamic State representatives in Libya, Sudan, and the Gulf. For more detailed information, see Foucher (2020).
[29] Interviews with JAS Commander-3, ISWAP Commander-7, 2026. The JAS commander did not claim that JAS has received training from these individuals. He recognized their names and confirmed awareness of their role in training ISWAP, reflecting knowledge of ISWAP's external support rather than a shared training relationship.
[30] Interview with ISWAP Commander-7, 2025.
[31] Interview with ISWAP Commander-24, 2026.

2023). According to the U.S. State Department (2023), "ISIS Core has relied on its regional General Directorate of Provinces (GDP) offices to provide operational guidance and funding around the world." In addition to GDP's key role in influencing military and economic affairs, it also contributes to external attack planning and execution, making external operations pan-provincial (Zelin 2024). The regional GDP office known as *al-Furqan* oversees the Lake Chad Basin, the Sahel, and North Africa (Hamming 2023; Rousselle 2025) and is apparently headed by ISWAP leader Habib Yusuf (Foucher 2024, 13–14), following the recent death of former co-leader Abubakar Mainok (Samuel 2026b). It is therefore conceivable that the LLM assistance ISWAP obtained under *al-Furqan* was similarly provided to other provinces under that office, and to those under other regional GDP offices.[32] Viewing findings on AI adoption by a specific ISIS province independent of its integration into the Islamic State's global network therefore is likely to underestimate the scale of AI uptake. Relatedly, these linkages may also matter when evaluating, for example, the type and sophistication of AI usage or financial requirements for AI-enabled weapons development. In fact, provinces are obliged to share monthly reports on their military situation with the GDP for knowledge transfer and advice, and to contribute funds that are redistributed within the network where needed (Hamming 2023; Zelin 2024). While it remains unknown if similar knowledge- and resource-sharing obligations extend to AI, existing structures could theoretically facilitate it and accelerate uplift.

The diffusion of AI training is not limited to the Islamic State's network. Former JAS members, whose faction is at war with ISWAP, also reported that their group

[32] However, ISWAP may have received preferential access as the Islamic State's currently most active and lethal province globally. According to data published by *al-Naba*, ISWAP claimed the highest number of attacks (445) and casualties (1,552) between July 2024 to July 2025 among all Islamic State provinces (Garofalo 2024).

received such training.[33] A former *qaid* who oversaw operations in Cameroon explained that they were first introduced to ChatGPT during one of their quarterly coordination meetings "with the foreigners," who subsequently set up training sessions with a small group of selected leaders.[34, 35] This aligns with the account of another JAS ex-combatant who stated that "about three of their *amirs* got the training from top leaders from Arab countries."[36] For context, this cuts against the prevailing understanding of the movement. JAS is generally seen as the more locally focused and isolated faction, yet the fieldwork indicates that it too received external assistance. These external connections may build on JAS's long-standing international jihadist ties, with some JAS militants having spent time with al-Qaeda in the Islamic Maghreb (AQIM) in Algeria and Mali following the death of Boko Haram's founder in 2009 and with al-Shabaab in Somalia (Mahmoud 2018; Zenn 2020).[37] That rival factions also received external technical assistance suggests that AI training is spreading through multiple jihadist networks, resulting in parallel expertise-building initiatives. Diffusion may be further reinforced by the fact that, despite being rivals, ISWAP and JAS are not entirely independent entities. Members have switched sides, and personal ties persist across factional lines, making it possible that AI knowledge may also circulate informally.

---

[33] Interviews with JAS Commander-3, JAS Fighter-11, JAS Commander-12, 2025; JAS Fighter-25, JAS Commander-27, 2026.

[34] While JAS uses the same ranks as ISWAP, troop allocation is less standardized and systematic (Foucher 2024, 19).

[35] Interview with JAS Commander-12, 2025.

[36] Interview with JAS Fighter-11, 2025.

[37] The study cannot establish who provided assistance to JAS. The possibilities range from individual sympathizers with no formal ties to the global franchises, to al-Qaeda elements, to the Islamic State itself keeping a channel open to JAS in the hope of drawing it back into the fold.

Organizing AI Access & Expertise

The AI training consisted of senior members coming together for a general introduction, demonstration of use cases, and continuous assisted experimentation. "The white guys assembled the top people in a room. They used a projector to show how it works on a big screen," explained the ISWAP *munzir*, adding that this was where he first saw the OpenAI logo.[38] "Each battalion of 500 fighters sent their top people to participate and learn how to use the technology," resulting in an estimated 30 to 50 leaders and selected fighters. They were drawn from the entire ISWAP territory — "from Timbuktu to Tumbuma" — and took part in one of the main training sessions in the Lake Chad stronghold.[39] JAS organized training similarly. "In the general training they did on AI, they tried to find smart and technical people among the fighters," said a JAS *munzir*.[40] "They were given demonstrations on how to use the robot [a term used to describe AI chatbots]," another respondent said.[41]

Following the training, the most capable among the fighters formed specialized AI units, with respondents suggesting team sizes between five and 20 people.[42] At other times, the foreigners selected those with "special knowledge, like bombing or spying"[43] or with "computer literacy"[44] for training. These units appear to operate in ISWAP's major regional strongholds.[45] As a former deputy *munzir* explained, "Sambisa has a special unit, Timbuktu has one, Lake Chad has one," suggesting that

[38] Interview with ISWAP Commander-7, 2025.
[39] Interview with ISWAP Commander-22, 2026.
[40] Interview with JAS Commander-26, 2026.
[41] Interview with JAS Fighter-11, 2025.
[42] Interviews with ISWAP Commander-7, 2025; ISWAP Commander-17, ISWAP Fighter-20, ISWAP Commander-21, ISWAP Commander-24, 2026.
[43] Interview with ISWAP Commander-21, 2026.
[44] Interview with ISWAP Commander-23, 2026.
[45] ISWAP has divided its territories into two provinces (*wilaya*), which are in turn subdivided into a total of five smaller districts (*mantiqa*) (Foucher 2024, 14–15).

each main command has its own dedicated AI unit.[46] The Lake Chad unit in ISWAP's core territory has been described as the highest-ranked of these,[47] and as being "directly supervised by ISIS,"[48] which, even if exaggerated, is suggestive of very close ties. Similarly, within JAS, "people from different units form the AI unit, like a bombmaker, a computer specialist, a gun specialist, and an engineer. The top leaders form the key unit, but then there are smaller ones in different locations. We have four *fiya* [senior commanders] and each *fiya* has this unit under them."[49]

In both groups, these technical, non-combat units are positioned alongside the military hierarchy, just like other non-military units, from internal security to the Islamic police to administration. That members were drawn from senior functional roles reflects the applied nature of AI use within each organization and its integration with operational and technical domains, discussed in more detail in the following section. It also indicates that leadership places significant value on AI, considering that this staffing decision carries an opportunity cost, since those qualified individuals are no longer contributing as fully to other areas. It further reflects ISWAP's broader organizational model of centralized military power, based on that of the Islamic State (International Crisis Group 2024, 9), and a preference for smaller, well-controlled, and well-trained units, in contrast to JAS's larger militia-style formations (Foucher 2024, 16). Accordingly, the deployment of LLMs has been ordered from the top, integrated within the centralized chain of command, and entrusted to a dedicated cadre of specialists rather than disseminated broadly. Having a separate, specialized research and development unit has been shown to be an important factor for successful terrorist innovation (Ackerman 2016, 5), but the

[46] Interview with ISWAP Commander-17, 2026.
[47] Interview with ISWAP Commander-24, 2026.
[48] Interview with ISWAP Commander-23, 2026.
[49] Interview with JAS Commander-3, 2026.

concentration of knowledge within a small team can also make it a high-value counterterrorism target.

The special units have at least three responsibilities. First, they are in charge of the operational AI infrastructure, managing devices and accounts.[50] The foreign operatives arrived with additional laptops that were distributed. "You cannot use other laptops because they were specifically assigned for this purpose [of AI use]. We have lots of smart people with degrees who control the systems and have this level of technological understanding," explained the ISWAP *munzir*.[51] The group holds premium subscriptions with multiple providers, having "different accounts with different companies."[52] Regarding account management, the former ISWAP war strategist explained: "We have people in different places who set up accounts that can't be linked to us. They also pay for the subscriptions. When we need anything, these people pay for us. We have leaders in Sudan and all over who do the subscriptions for us."[53] When asked whether they use fake email accounts, he denied this, stating instead that they belong to "real people elsewhere." Others similarly suggested that the email accounts belong to people in the wider network of supporters, or to deceased members.[54] The specifics of whose accounts are used remains somewhat unclear, as respondents confirmed that the AI units were managing these matters and that they themselves were not allowed to set up accounts individually. As the *munzir* further added, "I don't know who installed it and signed up. I was just told what platforms to use."[55] What is clear, however, is that account setup and management is closely coordinated with ISIS-linked intermediaries.

---

[50] Interviews with ISWAP Commander-7, ISWAP Commander-17, 2026.
[51] Interview with ISWAP Commander-7, 2026.
[52] Interview with ISWAP Commander-5, 2026.
[53] Interview with ISWAP Commander-24, 2026.
[54] Interviews with JAS Commander-3, ISWAP Commander-5, 2026.
[55] Interview with ISWAP Commander-7, 2026.

Second, the units are responsible for building capacity through internal training, passing on what they learned from the foreign operatives to the military command. A former ISWAP fighter explained that "the original unit trained about 10 people in 12 different camps in Lake Chad," who were then responsible for instructing others.[56] "They took them rank-by-rank. The major goal was to equip commanders with this knowledge, so that fewer people will die in the war, and to get new tactics."[57] Each unit commander is supposed to learn to use AI for day-to-day operational purposes, specific to their unit's needs. Knowledge thus trickles down the military hierarchy until the level of *qaid*, which unanimously emerged as the last rank authorized to use LLMs. Some ISWAP *munzirs* had exposure to the tools, but were not permitted to use them independently:

> Our leader, *baba qaid*, who is technologically sound, also has a leader who taught him these things. [...] There is comprehensive training for those who handle the systems, like above the level of *munzir* [which is the rank of *qaid*]. For others like me [deputy *qaid*], it is just in case of emergency to know how it works. [...] *Baba qaid* showed me how to use it. He said this software will help give us new tactics. I sat next to him and watched on the laptop when he put me through the process of typing questions. [...] I was trained bit by bit. Because I was a commander, I was often out on missions, but my *qaid* would call me occasionally to show me how he used it.[58]

The description from a former JAS commander is similar:

> There is a specific unit in Sambisa that is dedicated to AI. They don't go to war. Their role is to disseminate information on how to use AI. They are training the people in the hierarchy. [...] There are 23 in the unit. They have a special room that is powered with solar. The unit sits directly under the leadership. [...] They come and gather people around a laptop. They type and then show them step-by-step how to

[56] Interview with ISWAP Fighter-20, 2026.
[57] Interview with ISWAP Commander-7, 2026.
[58] Interview with ISWAP Commander-7, 2026.

> ask questions. [...] The training is received by the *imam*, *jaysh*, *fiya*, and *qaid* [in descending order of seniority].[59]

He explained that each *qaid* oversees ten commanders with different specialties, of whom he was one. The ten of them would sit around a computer while their *qaid* introduced them to the different LLMs and instructed them on how to use them. Generally speaking, there seemed to be more discretion within JAS to pass on this knowledge as commanders tried to train "intelligent fighters who understand tech and can take notions of AI guidelines," he added. Internal AI training thus forms part of Boko Haram's broader approach to knowledge acquisition. It combines foreign assistance and the internal recruitment and training of subject-matter expertise, as employed in the case of AI, with horizontal knowledge transfer between regional commands, and the recruitment or coercion of external professionals when skills are lacking.[60, 61]

Limiting AI access to certain ranks reflects an effort to balance the benefits of LLM use with operational security risks. Internet access is generally only granted to mid-level and senior leadership, while lower-ranking members use phones without internet access, and foot soldiers are limited to devices without SIM cards.[62] This

---

[59] Interview with JAS Commander-3, 2026. Regarding the reference to Sambisa, it should be noted that its core has been under ISWAP control since 2021, despite frequent and ongoing contestation (Africa Defense Forum 2026a). Upon follow-up, this interviewee, and a few others who similarly referenced Sambisa, clarified that they were referring to the forest's outer areas, some of which reach into the Gwoza Hills at the border between Nigeria and Cameroon, where JAS continues to hold territorial power. JAS-affiliated respondents appeared to still conceptually regard Sambisa as their territory, which could have produced this imprecision.

[60] Interviews with JAS Technical Specialist-10, ISWAP Fighter-9, ISWAP Commander-5, ISWAP Commander-7, 2025.

[61] As AI expertise will become more prevalent, with Nigeria showing some of the highest levels of AI adoption and trust globally (Gillespie et al. 2025), external recruitment could supplement the current strategies.

[62] Interviews with ISWAP Fighter-9, ISWAP Commander-7, 2025.

policy seeks to both prevent information leakage and evade state surveillance. As a former *naqib* (the rank below *munzir*) explained:

> If you are not part of the AI unit, you will not know which platforms they are using. This knowledge is restricted because the leaders want to keep it secret and confidential. Just like they take precautions when it comes to networks and communication, they are worried that the military will know that they are using this technology.[63]

Despite some variation in how strictly these policies were enforced across camps, they were generally followed. VPNs and encryption software provide an additional layer of protection.[64] As a result, AI usage has not been diffused throughout the entire organization. Instead, AI access is concentrated among trained and trusted operators, with the leadership attempting to retain oversight over deployment. Compared with ISWAP, there was more discretion within JAS: "No one shares the whole AI strategy downwards in the hierarchy – like, the *imam* doesn't share everything with the *jaysh*. But at each level, they [commanders] can use AI as they please. There are no restrictions and they don't have to ask for any permission."[65] This reflects JAS's organizational character as a more militaristic, less bureaucratized system in which regional commanders maintain greater autonomy over their strategies, resources, and fighters, with the top leadership exerting comparatively less control (International Crisis Group 2024, 9). This more decentralized approach could accelerate the proliferation of AI use and enable experimentation with dangerous applications without organizational oversight, but may equally limit the development of more advanced AI proficiency and create operational security vulnerabilities going forward.[66]

---

[63] Interview with ISWAP Commander-21, 2026.
[64] Interviews with ISWAP Commander-5, ISWAP Commander-24, 2026. See also, Samuel (2023).
[65] Interview with JAS Commander-3, 2026.
[66] In line with the potential benefits and limitations of (de-)centralized control for AI use, there is no consensus on the effects of organizational structures in the literature on weapons

The specialized units' third main activity is to drive the groups' AI use by generating insights that feed directly into daily operations and strategic planning. "They are not going to expose everything they do, but you can see the outcome," said a former *naqib*.[67] Respondents emphasized that the units continuously generated AI-derived strategies that were then communicated down the hierarchy for implementation.[68] "The team is known for disseminating the strategic and technical guidance," said a former JAS *qaid*, who further differentiated their roles by adding, "we were the commanders who implement, not the commanders in charge of AI."[69] The former ISWAP *munzir* described a similar process, in which his *qaid* — who was originally trained by the "the white guys" to use the chatbots in Arabic — translated the responses from English into Arabic and turned them into written and oral briefings for his subordinates.[70] "He is very knowledgeable in Arabic but prefers asking the questions in English because it gives him more accurate answers," he added.[71]

---

innovation by terrorist groups (Trujillo and Jackson 2006, 60–61; Tishler 2018, 377–78). But when taking ISWAP's and JAS's track record of weaponizing new technologies as an indication for their ability to make use of LLMs, ISWAP may be of greater concern. For example, Boko Haram was first introduced to drones in 2014 when the group seized equipment from the Cameroonian military and, after sending pictures to the IS to inquire about its purpose, received video instructions for assembly and use (Foucher 2020). Thereafter, the group began using drones for surveillance, reconnaissance, and producing propaganda material. However, following the split, the two factions achieved different outcomes. While ISWAP has now successfully launched attack drones carrying grenades (Jamiu 2025), former JAS commanders reported repeated unsuccessful efforts to weaponize drones within their units, citing technical problems such as excessive weight. Identical starting points can thus yield different technological trajectories.

[67] Interview with ISWAP Commander-22, 2026.

[68] Interviews with ISWAP Commander-7, ISWAP Commander-17, ISWAP Commander-21, ISWAP Commander-22, ISWAP Commander-23, JAS Commander-3, 2026.

[69] Interview with JAS Commander-3, 2026.

[70] Interview with ISWAP Commander-7, 2026.

[71] Benchmarking data on language proficiency suggests the gap between English and Arabic is modest, with leading frontier models performing comparably in both languages on reasoning and knowledge tasks, and with only a slight difference in fluent text generation (Pomerenke et al. 2025). Whether Hausa was also used could not be determined, but it would have been a realistic working language considering that leading models score in the 75–90%

Beyond disseminating strategies downward, the specialized units also serve as the primary resource commanders turn to when they encounter challenges they cannot resolve independently. When members face difficulties, they turn to their *qaid* as the first point of contact, who in turn refers upward when they cannot resolve the issue themselves, whether technical problems or matters requiring higher-level judgment. According to an ISWAP *naqib*, "[t]he unit can give you solutions to all kinds of problems. When we have problems we can't solve ourselves, we run to them."[72] The AI unit was approached when "you need help," echoed a JAS *munzir*,[73] as well as another ISWAP *naqib*, who said that "they ask the unit when there is a specific problem, or a very tough event, like when the military attacks us and we need advice. It happens a lot."[74] In other words, "[e]very unit approaches the AI team on their own needs."[75] "We are not allowed to access the computers," said yet another ISWAP *naqib*, "but we present the problem to them to ask the AI. I don't think there is a problem that these people cannot overcome. They are the masters. They do the analysis with the AI and give us the strategies to implement."[76]

This support extends beyond the camp. While AI unit members typically remain at base, they provide assistance to commanders in the field remotely. For example, fighters relay problems they encounter, and the unit queries a model and communicates its guidance back. Such coordination is possible through ISWAP's documented communications infrastructure, including specific vehicles that ISWAP reportedly outfits with satellite internet to enable communication and data sharing on the move (Samuel 2023). In one account, a respondent even described wearing a

---

range on reasoning and knowledge tasks in Hausa, with text generation somewhat less reliable than in English or Arabic (Pomerenke et al. 2025).

[72] Interview with ISWAP Commander-22, 2026.

[73] Interview with JAS Commander-26, 2026.

[74] Interview with ISWAP Commander-21, 2026.

[75] Interview with JAS Commander-27, 2026.

[76] Interview with ISWAP Commander-23, 2026.

chest camera that transmitted footage back to camp, where a commander followed the feed, "uploaded the pictures to ChatGPT to analyze the situation," and relayed tactical adjustments back to the field.[77] On larger engagements or operations that require specific expertise, designated personnel join operations in person with laptops to provide direct support.[78]

The specialized units thus serve as the primary point of AI expertise within the organization, though commanders at the *qaid* level and above retain considerable autonomy over day-to-day usage. When internal knowledge is insufficient, they "consult with the foreigners,"[79] noted one respondent, while another added that "if it [AI] is not helpful, they ask the foreigners and they then advise on how to best use the AI."[80] These findings highlight that, beyond the formal training sessions, the foreign operatives provide ongoing assistance, including guidance on prompting strategies and navigating platform restrictions, such as content filters and account blocks (as discussed in more detail later).

AI Use Cases

AI use within both factions is extensive and appears embedded in day-to-day operations. "Anytime they did not have a clear understanding of something, they would ask the AI,"[81] trying to "get information about religion, tactics, and other things that need to be done."[82] Across respondents' accounts, it became clear that LLMs have become a key resource that has been integrated across domains, rather

[77] Interview with ISWAP Commander-17, 2026.
[78] Interviews with JAS Commander-3, JAS Commander-26, ISWAP Commander-17, ISWAP Commander-21, ISWAP Commander-23, 2026.
[79] Interview with ISWAP Commander-21, 2026.
[80] Interview with ISWAP Fighter-20, 2026.
[81] Interview with ISWAP Fighter-20, 2026.
[82] Interview with ISWAP Commander-22, 2026.

than an occasional tool.[83] Use cases are technical, operational, and strategic, applied at every stage of military activity — in preparation for missions, during operations, and in post-mission analysis.

In practice, group members seem to access the chatbot directly through the standard web interface, which respondents confirmed when shown the process on my laptop during interviews. Whether the specialized units also make use of API access could not be determined from the current sample, given the limited visibility respondents had into such details. As already touched on, the setting in which AI was used varied. In some cases, a group gathered around a laptop while a senior commander prompted and discussed the generated content.[84] In others, specialists worked side-by-side with the tools, consulting the chatbot in direct support of technical work, as in the recounted case of a bombmaker who iteratively refined new device designs with AI, returning to the laptop for troubleshooting when something was not working or needed clarification.[85] In still others, operators prompted independently and passed the resulting strategies or instructions down the hierarchy, which introduced an additional step and friction between query and application. Some commanders also appear to cross-reference responses across multiple AI systems, as one respondent noted: "I just see that they are typing into different systems, but if I had asked whether they were comparing answers, they would have thought that I was spying."[86]

When asked what kind of questions they typically posed, the former ISWAP *munzir* explained:

[83] Interestingly, Nigeria ranks first globally in both AI adoption, at 92% regular use, and trust in AI systems, which far exceeds the U.S. baseline of 53% (Gillespie et al. 2025).
[84] Interview with JAS Commander-3, 2026.
[85] Interview with ISWAP Commander-7, 2026.
[86] Interview with JAS Commander-3, 2026.

> We mostly used it in three ways: the first one is to learn how to assemble and use guns and how to manufacture bombs. The second one is for surveillance, like how to improve our surveillance strategies to monitor what is happening in our camps and also to better understand our enemy and prepare attacks. The third one is to make plans, like, when we come up with new ideas on how to attack, we ask it for tactics on how to make it work in practice to be successful.[87]

Regarding the first usage, both factions seize a significant part of their weaponry, military equipment, and ammunition from the Nigerian military. Struggling to operate some of the loot, ISWAP's leader al-Barnawi stated in a letter to the Islamic State back in 2017: "I am reminded of a funny story when about a year ago, we seized Dragunov rifles as war spoils and we had to make them work so we could use them. We checked many handbooks and specialized videos on this technical issue, but we eventually dropped it in despair after all our attempts failed."[88] This account contrasts with how these situations are handled and resolved today, where "we take all of the equipment back to the camp and the AI unit tells us how to use and shoot with it."[89] According to a former JAS technical specialist: "When we managed to seize a sophisticated weapon, the leaders took it to a room where they typed in the number of the weapon. It [AI] then tells you what model it is, how it will be loaded, used, and serviced."[90] In one recounted instance, when ISWAP fighters were handed out new guns and they did not know how to correctly use them, they approached their *qaid*, who passed on the message to a specialist, who in turn replied, "just ask Grok," which they then did.[91]

---

[87] Interview with ISWAP Commander-7, 2025.
[88] Abu Musab al-Barnawi, untitled letter to the Administration of Remote Provinces, October 10, 2017. In: Hamming (2023, 24).
[89] Interview with ISWAP Commander-21, 2026.
[90] Interview with JAS Technical Specialist-10, 2025.
[91] Interview with ISWAP Commander-7, 2026.

AI also assists with troubleshooting during combat. "It happens all the time during attacks that the guns are jammed and the trigger gets stuck," explained the former ISWAP *munzir*, adding that AI provided both immediate technical fixes by teaching "how to uncouple the gun by washing it with diesel" and tactical guidance, in terms of "how to change the military formation so that fighters with jammed guns move to the back and others take their positions until the problem is solved."[92] While AI has not yet replaced other ways to gain such knowledge, whether through the capturing of military personnel or assistance from other militant groups, it already complements them. AI provides information reliably, without the delays, costs, and security risks of human sources, though not without their own limitations and risks.

LLMs have also been used to innovate on explosive devices, with both factions reporting improvements in design and lethality. According to interviewees, AI-derived advice has enabled the groups to introduce new device types, including pressure-activated improvised explosive devices (IEDs) that require no remote detonation: "You just bring two slippers together and connect both sides with wires. Before, we used fertilizer and bottles, and needed remote control to detonate. But this was completely new. We plant it somewhere and if even a mouse touches it, it goes boom and explodes."[93] Similarly, fighters were taught to construct improvised grenades from everyday materials.[94] "AI taught us about substances we can use to fill a can. Then you add some matches, seal it, and you got a hand bomb."[95] AI has also been used to enhance existing methods, for instance by identifying chemical additives and fertilizer-based compounds that increase explosive yield, as well as

[92] Interview with ISWAP Commander-7, 2025.
[93] Interview with ISWAP Commander-7, 2026.
[94] Interviews with JAS Fighter-25, JAS Commander-26, ISWAP Commander-21, ISWAP Commander-22, 2026.
[95] Interview with JAS Fighter-25, 2026.

fragmentation materials such as metal particles to maximize casualties.[96] For example, "[b]efore, the bomb explosion was not that big, but then they studied it. AI told us what chemicals to put in that made the explosion heavier," said a JAS commander.[97] "They want to increase the explosive material. Depending on the target, they add different chemicals now,"[98] said the former ISWAP war strategist, or they add "particles that make a greater impact,"[99] said another respondent. ISWAP further received guidance on defusing and disassembling unexploded ordnance — bombs dropped during airstrikes that failed to detonate — to recover military-grade explosive inside that is more potent than the group's own improvised compounds and to repurpose the material for constructing new devices.[100] The first time:

> They argued about what to do with the bomb. Some fighters wanted to dig it out, others not. They touched it and it exploded. 40 people died. Now they have new rules. Everyone has to stay far away and only one person digs.[101]

Once unexploded ordnance is recovered, the AI unit's bomb experts study it before beginning the defusal process.[102] Moreover, while ISWAP's ability to build weaponized drones has been documented (Africa Defense Forum 2026b; Jamiu 2025), respondents suggested that AI assistance played a crucial role in the research and development process.[103] For example, it advised on payload weight reduction to stay within the drone's lift capacity, and on the design of explosive release mechanisms.[104]

[96] Interviews with ISWAP Commander-7, ISWAP Commander-21, ISWAP Commander-22, ISWAP Commander-24, JAS Commander-3, JAS Fighter-25, 2026.
[97] Interview with JAS Commander-3, 2026.
[98] Interview with ISWAP Commander-24, 2026.
[99] Interview with JAS Fighter-25, 2026.
[100] Interviews with ISWAP Commander-7, ISWAP Commander-21, ISWAP Commander-22, ISWAP Commander-23, ISWAP Commander-24, 2026.
[101] Interview with ISWAP Commander-21, 2026.
[102] Interview with ISWAP Commander-24, 2026.
[103] Interviews with ISWAP Commander-21, ISWAP Commander-22, ISWAP Commander-24, 2026.
[104] Interviews with ISWAP Commander-21, ISWAP Commander-24, 2026.

Consequently, AI enabled iterative, low-cost experimentation with explosive devices that has yielded considerable success.

Both factions have drawn on LLMs for strategic and tactical improvements in their military operations. "It taught us about guerilla strategies," said a respondent, who gave the example of having learned "to decide on a safe spot for everyone to reconvene when we had to retreat during an attack. Before, everybody tried to find their own way to get back to the camp; you run to the bush; you don't have water; you get captured or die. Now we retreat together."[105] Reflecting a broad integration of AI into day-to-day operational planning, they sought guidance on matters ranging from military training and uniform selection to ambush planning, raiding military bases, detailed attack routes into and out of target towns, and tactics for when ammunition ran low.[106] AI has also informed operational decisions, including the right allocation of fighters: "We used to rely on our traditional methods. We sent 200 fighters because we had a lot of strength, but then 60 got killed. With the help of AI, we learned that it sometimes makes sense to only send 20. We learned more about well-coordinated attacks and deployment of smaller units," said a former ISWAP gunner and later bodyguard to senior leaders.[107] This kind of AI-assisted force optimization represents a shift in how commanders make decisions, moving from experience-based intuition toward data-informed planning.

Another such example concerns tactical adaptations in the field, as illustrated by ISWAP's response to a new counterterrorism measure. When government forces dug defensive trenches around their bases, ISWAP's initial assault failed. The standard tactic — deploying motorcycle-mounted fighters in the first wave — proved ineffective

[105] Interview with ISWAP Commander-17, 2026.
[106] Interviews with ISWAP Commander-17, ISWAP Commander-7, ISWAP Commander-21, ISWAP Commander-22, JAS Fighter-25, JAS Commander-26, 2026.
[107] Interview with ISWAP Fighter-20, 2026.

as riders fell into the trenches. To implement a new approach, commanders consulted AI for guidance on adapting motorcycle jumping techniques seen in a movie to cross the trenches. The former ISWAP *munzir* recounted:

> We saw in a movie how motorcycles can jump over bridges. We used AI to learn how to do this. We gave it information, like what motorcycles we use and the distance we need to jump and so on and it gave us steps on what we have to do. We practiced a lot and kept asking questions. We dug holes and filled them with broken glass and fire to practice. 18 of us died in the process. Eight of us managed to do it. The next time we attacked, we could jump.[108]

While entertainment media is considered *haram* (proscribed by Islamic law) and hence prohibited, war movies and documentaries are an exception. Besides combat footage from other Islamic insurgencies, fighters actively study Western military content for tactical inspiration.[109] "We especially like to watch U.S. war documentaries, like from Afghanistan, to get inspiration and learn new tactics," the *munzir* added.[110] AI then helps translate observed tactics into practice, tailored to the organization's specific equipment and constraints.

AI is also used as a tool for post-mission analysis and organizational learning. Rather than limiting AI use to planning and execution, ISWAP consults LLMs after operations to understand why strategies fail and how to improve. "I saw them using it when we went to war and lost. When they went home, they typed in what strategies they had used and learned why they had failed," observed the former ISWAP bodyguard.[111] One respondent described footage from the media units that

---

[108] Interview with ISWAP Commander-7, 2025. While this may seem extreme, the episode reflects a pattern evident across other interviews, in which the group absorbed heavy casualties during dangerous experimentation and training.
[109] Interview with JAS Commander-3, ISWAP Commander-7, 2025.
[110] Interview with ISWAP Commander-7, 2025.
[111] Interview with ISWAP Fighter-20, 2026.

film operations, alongside fighters' own recordings, being uploaded for analysis, on the basis of which "AI analyzed what went wrong to come up with new strategies."[112]

In addition to enhancing offensive capabilities, AI has been employed to improve operational security. To evade detection, "[i]t can advise you on how to send secret messages"[113] and "communicate with leaders abroad."[114] Beyond encrypted messaging, the former ISWAP bodyguard described how AI units trained communications and media teams on evading detection based on AI-generated recommendations: "When we are going to war, the unit trains the media team. They select like five people or so and tell them how to document the war without being traced. AI guides them on how to take precautionary measures."[115] This includes advice on encrypting and storing footage securely, avoiding internet connectivity until back at base, and disseminating content in ways that conceal their location. "The AI unit brought out guidelines" that changed their practices because, "[b]efore, we had phones in our pockets and just recorded things [during attacks] that could expose us," he added.

In al-Barnawi's 2017 letter to the Islamic State, referenced above, he also states: "When it comes to military affairs, your guidance is required to organize the army, to recruit new fighters, to improve defenses, to learn attack tactics and the making of explosives, for the use of canons, mortars, and howitzers. This is the biggest and the most chaotic sector and we deploy enormous efforts there in vain. It is necessary to send us a framework to help us overcome the big imbalance in our province."[116]

---

[112] Interview with ISWAP Commander-24, 2026. For context, uploading recorded footage for prompt-driven analysis became feasible for non-technical users by mid-2024, when models such as Google Gemini 1.5 Pro introduced native video understanding through a standard browser interface.
[113] Interview with JAS Commander-3, 2026.
[114] Interview with ISWAP Fighter-20, 2026.
[115] Interview with ISWAP Fighter-20, 2026.
[116] Abu Musab al-Barnawi, untitled letter to the Administration of Remote Provinces, October 10, 2017. In: Hamming (2023, 24).

Although ISWAP has since received such guidance and has improved significantly, it is striking that the list covers LLM use cases that interviewees reported. This demonstrates that terrorist groups are already turning to AI to help them overcome technical, tactical, and operational obstacles that they previously struggled to solve on their own, even if the degree of uplift, if any, remains difficult to assess.

The uplift that LLMs provide depends, among other things, on the ability to formulate effective prompts, which is a skill that remains unevenly distributed and partially dependent on foreign assistance. The former ISWAP *munzir* explains this well:

> I went to the *qaid* to type a question about different ways to manufacture bombs. He said he could only get the answer if he knew exactly what the problem was. I told him about how the wires were connected in a way that seemed to prevent the bomb from going off. ChatGPT gave some explanations but they were not very clear. He contacted some people about how to put the question, and then it gave us useful information on how exactly to connect the wires, and it worked. I don't know what he typed that made it work. They call people in the network for this kind of help every day.[117]

This account illustrates the role of precise problem specification for obtaining useful outputs, the iterative nature of prompting, and ongoing reliance on foreign operatives, not just for initial training, but for day-to-day assistance. It also illustrates the gap between those with superior prompt engineering expertise and those without, which the organizational structures described earlier seek to bridge.

Safeguards do not appear to have posed significant obstacles to LLM use. Some respondents acknowledged occasional difficulties in accessing "sensitive information," saying that "there are things you can't get. Some information, it won't give you, like when we wanted all the locations where the Nigerian military stores its

[117] Interview with ISWAP Commander-7, 2026.

weaponry. It knows it but it is not going to tell you."[118] The former JAS commander added: "My boys that have received extensive training [...] then bypass the restrictions. They say they need it for a movie or something like that," while also admitting that "[w]hen you start asking something sensitive, it knows that you want to use the information for something different, and we know that it knows." Others similarly suggested that refusals were not a problem because "the white guys taught us how to bypass restrictions."[119] Most respondents could not speak to jailbreaking techniques but suggested that the group was able to access desired content or received external assistance to do so, based on their experience that senior commanders and AI units were consistently able to provide answers when approached with problems. Beyond content restrictions, respondents also stated that they were not aware of account suspension being an issue. The *munzir* clarified that "they are very careful" that accounts do not get suspended, and in turn, that "the *qaid* is in charge of blocking accounts if it could create a problem for us" from an operational security perspective, by which he probably refers to deleting the account.[120] The JAS *qaid* said that the AI units are responsible for ensuring alternative accounts are accessible if one is suspended.[121] It should be noted, however, that most interviewees' disassociation around 2024 and limited direct exposure to prompting and platform restrictions mean that the effectiveness of jailbreaking techniques and the impact of more recent safeguards cannot be fully assessed from the available data.[122]

[118] Interview with JAS Commander-3, 2026.
[119] Interview with ISWAP Commander-7, 2025.
[120] Interview with ISWAP Commander-7, 2026.
[121] Interview with JAS Commander-3, 2026.
[122] As noted earlier, however, the sample includes one participant who could speak about AI use patterns up to mid-2025.

Attitudes Toward Weapons of Mass Destruction

One of the interviewees was part of Boko Haram's "pioneers," as he put it, who had joined the movement from its very beginning in the mid-2000s, alongside youths who were "tired of oppression and corruption by the elite."[123] He recalled, "We felt like the only way to liberate ourselves is to defend ourselves, and the only way to defend ourselves is to attack." He quoted Karl Marx's "Religion is the opium of the people" to explain how "some of us became convinced that we can do whatever is necessary to achieve our goal. If anyone says, 'This is wrong,' you kill them." He had spent almost 20 years with the group. The interview was conducted in English, and before getting started, he asked for a pen and a piece of paper to take notes. He talked about his experiences with notable clarity and assertiveness:

> Q: Are there any weapons that are prohibited to use for strategic or ideological reasons?
> A: You mean like WMD [weapons of mass destruction]?
>
> Q: For example.
> A: Chemical or biological weapons are allowed. Traditionally, they are prohibited. But they have been legitimized. [...] If you have access to them, you can use them.
>
> Q: Has the use of biological weapons been considered?
> A: Yes.
>
> Q: And you would use them?
> A [responds without hesitation]: Yes, of course.
>
> Q: Why haven't you used them?
> A: They are not easy to get. Unless you can invent or buy them, you waste your time discussing this.
>
> Q: Have you tried to invent or buy them?

[123] Interview with ISWAP Commander-5, 2025.

A [responds firmly]: I don't have anything else to say about this.

While his statement could hardly be more straightforward, the following points provide further context for dynamics surrounding terrorist groups' attitudes toward and pursuit of WMD.

First, attitudes toward WMD are not fixed, but vary among leaders and over time. General characterizations of militant groups embracing or rejecting certain types of violence or targets often brush over more complicated internal power dynamics where the "right" ideological and strategic approach can be an issue of debate, change, and sometimes even schism. For example, the question of who counts as an unbeliever and thus a legitimate target to be killed (*takfir*) was one of the main reasons that led to the split between JAS and ISWAP in the first place (Kassim 2018). These ideological differences continue to exist:

> Some of us are so radical that they are ready to kill everyone; even the entire world. Others think that life is sacred and you have to be more selective. That's why there is disagreement about WMD. Some go strictly by the laws of the Quran. Others would justify anything when they feel pushed against the wall. They want something, and then they rationalize it in religious terms. When Shekau [JAS's former leader] felt pushed into a corner, he would have taken any action; that's what got him killed in the end.[124]

Hence, positions about WMD are not always homogeneous among members of a group, and not even among its top leaders, who may also change policies on violence over time. "Today, this is the rule; tomorrow it may change. It depends on how they translate the Quran into rules. It's up to whoever is in charge," noted a respondent.[125] Al-Qaeda's ideological justifications for pursuing WMD also transitioned over time from self-defense to deterrence to retribution (Santhana Dass 2021, 8). When

[124] Interview with ISWAP Commander-5, 2025.
[125] Interview with JAS Fighter-15, 2025.

assessing intent for large-scale harm, it therefore needs to be taken into account that "in the past decade, several jihadist groups have overturned their interpretations of the rules, embraced tabooed forms of violence, and even celebrated abuses that they once considered forbidden, and even shameful" (Ahmad 2019, 81).

Second, interpretations of prohibitions on weapons are not uniform within groups and may vary by rank and ideological knowledge. When asked about any prohibited weapons, many interviewees named "poison." The most common explanation for why it was prohibited was the indiscriminate harm it causes, including among "the innocent who support our ideology."[126] Respondents emphasized that the transmission of poisonous agents via water or air was prohibited, that they understood it to be against the Quran, and that the rule's enforcement was strict. "It is a general rule of engagement. You would get killed right away if you did this."[127] One interviewee recounted an incident where a JAS commander suggested poisoning ISWAP's water supply. "When his superiors heard about it, they called for a meeting and told him that we don't play around with such weapons," he said, "and then they killed him."[128] What seemed like a ban, however, was qualified by "the pioneer":

> You have to understand that when we talk about poison, we are not talking about weapons. Poison is traditionally not considered a weapon. That means that if you weaponize it, you can use it, like when you put it in bullets or on arrows. That's why biological or chemical weapons are allowed to be used; they are modernized versions of poison. And anyway, if your enemy uses something that is forbidden, you are allowed to use it, too.[129]

[126] Interview with JAS Fighter-11, 2025.
[127] Interview with ISWAP Commander-7, 2025.
[128] Interview with JAS Fighter-11, 2025.
[129] Interview with ISWAP Commander-5, 2025.

The last part is in line with retribution as a justification for WMD on which al-Qaeda and ISIS operatives have drawn, especially the *fatwa* entitled "A Treatise on the Legal Status of Using Weapons of Mass Destruction Against Infidels," issued by Saudi cleric Sheikh Nasser bin Hamad al-Fahd in May 2003. The diverging statements from respondents about the prohibition of poison may be due to different levels of ideological proficiency, as well as different information access corresponding to rank. The organization may deliberately communicate and enforce a strict prohibition to prevent any experimentation and deployment that has not been authorized by the leadership. Concerns over insider threats and external attacks using chemical or biological agents are further evidenced by the reported strict monitoring of the water supply, with anyone approaching it at night getting "in trouble."[130]

Third, observed weapon preferences should not be mistaken for ideological red lines. Some interviewees differentiated poison from "powders," which they argued were allowed due to their more precise targeting:

> We can use powder to target a particular group. We once seized some from the military and used it against them during an attack. A few soldiers suffocated and died. We have tried to get powder of the same quality, but couldn't find it. Our *munzir* had some experience with powders and brought in foreigners to teach us.[131]

One respondent claimed that a foreign operative, guided by AI, instructed members on how to manufacture ammunition laced with a chemical that, once a target is shot, causes "bleeding from nose and eyes," which was a weapon whose use was restricted to senior commanders.[132] The Islamic State has also experimented with chemical weapons, rather than investing in biological or nuclear programs. Despite sharing

[130] Interview with ISWAP Commander-7, 2025.
[131] Interview with JAS Technical Specialist-10, 2025.
[132] Interview with ISWAP Commander-7, 2026.

al-Qaeda's stance on WMD, the group prioritized developing weapons for battlefield use and was the first non-state armed group that developed a banned chemical warfare agent and combined it with a projectile delivery system (UNITAD 2023). Even Abu Khabab, who led one of al-Qaeda's training camps for biological and chemical weapons, supported the development and use of chemical weapons, but found nuclear and biological weapons a "waste of time" (Dean et al. 2018, 105). This comment echoes the statement above regarding discussions about the pursuit of biological weapons being a waste of time "unless you can invent or buy them." Decisions about what CBRN capabilities to pursue are thus not necessarily based on ideological distinctions but are influenced by strategic considerations, including feasibility. Individual leadership preferences also matter (Tishler 2018). For example, Osama bin Laden was particularly interested in the pursuit of chemical and nuclear weapons, while his successor Ayman al-Zawahiri, who had a scientific educational background in medicine, emphasized the biological weapons program and initiated al-Qaeda's anthrax development in 1999 (Pita and Gunaratna 2009). This flexibility in weapon selection suggests that groups may shift priorities rather than being bound to certain weapon types for ideological reasons alone. Risk assessments that extrapolate from past weapon usage patterns may therefore underestimate groups' willingness to switch weapon types or expand their repertoire. AI could be especially useful here, providing the technical information needed to evaluate the feasibility of adopting new weapons.

In summary, though there are considerable internal disagreements, neither faction of Boko Haram maintains a clear or consistent rejection of WMD. In addition, respondents from both factions emphasized their global ambitions with a willingness to "attack anywhere in the world"[133] if given the opportunity. While there is no evidence that ISWAP or JAS have WMD programs, the combination of ideological

[133] Interview with ISWAP Commander-7, 2025.

flexibility, rudimentary attempts with chemical weapons, and a global agenda could create a permissive environment for serious AI-enabled CBRN experimentation that should be considered when assessing which actors might have the intent to leverage AI for that purpose.

Uplift & Optimism

Respondents' overall assessment of AI was consistently positive, with some noting that AI "is working well"[134] and that "it has helped them a lot."[135] Even if exaggerated, the perception that "there is nothing we haven't received an answer on; we believe it knows everything,"[136] illustrates the degree to which AI has become a trusted resource within Boko Haram, and the extent to which confidence in its capabilities may outpace the benefits it actually provides.[137] Although both factions have used the internet extensively, participants noted that LLMs offer advantages over traditional internet searches through structured, step-by-step guidance. "The steps it gave us to solve problems were so helpful," one interviewee said.[138] Respondents also highlighted that "before AI, everybody used traditional thinking and asked people randomly, but with AI you can get different strategies and then you can decide which one to use."[139] This echoed what the former ISWAP war strategist said: "I have my own traditional methods, but AI comes up with modified versions."[140]

---

[134] Interview with ISWAP Commander-21, 2026.
[135] Interviews with ISWAP Commander-17, ISWAP Commander-22, 2026.
[136] Interview with ISWAP Commander-7, 2026.
[137] Some studies find that users significantly overestimate AI-derived gains, believing AI accelerated their work even when it objectively did not (Becker et al. 2025), whereas others find that extended LLM use was associated with reduced confidence in task performance relative to baseline (Hong et al. 2026, 23), casting doubt on the reliability of self-reported efficiency gains.
[138] Interview with ISWAP Commander-7, 2025.
[139] Interview with ISWAP Commander-22, 2026.
[140] Interview with ISWAP Commander-24, 2026.

Beyond specific use cases, members pointed to broader efficiency gains. For example, AI was credited with having led to "a lot of innovation in a short time" within the group.[141] It was also credited with reducing casualties, such as during weapons development. "Trial and error can kill you. AI gives you accuracy," noted one respondent, recounting how one of his fighters was pierced by shrapnel when attempting to cut open a bullet and how such incidents were reduced thanks to AI.[142] This resonated with the description of another commander, who explained that "[s]o many times, the [AI] unit said, 'No, don't do that!'" and how such warnings "reduced fatalities during trial and error."[143] These accounts suggest that AI is at least perceived as having meaningfully improved insurgent activities both behind and on the front line.

This enthusiasm was not entirely uncritical, however, with respondents acknowledging AI's and their own limitations. When asked for any problems they have had with AI, one respondent noted that "sometimes it is not accurate."[144] Another explained that "we don't just believe whatever it tells us, but we test it."[145] Respondents also acknowledged that AI does not always provide the answers they need. "It helps us with technical strategies, but we still use our brain if the AI can't help,"[146] said one, while a JAS commander put it more bluntly: "If you don't get what you need from AI, we use our brain to supplement."[147] Aside from the recognition of restrictions, it is equally revealing how respondents framed the relationship between AI and their own cognitive abilities. That human judgment is positioned as the fallback rather than the default speaks to the degree of reliance and trust these

[141] Interview with ISWAP Commander-7, 2026.
[142] Interview with JAS Commander-3, 2026.
[143] Interview with ISWAP Commander-21, 2026.
[144] Interview with ISWAP Commander-17, 2026.
[145] Interview with ISWAP Commander-7, 2026.
[146] Interview with ISWAP Commander-24, 2026.
[147] Interview with JAS Commander-3, 2026.

groups have placed in AI systems. The JAS commander further reflected on the source of these limitations, saying, "Sometimes, we think it can't help us. It has limitations. But maybe we are just not technical enough to use it deeper. This is our limitation."[148]

Despite respondents' assurances that they had "no experience of something going horribly wrong"[149] with AI, regular weapons experimentation continued to carry human costs, and in some cases AI guidance itself contributed to them: "Sometimes the [AI] unit would experiment and people died. New people then joined."[150] Whether these deaths resulted from flawed AI recommendations or incorrect implementation remains unclear. Casualties during experimentation are a normal feature of insurgent activity, and participants consistently perceived AI as having reduced their overall frequency, suggesting that these costs should be noted but not overstated as a counterweight to the generally positive picture that emerges from participant accounts.

Members displayed uneven awareness of and concern about the risks of being monitored and tracked through their use of AI and other technologies. As discussed earlier, both factions have put in place measures to mitigate surveillance risks. These concerns were most pronounced in the context of operations and external communications, where the risk of exposure is highest.[151] Within their military strongholds, however, a markedly more relaxed attitude prevailed, with a former JAS *qaid* capturing a frequently voiced sentiment when saying, "we have bombs everywhere in the area, so let them come."[152] The former ISWAP *munzir* said that

[148] Interview with JAS Commander-3, 2026.
[149] Interview with ISWAP Commander-7, 2026.
[150] Interview with ISWAP Commander-21, 2026.
[151] Interviews with ISWAP Commander-5, ISWAP Commander-7, JAS Commander-3, ISWAP Commander-24, JAS Commander-26, 2026.
[152] Interview with JAS Commander-3, 2026.

"no matter what they know, they are afraid to come to us."[153] Awareness of surveillance risks among senior leadership and technical personnel is likely to be considerably higher, as suggested by the notably greater preoccupation with operational security among the more high-ranking and technically sophisticated respondents in the sample. According to the pioneer, "the digital war is not easy to escape," but "what gives us confidence is that they might get information that can be used against us, but it is still difficult for them to come to the bush."[154] These concerns thus do not appear to have deterred AI adoption, although this confidence may underestimate the extent to which digital surveillance can enable targeted operations even in remote strongholds.

This approach toward AI needs to be viewed in the context of an organizational culture characterized by high confidence in the groups' own technical problem-solving abilities. That "they always come up with new strategies and ways to attack, shoot, and bomb"[155] was an often-expressed observation among interviewees. The former JAS *qaid* emphasized the role of members' creativity that enabled innovation: "They were skillful in developing new strategies. I myself was creative and came up with new ideas. Even as we sit here now, I could think about different ways to make use of this glass," he said,[156] pointing at a glass on the table. This confidence manifested as a problem-solving mindset in which technical constraints were treated as temporary and surmountable. To stay ahead of a more powerful state military as a resource-constrained insurgency, they had to change course "whenever the military started to understand [their] strategy,"[157] he said, and make use of materials and tools at their disposal. Regarding the latter, another

[153] Interview with ISWAP Commander-7, 2026.
[154] Interview with ISWAP Commander-5, 2026.
[155] Interview with JAS Commander-2, 2025.
[156] Interview with JAS Commander-3, 2025.
[157] Interview with JAS Commander-3, 2025.

respondent stated that "many things were invented locally. Just with a small plastic bottle, you can build something so destructive. People are coming up with lots of ideas. If we couldn't go for advanced weapons, we went for local solutions. When someone has to defend themselves, they use anything they can find, you know. They have local laboratories to experiment with explosives and so on."[158] "Many die in the process," said a former explosives expert whose sister got killed and who himself got severely burned experimenting, "but that means that whatever we are trying is working!"[159]

With regard to expertise as a requirement for innovation, Ackerman (2016, 24) notes that "the literature suggests that VNSAs [violent non-state armed groups] do not necessarily require members with outstanding technical expertise, but instead a membership that is stable, proficient in analyzing existing methods and resources, and can reconfigure these to meet an organization's goals." This resonates with the impression a former JAS commander gave when asked about moments in which his unit lacked technical expertise:

> People are skillful and learn how to do things, even someone who never went to school, like small children; we teach them how to fix a phone, a TV, or how to make ammunition. When we found a vehicle and didn't know how to use it, we climbed in and figured it out. When we detected a drone from the Cameroonian military, we shot it down, studied it, fixed it, and started to use it. We then learned how to manufacture them locally [i.e., to reassemble drones using repurposed parts from other electronics]. There was one time when we had trouble fixing the chain of an armored tank, but we managed to figure it out with the internet. Whatever we needed, we figured it out.[160]

[158] Interview with ISWAP Commander-5, 2025.
[159] Interview with JAS Technical Specialist-10, 2025.
[160] Interview with JAS Commander-3, 2025.

Expressing a similar attitude, a former ISWAP commander explained: "We had people who shoot down aircraft or who defuse bombs. We had people with all kinds of skills. If there was something we couldn't do, we learned how to do it."[161] While these examples involve relatively basic technical skills, they reveal a culture of learning and innovation paired with high confidence that shapes how members approach new technologies. This self-perception was so pronounced that eliciting accounts of challenges the group faced required repeated probing. When asked about difficulties, interviewees' initial responses were typically that there were none. Only through rephrasing questions did acknowledgments of constraints emerge, primarily in the fighting between JAS and ISWAP rather than with the Nigerian security forces, along with shortages of medication.

Group members' belief in their ability to solve technical problems may lower psychological barriers to query LLMs about high-risk capabilities and to pursue ambitious goals. In some instances, technological aspirations were discussed alongside limitations:

> We wanted to move in the fastest lane. We tried to see how we could catch up technologically, but our level of exposure was not that high. Sophisticated tech was a major problem. We needed experts, but where do you find people with this kind of knowledge here? Like, we wanted to use drones for surveillance and attacks but we couldn't get the right people. We needed technical experts who have long operated in war zones, like from the Sahara, Algeria, Iran, or Somalia, but trans-border travel is risky. It is a problem to get them in and out of the country. [...] We used the internet a lot, but it was not enough. We were aware of AI but couldn't get someone with the right skills who could teach us. People were eager to use it.[162]

[161] Interview with ISWAP Commander-7, 2025.
[162] Interview with ISWAP Commander-5, 2025.

As shown earlier, some of these constraints have since been overcome, with ISWAP having obtained in-person training to both weaponize drones and use LLMs. Those who had engaged with AI while active in the group recognized its potential and described a sense of excitement and optimism among members. In the words of the former ISWAP *munzir*, "God has helped us, and so will AI."[163]

[163] Interview with ISWAP Commander-7, 2025.

OBSERVATIONS & IMPLICATIONS

This research establishes that AI misuse by terrorist groups is no longer a prospective threat but one that has already materialized, unfolding more systematically and across a wider range of operational domains than existing analyses have suggested. Several observations and implications emerge:

Terrorist groups have already adopted AI, making it a current national security problem. Risk assessments, red-teaming studies, and expert predictions have focused on what LLMs could enable malicious actors to do. This study complements those approaches by demonstrating how terrorist organizations have already been using AI. Within roughly two years of ChatGPT's public release, both factions of Boko Haram moved from initial exposure to establishing dedicated AI units, internal training programs, and routine operational deployment. That this occurred in resource-constrained groups operating under sustained military pressure underscores that the barriers to adoption are lower than often presumed, and that adoption is unlikely to be the primary constraint on terrorist use of AI. If current and future models provide meaningful uplift, at least some militant groups are willing and already positioned to exploit AI. Thus, the window between a model becoming more capable and an adversary operationalizing that capability may be relatively short.

The use cases extend well beyond propaganda into the operational core of insurgent warfare. Existing empirical work has focused predominantly on online propaganda and recruitment content produced by jihadist sympathizers and unofficial media outlets. This study reveals a qualitatively different picture. Both factions studied here have employed LLMs for weapons troubleshooting, design of explosive devices, tactical and strategic planning, battlefield adaptation, and operational security, among other purposes. AI has been consulted at every stage of

military activity — in mission preparation, during operations, and in post-mission analysis. This shifts the primary concern from information warfare to kinetic operations, where AI-derived guidance informs the planning and execution of political violence.

AI has diffused within transnational jihadist networks through systematic knowledge transfer. The implications of this research therefore reach beyond the documented case. Use did not emerge from individual experimentation but through top-down, externally facilitated diffusion. Islamic State-linked operatives delivered in-person training to ISWAP, supplying laptops with VPNs and encryption software along with follow-up assistance, while other networks trained JAS. This diffusion pathway mirrors how the Islamic State has historically transferred other capabilities through its network. Given its architecture of interconnected global provinces (*wilayas*), with established mechanisms for sharing information and resources, similar AI training is likely to have reached affiliates elsewhere. Viewing AI adoption by a single province in isolation therefore risks substantially underestimating the scale of uptake across the wider network. Moreover, once trained, groups gain greater operational autonomy. LLMs supply the technical and tactical information that once required an external expert, reducing reliance on periodic visits that could be delayed, denied, or interdicted. Therefore, a single training intervention can have compounding effects as groups continue to develop capabilities independently.

Terrorist organizations have institutionalized AI. Moving beyond ad hoc experimentation, both Boko Haram factions have established organizational structures for AI use. These include dedicated units staffed by personnel from specialized operational roles, managed accounts and premium subscriptions, internal training cascades that transmit knowledge down the command hierarchy, and access policies that restrict use to mid- and senior-level leadership. This infrastructure means that AI fluency does not lie with any single individual but is embedded in

organizational processes, making it more resilient to personnel attrition and harder to disrupt.

For a resource-constrained group, the level of investment in training and personnel signals that leadership views AI as strategically important. The form the internal structures take varies, however, with ISWAP's more centralized model concentrating expertise under close leadership oversight, whereas JAS's greater commander autonomy enables faster proliferation with less coordination. These organizational differences mean the same technology can produce distinct risk profiles across groups, which is a dimension that current threat assessments should take into consideration.

Safeguards have not prevented misuse by organized adversaries. Respondents consistently described content restrictions as surmountable rather than prohibitive. Jailbreaking techniques taught by foreign operatives, combined with ongoing prompt-engineering assistance, enabled both factions to access harmful content across multiple platforms. Some of what these groups use AI for — drafting communications, processing information, planning logistics — is indistinguishable from legitimate activity, and obtaining help with them is not a safeguard failure. But some of the evidence falls into a category that safeguards should block, such as attack planning and design of explosive devices. That respondents talked about restrictions as inconveniences rather than barriers suggests safety architectures at the time were insufficient against this kind of adversary, though more research is needed on the specific techniques used and their effectiveness against updated safeguards.

Analysis of online content alone yields an incomplete picture of terrorist adoption of AI. Analysts drawing on online propaganda previously observed a relatively slow rate of adoption and concluded that official jihadist uptake was not yet proved as widespread as might be expected. This study finds otherwise. The divergence is not incidental considering that many AI applications, such as for weapons design,

tactical planning, or operational security, are precisely those that groups have the strongest incentives to conceal. Ideological disputes among online supporters over whether AI-generated content violates Islamic law may further suppress public acknowledgment. Conclusions drawn primarily from online chats and propaganda materials therefore risk systematic underestimation. Studying what happens inside clandestine organizations is inherently difficult, but the gap between what is visible and what is hidden is precisely why open-source analysis must be complemented by other forms of data.

Attitudes toward AI may accelerate future risk. Respondents described AI as highly useful, crediting it with accelerating innovation and weapons development, reducing casualties, and providing structured problem-solving guidance that surpassed traditional internet searches. That they frame human expertise as a fallback rather than the default reveals the extent to which AI has become a trusted and relied-upon resource. Even where the actual magnitude of uplift remains uncertain, enthusiasm and continued investment suggest these groups will deepen their engagement as models improve. Such perception-driven momentum may matter in its own right, as groups that are convinced that AI can solve their technical challenges are more likely to attempt ambitious applications, including in domains where they currently lack expertise.

Neither faction studied here categorically rejects weapons of mass destruction, which raises concerns about potential AI-enabled CBRN pursuit. The study finds no evidence of AI-assisted CBRN programs, and the findings should not be read as suggesting imminent acquisition. But several elements warrant attention in combination. Feasibility is a significant constraint, alongside others including ideological debates, strategic concerns, and operational priorities, yet neither faction maintains a clear categorical prohibition on chemical or biological weapons, and a few commanders expressed willingness to at least acquire them, if they could. A

small number of respondents also described some experimentation with chemical agents, though these accounts could not be independently verified and should be interpreted with caution. Both factions, meanwhile, consistently turn to AI to overcome technical obstacles they cannot resolve on their own. Respondents did not explicitly link AI to high-risk CBRN development, but the combination of intent to cause large-scale harm, capability gaps, and demonstrated reliance on AI for bridging such gaps is concerning. The fact that Boko Haram's primary focus on conventional political objectives did not preclude interest in chemical or biological weapons also suggests that risk frameworks treating omnicidal or eschatological ideology as a precondition for WMD interest may overlook significant threats. Chemical weapons appear to be the more likely near-term pursuit, especially given Islamic State precedent and the comparatively low technical barriers.

These findings have relevance beyond the case of Boko Haram. The group commands no unusual resources or technical sophistication, and although a transnational network shaped and accelerated its AI adoption, such a network is a route to what is documented here, not a requirement for it. The tools are publicly available, and a motivated group could plausibly reach comparable or more advanced uses on its own. The vulnerability lies less in any particular actor than in the combination of accessible models, surmountable safeguards, and a diffusion environment that links many comparable groups. That is why a single, well-evidenced case is sufficient evidence of the serious security risk of AI adoption.

Significant uncertainties remain about the scope, sophistication, and implications of terrorist adoption of AI. Several limitations constrain the findings of this study. First, interviewees were mostly low- to mid-level commanders rather than top leadership, so high-level decision-making about AI and the most sensitive applications may not be captured. Second, participants reported on activities during their active membership, which ended at least several months before the interviews,

so current usage patterns are likely to have evolved. Third, both AI capabilities and safety measures have advanced since, raising the question of whether the misuse described here remains possible with current models. Fourth, the extent to which LLMs have provided uplift relative to traditional internet searches or other sources cannot be conclusively determined from qualitative accounts alone.

To be clear, the findings do not demonstrate that AI enables terrorist groups to accomplish objectives that were previously not possible, nor do they determine the exact threat level posed by AI-enabled terrorism. However, they show that AI uptake occurred across more domains and more systematically than prior assessments have suggested; that existing safeguards at the time proved insufficient to prevent misuse from which terrorist organizations at least subjectively benefitted; and that terrorist groups are optimistic about AI and their own ability to leverage it for their purposes in the future.

More evidence on AI-enabled terrorism is needed. These findings open several lines of inquiry that warrant attention across disciplinary boundaries. First, the scope and character of AI diffusion within militant networks remains poorly understood. This study documents adoption by two factions with links to the Islamic State and broader jihadist networks, but whether and how similar training has reached other ISIS provinces, al-Qaeda affiliates, and non-jihadist armed groups is unknown. Comparative research across organizations, regions, and ideological orientations is needed.

Second, safety testing may be missing where gains are currently concentrated. Existing studies are largely organized around CBRN and cyber capabilities with the potential for catastrophic harm. Yet the respondents in this study derived substantial value from applications that fall below that threshold but are far from benign and enhance operational capacity in ways that compound across an organization. A

research agenda calibrated only to the most catastrophic use cases risks missing the steps that may precede them. As Hersman and Nelson (2026) aptly put it, "[w]e are in danger of creating a safety system that fixates on guarding against the next pandemic while leaving the door wide open to other forms of terror."

Third, understanding which AI capabilities translate into actual risk depends on knowing how armed groups make decisions, adopt technologies, select weapons, and respond to constraints. These are empirical questions about the drivers and dynamics of political violence that are the terrain of conflict and terrorism research, which could make important contributions to AI threat assessments. But they require conflict scholars to engage with the potential and risks of AI and how it may alter the behavior of militant groups. Capability evaluations alone cannot determine whether and under what conditions groups interested in large-scale harm would attempt to leverage AI for it.

Finally, the risk cannot be adequately understood and addressed by any single actor. While AI companies hold information about their systems' capabilities and how they are queried, governments hold classified operational details about threat actors, and academics bring knowledge of how militant organizations function. Building the partnerships needed to integrate these types of evidence is a precondition for any serious response to the present and growing risk of AI-enabled terrorism.

ACKNOWLEDGEMENTS

My deepest thanks go to the interviewees who shared their stories, experiences, and knowledge with me; this research would not have been possible without their willingness to speak with me. I am profoundly indebted to my research assistant, who must remain anonymous, and who not only contributed countless hours of logistical support, translation, and interpretation, but also kept me in good company. I am very grateful to Gary Ackerman, Vincent Foucher, and Alan Z. Rozenshtein for their constructive feedback as peer reviewers. Many thanks also to Markus Anderljung, Forrest W. Crawford, and Cassidy Nelson for their thoughtful comments and support, and to the many others who provided insights and guidance. A special thanks goes to Christoph Winter for his help and encouragement throughout this process. I would like to thank Harvard University and the University of Cambridge for their institutional support, and ERA and Coefficient Giving for their funding and assistance. Any errors are my own.

REFERENCES

Abubakar, Dauda. 2017. "From Sectarianism to Terrorism in Northern Nigeria: A Closer Look at Boko Haram." In *Violent Non-State Actors in Africa: Terrorists, Rebels and Warlords*, edited by Caroline Varin and Dauda Abubakar. Springer International Publishing.

Ackerman, Gary A. 2016. "'Designing Danger': Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue." *Journal of Strategic Security* 9 (1): 1–11.

Ackerman, Gary A. 2023. "The Emerging Terrorist Technological Landscape." In *Routledge Handbook of Transnational Terrorism*, 1st ed., by Nicolas Stockhammer. Routledge. https://doi.org/10.4324/9781003326373-11.

Adebayo, Taiwo. 2025. "Borno Model's Valuable Lessons on Handling Boko Haram Deserters." ISS Africa, October 1. https://issafrica.org/iss-today/borno-model-s-valuable-lessons-on-handling-boko-haram-deserters.

Africa Defense Forum. 2026a. "Boko Haram and ISWAP Fight For Control of Sambisa Forest." *ADF Magazine*, May 19. https://adf-magazine.com/2026/05/boko-haram-and-iswap-fight-for-control-of-sambisa-forest/.

Africa Defense Forum. 2026b. "ISWAP Turns to Armed Drones." *ADF Magazine*, February 3. https://adf-magazine.com/2026/02/iswap-turns-to-armed-drones/.

Ahmad, Aisha. 2019. "'We Have Captured Your Women': Explaining Jihadist Norm Change." *International Security* 44 (1): 80–116. https://doi.org/10.1162/isec_a_00350.

AI Incident Database. 2026. "The MIT AI Risk Repository." https://incidentdatabase.ai/taxonomies/mit/.

AIxBio Global Forum. 2025. "Statement on Biosecurity Risks at the Convergence of AI and the Life Sciences." July 17.

Alakoc, Burcu Pinar. 2017. "Competing to Kill: Terrorist Organizations Versus Lone Wolf Terrorists." *Terrorism and Political Violence* 29 (3): 509–32. https://doi.org/10.1080/09546553.2015.1050489.

al-Lami, Mina, and Steven Humphrys, guests. 2025. *Jihadists and AI*. The Global Jigsaw, BBC World Service. November 2. 12:32. https://www.bbc.co.uk/programmes/w3ct7yvf.

Anthropic. 2025a. *Activating AI Safety Level 3 Protections*. May 22. https://www.anthropic.com/news/activating-asl3-protections.

Anthropic. 2025b. *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign*. https://www.anthropic.com/news/disrupting-AI-espionage.

Anthropic. 2025c. *Threat Intelligence Report: August 2025*. Anthropic.

Anthropic. 2026. *System Card: Claude Mythos Preview*. https://www.anthropic.com/claude-mythos-preview-system-card.

Bacon, Auzinea. 2025. "The New Orleans attacker wore Meta glasses. What can they be used for?" *CNN*, January 6. https://www.cnn.com/2025/01/06/tech/meta-glasses-new-orleans-attack.

Bacon, Tricia, and Jason Warner. 2021. "Twenty Years after 9/11: The Threat in Africa the New Epicenter of Global Jihadi Terror." *CTC Sentinel* 14 (7): 76–90.
Baele, Stephane J., Elahe Naserian, and Gabriel Katz. 2025. "Is AI-Generated Extremism Credible? Experimental Evidence from an Expert Survey." *Terrorism and Political Violence* 37 (8): 1060–76. https://doi.org/10.1080/09546553.2024.2380089.
Barrett, Steve, Malcolm Murray, Otter Quarks, et al. 2025. "Toward Quantitative Modeling of Cybersecurity Risks Due to AI Misuse." *arXiv*, ahead of print, December 11. https://doi.org/10.48550/arXiv.2512.08864.
BBC News. 2026. "Family of child injured in Canada school shooting sues OpenAI" March 10. https://www.bbc.co.uk/news/articles/c309y25prnlo.
Becker, Joel, Nate Rush, Elizabeth Barnes, and David Rein. 2025. "Measuring the Impact of Early-2025 AI on Experienced Open-Source Developer Productivity." *arXiv*, ahead of print, July 25. https://doi.org/10.48550/arXiv.2507.09089.
Boycott-Owen, Mason. 2026. "ISIS Teaching Recruits How to Use AI 'Responsibly.'" *POLITICO*, February 23. https://www.politico.eu/article/isis-teaching-recruits-how-to-use-ai-responsibly/.
Broekaert, Clara, and Colin P. Clarke. 2026. "The Pandemonium Narrative and Its Limits: Artificial Intelligence and the Islamic State's Innovation Pattern." *Hudson Institute*, May 11. https://www.hudson.org/terrorism/pandemonium-narrative-its-limits-artificial-intelligence-islamic-states-innovation-clara-broekaret-colin-p-clarke.
Brounéus, Karen. 2011. "In-Depth Interviewing: The Process, Skill and Ethics of Interviews in Peace Research." In *Understanding Peace Research: Methods and Challenges*, edited by Kristine Hoglund and Magnus Oberg. Taylor & Francis Group.
Brundage, Miles, Shahar Avin, Jack Clark, et al. 2018. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Apollo - University of Cambridge Repository. https://doi.org/10.17863/CAM.22520.
Bukarti, Bulama. 2022. "It's a Bit Tricky: Exploring ISIS's Ties with Boko Haram." *Program on Extremism* (Washington, D.C.).
Catalini, Mike. 2025. "Man Who Exploded Tesla Cybertruck Outside Trump Hotel in Las Vegas Used Generative AI, Police Say." *AP News*, January 7. https://apnews.com/article/tesla-cybertruck-explosion-trump-hotel-las-vegas-248b41d87287170aa7b68d27581fdb4d.
Cheng, Christine, and Christopher Day. 2024. "Research Ethics and the Study of Armed Actors: Process vs. Practice." *Conflict, Security & Development* 24 (6): 501–23. https://doi.org/10.1080/14678802.2024.2436546.
Comolli, Virginia. 2015. *Boko Haram: Nigeria's Islamist Insurgency*. Hurst Publishers.
Council on Foreign Relations. 2023. *Nigeria Security Tracker*. July 1. https://www.cfr.org/nigeria/nigeria-security-tracker/p29483.
Criezis, Meili. 2024. "AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI." *Global Network on Extremism & Technology*, February 5. https://gnet-research.org/2024/02/05/ai-caliphate-pro-islamic-state-propaganda-and-generative-ai/.

Dance, Gabriel J. X. 2026. "A.I. Bots Told Scientists How to Make Biological Weapons." *The New York Times*, April 29. https://www.nytimes.com/2026/04/29/us/ai-chatbots-biological-weapons.html.

Davies, Xander, Giorgi Giglemiani, Edmund Lau, Eric Winsor, Geoffrey Irving, and Yarin Gal. 2026. *Boundary Point Jailbreaking: A New Way to Break the Strongest AI Defences*. UK AI Security Institute.

Dean, Aimen, Paul Cruickshank, and Tim Lister. 2018. *Nine Lives*. Oneworld Publications Ltd.

Epoch AI. 2026. "Epoch Capabilities Index." https://epoch.ai/benchmarks/eci?view=graph&tab=release-date&subset-view=graph&subset-tab=Software+engineering.

Faleg, Giovanni, and Katariina Mustasilta. 2021. *Salafi Jihadism in Africa: A Winning Strategy*. Conflict Series Brief 12. European Union Institute for Security Studies. https://data.europa.eu/doi/10.2815/548.

Firdous, Iftikhar. 2024. "ISKP Begins Publishing Pashto News Bulletins Using Artificial Intelligence." Article. *The Khorasan Diary*, May 21. https://thekhorasandiary.com/en/2024/05/21/iskp-begins-publishing-pashto-news-bulletins-using-artificial-intelligence.

Foucher, Vincent. 2020. *The Islamic State Franchises in Africa: Lessons from Lake Chad*. Commentary. International Crisis Group.

Foucher, Vincent. 2024. *Boko Haram: Mapping an Evolving Armed Constellation*. MEAC, UNIDIR.

Fujii, Lee Ann. 2010. "Shades of Truth and Lies: Interpreting Testimonies of War and Violence." *Journal of Peace Research* 47 (2): 231–41. https://doi.org/10.1177/0022343309353097.

Fujii, Lee Ann. 2012. "Research Ethics 101: Dilemmas and Responsibilities." *PS: Political Science & Politics* 45 (4): 717–23. https://doi.org/10.1017/S1049096512000819.

Garofalo, Daniele. 2024. "A Year of Islamic State Terrorist Attacks. Analysis and Translation of the Al-Naba Newspaper Infographic for the Year 1446." December 14. https://www.danielegarofalomonitoring.com/p/a-year-of-islamic-state-terrorist-c54.

Gillespie, Nicole, Steven Lockey, Tabi Ward, Alexandria Macdade, and Gerard Hassed. 2025. *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025*. The University of Melbourne and KPMG.

Google Threat Intelligence Group. 2025a. *Adversarial Misuse of Generative AI*. Google. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai.

Google Threat Intelligence Group. 2025b. *GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools*. Google. https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools.

Götting, Jasper, Pedro Medeiros, Jon G. Sanders, et al. 2025. "Virology Capabilities Test (VCT): A Multimodal Virology Q&A Benchmark." *arXiv*, ahead of print, April 29. https://doi.org/10.48550/arXiv.2504.16137.

Gustavsson, Andreas, and Viktor Asp. 2025. "Police Source Confirms to Dagens ETC: 'It Is the Suspect's Manifesto.'" Utrikes. *Dagens ETC*, May 20.

https://www.etc.se/utrikes/poliskaella-bekraeftar-till-dagens-etc-det-aer-den-misstaenktes-manifest.
Halstead, John, and Luca Righetti. 2025. *Assessing The Risk Of AI-Enabled Computer Worms*. Centre for the Governance of AI. https://www.governance.ai/research-paper/assessing-the-risk-of-ai-enabled-computer-worms.
Hamming, Tore R. 2023. "The General Directorate of Provinces: Managing the Islamic State's Global Network." *CTC Sentinel* 16 (7): 20–29.
Hansen, Stig Jarle. 2022. "'Forever Wars'? Patterns of Diffusion and Consolidation of Jihadism in Africa." *Small Wars & Insurgencies* 33 (3): 409–36. https://doi.org/10.1080/09592318.2021.1959130.
Helbardt, Sascha, Dagmar Hellmann-Rajanayagam, and Rüdiger Korff. 2010. "War's Dark Glamour: Ethics of Research in War and Conflict Zones." *Cambridge Review of International Affairs* 23 (2): 349–69. https://doi.org/10.1080/09557571003752688.
Hersman, Rebecca, and Cassidy Nelson. 2026. "The Weapons of Mass Destruction AI Security Gap." Ideas. *TIME*, February 12. https://time.com/7373405/weapons-of-mass-destruction-ai-security-gap/.
Hong, Shen Zhou, Alex Kleinman, Alyssa Mathiowetz, et al. 2026. "Measuring Mid-2025 LLM-Assistance on Novice Performance in Biology." *arXiv*, ahead of print. https://doi.org/10.48550/ARXIV.2602.16703.
Houser, Tyler, and Beidi Dong. 2025. "The Convergence of Artificial Intelligence and Terrorism: A Systematic Review of the Literature." *Studies in Conflict & Terrorism*, July 14, 1–24. https://doi.org/10.1080/1057610X.2025.2527608.
Humphrys, Steven. 2024. *Analysis: How Jihadists Experimented with AI in 2024*. BBC Monitoring.
Institute for Economics & Peace. 2025. *Global Terrorism Index 2025: Measuring the Impact of Terrorism*. Sydney.
International Crisis Group. 2024. *JAS vs. ISWAP: The War of the Boko Haram Splinters*. Crisis Group Africa Briefing No. 196. Dakar/Brussels.
Jamiu, Abiodun. 2025. "Nigeria: ISWAP Extremists Launching Attack Drones." *Deutsche Welle*, April 16. https://www.dw.com/en/iswap-extremists-launching-attack-drones-in-nigeria/a-72241455.
Janjeva, Ardi, Anna Gausen, Sarah Mercer, and Tvesha Sippy. 2024. *Evaluating Malicious Generative AI Capabilities*. Briefing Paper. Centre for Emerging Technology and Security.
Jha, Satish. 2025. "Hyderabad ricin terror plotter wanted to 'separate South India from rest of country" *Deccan Herald*, November 20. https://www.deccanherald.com/india/telangana/hyderabad-ricin-terror-plotter-wanted-to-separate-south-india-from-rest-of-country-3804094.
Juelich, Antonia. 2024. "Turbulence and Stability: Civilian Cooperation in Boko Haram's Insurgency." PhD thesis, University of Edinburgh.
Juelich, Antonia. 2026. "Noncombatant Rebels: Coercion, Social Mobility, and Turbulent Cooperation." *Journal of Peace Research*, February 26, xjaf031. https://doi.org/10.1093/jopres/xjaf031.

Kassim, Abdulbasit. 2015. "Defining and Understanding the Religious Philosophy of Jihādī-Salafism and the Ideology of Boko Haram." *Politics, Religion & Ideology* 16 (2–3): 173–200. https://doi.org/10.1080/21567689.2015.1074896.

Kassim, Abdulbasit. 2018. "Boko Haram's Internal Civil War: Stealth Takfir and Jihad as Recipes for Schism." In *Boko Haram Beyond the Headlines: Analyses of Africa's Enduring Insurgency*, edited by Jacob Zenn. Combating Terrorism Center.

Lakomy, Miron. 2023. "Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities." *Studies in Conflict & Terrorism*, 1–21. https://doi.org/10.1080/1057610X.2023.2259195.

Last, Murray. 2014. "From Dissent to Dissidence: The Genesis & Development of Reformist Islamic Groups in Northern Nigeria." In *Sects and Social Disorder: Muslim Identities and Conflict in Northern Nigeria*, edited by Abdul R. Mustapha. Boydell & Brewer. Cambridge Core.

Leader Maynard, Jonathan. 2019. "Ideology and Armed Conflict." *Journal of Peace Research* 56 (5): 635–49. https://doi.org/10.1177/0022343319826629.

Levy, Ido. 2019. "Lethal Beliefs: Ideology and the Lethality of Terrorist Organizations." *Terrorism and Political Violence* 35 (4): 811–27. https://doi.org/10.1080/09546553.2021.1977282.

Loimeier, Roman. 2011. *Islamic Reform and Political Change in Northern Nigeria*. Northwestern University Press.

Maclean, Ruth, and Ismail Alfa. 2021. "Thousands of Boko Haram Members Surrendered. They Moved in Next Door." *The New York Times*, September 23. https://www.nytimes.com/2021/09/23/world/africa/boko-haram-surrender.html.

Mahmoud, Omar. 2018. "Local, Global, or in Between? Boko Haram's Messaging, Strategy, Membership, and Support Networks." In *Boko Haram Beyond the Headlines: Analyses of Africa's Enduring Insurgency*, edited by Jacob Zenn. Combating Terrorism Center.

Makuch, Ben. 2025. "How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations." *The Guardian*, July 8. https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence .

Marshall, Eleanor, Jasper Götting, Nelly Mak, Peter Peneder, Pedro Medeiros, and Seth Donoughe. 2026. *BioTIER: Biological Targeted Information for Exclusion and Refusal*. SecureBio. https://securebio.org/biotier/.

Marzuk, Alaa, and Rafael Green. 2025. "AI Through the Lens of ISIS: A Terrorist Organization's Guide to AI Tools." *ActiveFence*, May 13. https://www.activefence.com/blog/isis-genai-abuse-guide/.

McCants, William. 2015. *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State*. St. Martin's Press.

Meagher, Kate, and Ibrahim H. Hassan. 2020. "Informalization & Its Discontents. The Informal Economy & Islamic Radicalization in Northern Nigeria." In *Overcoming Boko Haram: Faith, Society and Islamic Radicalization in Northern Nigeria*, edited by Abdul R. Mustapha and Kate Meagher. Western Africa Series. Boydell & Brewer.

Mouton, Christopher A., Caleb Lucas, and Ella Guest. 2024. *The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study*. RR-A2977-2. RAND Corporation. https://doi.org/10.7249/RRA2977-2.

Mustapha, Abdul R. 2014. "Understanding Boko Haram." In *Sects and Social Disorder: Muslim Identities and Conflict in Northern Nigeria*, edited by Abdul R. Mustapha. Boydell & Brewer. Cambridge Core.

Mustapha, Abdul R., and Mukhtar U. Bunza. 2014. "Contemporary Islamic Sects & Groups in Northern Nigeria." In *Sects and Social Disorder: Muslim Identities and Conflict in Northern Nigeria*, edited by Abdul R. Mustapha. Boydell & Brewer. Cambridge Core.

Mustapha, Abdul R., and David Ehrhardt. 2018. "Diversity, Religious Pluralism & Democracy." In *Creed and Grievance: Muslim-Christian Relations and Conflict Resolution in Northern Nigeria*, edited by Abdul R. Mustapha and David Ehrhardt. Western Africa Series. Boydell & Brewer.

OpenAI. 2024. "Building an Early Warning System for LLM-Aided Biological Threat Creation." February 14. https://openai.com/index/building-an-early-warning-system-for-llm-aided-biological-threat-creation/.

OpenAI. 2025. "Preparing for Future AI Capabilities in Biology." November 6. https://openai.com/index/preparing-for-future-ai-capabilities-in-biology/.

OpenAI. 2026. "Scaling Trusted Access for Cyber with GPT-5.5 and GPT-5.5-Cyber." May 13. https://openai.com/index/gpt-5-5-with-trusted-access-for-cyber/.

Palmer, Annie. 2025. "FBI Says Palm Springs Bombing Suspects Used AI Chat Program to Help Plan Attack." AI Effect. *CNBC*, June 4. https://www.cnbc.com/2025/06/04/fbi-palm-springs-bombing-ai-chat.html.

Parkinson, Sarah E. 2021. "Practical Ideology in Militant Organizations." *World Politics* 73 (1): 52–81. https://doi.org/10.1017/S0043887120000180.

Pfaff, Anthony C., Brennan Deveraux, Sarah Lohmann, et al. 2025. *The Weaponization of AI: The Next Stage of Terrorism and Warfare*. No. 51450. Edited by Anthony C. Pfaff. Centre of Excellence Defence Against Terrorism.

Phillips, Brian J. 2017. "Deadlier in the U.S.? On Lone Wolves, Terrorist Groups, and Attack Lethality." *Terrorism and Political Violence* 29 (3): 533–49. https://doi.org/10.1080/09546553.2015.1054927.

Pita, René, and Rohan Gunaratna. 2009. "Revisiting Al-Qa'ida's Anthrax Program." *CTC Sentinel* 2 (5): 10–13.

Raineri, Luca. 2022. "Explaining the Rise of Jihadism in Africa: The Crucial Case of the Islamic State of the Greater Sahara." *Terrorism and Political Violence* 34 (8): 1632–46. https://doi.org/10.1080/09546553.2020.1828078.

Righetti, Luca. 2025. *Dual-Use AI Capabilities and the Risk of Bioterrorism: Converting Capability Evaluations to Risk Assessments.* GovAI.

Rose, Sophie, Richard Moulange, James Smith, and Cassidy Nelson. 2024. *The Near-Term Impact of AI on Biological Misuse*. The Centre for Long-Term Resilience. https://doi.org/10.71172/1ktf-xpxm.

Rousselle, Adam. 2025. "Combating Islamic State Finance: West Africa and the Sahel." *Global Network on Extremism & Technology*, February 18. https://gnet-research.org/2025/02/18/combating-islamic-state-finance-west-africa-and-the-sahel/.

Rustad, Siri Aas. 2025. *Conflict Trends: A Global Overview, 1946–2024*. PRIO Paper. Peace Research Institute Oslo.

Samuel, Malik. 2023. *ISWAP's Use of Tech Could Prolong Lake Chad Basin Violence*. ISS Today. Institute for Security Studies. https://issafrica.org/iss-today/iswaps-use-of-tech-could-prolong-lake-chad-basin-violence.

Samuel, Malik. 2025. *From the Levant to Lake Chad: ISIS Fighters Fuel ISWAP Resurgence*. May 30. https://gga.org/from-the-levant-to-lake-chad-isis-fighters-fuel-iswap-resurgence/.

Samuel, Malik. 2026a. "Did the US Military Strikes in Nigeria Hit the Right Target?" *The New Humanitarian*, January 12. https://www.thenewhumanitarian.org/analysis/2026/01/12/us-military-strike-nigeria-target.

Samuel, Malik. 2026b. "The Al-Minuki Raid Raises Questions about Nigeria-US Military Ties." *Good Governance Africa*, May 18. https://gga.org/the-al-minuki-raid-raises-questions-about-nigeria-us-military-ties/.

Santhana Dass, Rueben Ananthan. 2021. "Jihadists' Use and Pursuit of Weapons of Mass Destruction: A Comparative Study of Al-Qaeda and Islamic State's Chemical, Biological, Radiological and Nuclear (CBRN) Weapons Programs." *Studies in Conflict & Terrorism*, October 27, 1–35. https://doi.org/10.1080/1057610X.2021.1981203.

Sarnoff, Leah. 2025. "FBI Releases Timeline of Suspect Shamsud-Dim Jabbar's New Orleans Attack." *ABC News*, January 5. https://abcnews.com/US/fbi-releases-timeline-suspect-shamsud-dim-jabbars-new/story?id=117280639.

Smith, Mike. 2015. *Boko Haram: Inside Nigeria's Unholy War*. I.B. Tauris.

Solea, Anda. 2025. "Prompted to Harm: Analysing the Pirkkala School Stabbing and Its Digital Manifesto." *Global Network on Extremism & Technology*, June 12. https://gnet-research.org/2025/06/12/prompted-to-harm-analysing-the-pirkkala-school-stabbing-and-its-digital-manifesto/.

Stalinsky, Steven. 2023. "Terrorists Love New Technologies. What Will They Do With AI?" *Newsweek*, March 14. https://www.newsweek.com/terrorists-love-new-technologies-what-will-they-do-ai-opinion-1787482.

Stalinsky, Steven. 2025. *Artificial Intelligence and the New Era of Terrorism: An Assessment of How Jihadis Are Using AI to Expand Their Propaganda, Recruitment, and Operations and the Implications for National Security*. Inquiry & Analysis Series 1895. MEMRI. https://www.memri.org/reports/artificial-intelligence-and-new-era-terrorism-assessment-how-jihadis-are-using-ai-expand.

Tech Against Terrorism. 2023. *Early Terrorist Experimentation with Generative Artificial Intelligence Services*.

Thaler, Kai M., Antonia Juelich, and Sean Paul Ashley. 2024. "From Snapshots to Panoramas: Navigating Power, Space, and Time in the Study of Armed Groups." *Conflict, Security & Development* 24 (6): 725–55. https://doi.org/10.1080/14678802.2024.2390407.

The Economist. 2026a. "How AI Tools Could Enable Bioterrorism." May 5. https://www.economist.com/science-and-technology/2026/05/05/how-ai-tools-could-enable-bioterrorism.

The Economist. 2026b. "The World Must Stop AI from Empowering Bioterrorists." May 7. https://www.economist.com/leaders/2026/05/07/the-world-must-stop-ai-from-empowering-bioterrorists.
The Soufan Center. 2026. "Lakurawa's Growing Presence in Nigeria and the Crime-Terror Nexus." *Intelbrief*, February 6. https://thesoufancenter.org/intelbrief-2026-february-6/.
Thomas, Clayton. 2025. *The Islamic State and Its Affiliates*. In Focus No. IF10328. Congressional Research Service. https://www.congress.gov/crs-product/IF10328.
Thornhill, John. 2026. "Anthropic Chief Dario Amodei: 'I Don't Want AI Turned on Our Own People.'" *Financial Times*, April 17.
Thurston, Alexander. 2016. *'The Disease Is Unbelief': Boko Haram's Religious and Political Worldview*. Analysis Paper No. 22. The Brookings Project on U.S. Relations with the Islamic World.
Thurston, Alexander. 2018. *Boko Haram: The History of an African Jihadist Movement*. Princeton University Press.
Tishler, Nicole A. 2018. "Trends in Terrorists' Weapons Adoption and the Study Thereof." *International Studies Review* 20 (3): 368–94. https://doi.org/10.1093/isr/vix038.
Trujillo, Horacio R., and Brian A. Jackson. 2006. "Organizational Learning and Terrorist Groups." In *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*, by James J. F. Forrest. Rowman and Littlefield.
UK AI Security Institute. 2025. *Frontier AI Trends Report*. London. https://www.aisi.gov.uk/frontier-ai-trends-report.
UN OCHA. 2025. "Lake Chad Basin - Humanitarian Snapshot." March 6. https://www.unocha.org/publications/report/cameroon/lake-chad-basin-humanitarian-snapshot-3-march-2025.
UN Security Council. 2020. *Islamic State West Africa Province (ISWAP)*. February 23. https://main.un.org/securitycouncil/en/content/islamic-state-west-africa-province-iswap-0.
UN Security Council. 2024. *Letter Dated 23 January 2024 from the Chair of the Security Council Committee Pursuant to Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings and Entities Addressed to the President of the Security Council*. S/2024/92.
UNITAD. 2023. "UN Investigative Team Outlines Findings Around ISIL Chemical Weapons Use." June 8. https://news.un.org/en/story/2023/06/1137492.
United States Department of State. 2023. *Terrorist Designation of ISIS General Directorate of Provinces Leaders*. June 8. https://2021-2025.state.gov/terrorist-designation-of-isis-general-directorate-of-provinces-leaders/.
United States District Court for the Central District of California. 2025. "United States v. Daniel Jongyeon Park." Criminal Complaint, Case No. 5:25-mj-00400-DUTY. June 4. static.foxnews.com/foxnews.com/content/uploads/2025/06/ed25mj00400duty-lodged-complaint_redacted.pdf.
UNOCT, and UNICRI. 2021. *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes*.

U.S. House of Representatives. 2025. Generative AI Terrorism Risk Assessment Act. H.R. Rep. No. 119-373. 119th Congress. https://www.congress.gov/committee-report/119th-congress/house-report/373/1.

van der Merwe, Matthew. 2025. *Assessing the Risk of AI-Enabled Cyberattacks on the Power Grid*. GovAI. https://www.governance.ai/research-paper/ai-enabled-cyberattacks-on-the-power-grid.

Vasseur, Michael, Chad C. Serena, Colin P. Clarke, Irina A. Chindea, Erik E. Mueller, and Nathan Vest. 2022. *Understanding and Reducing the Ability of Violent Nonstate Actors to Adapt to Change*. Research Report. RAND Corporation. https://doi.org/10.7249/RR-A324-1.

Vienna Online. 2025. *Two Years Imprisonment for Vienna IS Supporter: Terror Plans Discussed with ChatGPT*. September 30. https://www.vienna.at/two-years-imprisonment-for-vienna-is-supporter-terror-plans-discussed-with-chatgpt/9706298.

Walker, Andrew. 2016. "Join Us or Die: The Birth of Boko Haram." *The Guardian*, February 4. https://www.theguardian.com/world/2016/feb/04/join-us-or-die-birth-of-boko-haram.

Weimann, Gabriel. 2025. "Generative AI and Terrorism." In *Oxford Intersections: AI in Society*, edited by Philipp Hacker. Oxford University Press. https://doi.org/10.1093/9780198945215.003.0100.

Weimann, Gabriel, Alexander T. Pack, Rachel Sulciner, Joelle Scheinin, Gal Rapaport, and David Diaz. 2024. "Generating Terror: The Risks of Generative AI Exploitation." *CTC Sentinel* 17 (1): 17–24.

Wells, David. 2025. "Mapping Terrorist AI Use: Identifying Factors Behind a Relatively Slow Adoption Rate." *Global Network on Extremism & Technology*, September 17. https://gnet-research.org/2025/09/17/mapping-terrorist-ai-use-identifying-factors-behind-a-relatively-slow-adoption-rate/.

Wells, Georgia. 2026a. "ChatGPT Wrestles With Its Most Chilling Conversation: How Do I Plan an Attack?" *Wall Street Journal*, May 3. https://www.wsj.com/us-news/chatgpt-mass-shooting-openai-78a436d1.

Wells, Georgia. 2026b. "OpenAI Employees Raised Alarms About Canada Shooting Suspect Months Ago." *Wall Street Journal*, February 21. https://www.wsj.com/us-news/law/openai-employees-raised-alarms-about-canada-shooting-suspect-months-ago-b585df62.

Williams, Bridget, Luca Righetti, Josh Rosenberg, et al. 2025. *Forecasting LLM-Enabled Biorisk and the Efficacy of Safeguards*. Forecasting Research Institute.

Wood, Elisabeth J. 2006. "The Ethical Challenges of Field Research in Conflict Zones." *Qualitative Sociology* 29 (3): 373–86. https://doi.org/10.1007/s11133-006-9027-8.

Zelin, Aaron Y. 2024. "A Globally Integrated Islamic State." *War on the Rocks*, July 15. https://warontherocks.com/2024/07/a-globally-integrated-islamic-state/.

Zenn, Jacob. 2020. *Unmasking Boko Haram: Exploring Global Jihad in Nigeria*. Lynne Rienner Publishers. https://doi.org/10.1515/9781626378933.

APPENDIX

Fieldwork Methods & Practices

This appendix describes how I selected participants, conducted interviews, and analyzed data for this study. It complements the methods section in the main text and provides additional detail on the practical and ethical dimensions of the research process. This study was conducted in line with the ethical procedures and safeguards established through my prior IRB-approved research with former members of Boko Haram in Nigeria.

Access and Recruitment

Access to this hard-to-reach population was made possible by an established network of contacts built through my prior doctoral fieldwork in northeast Nigeria. Participants were recruited through community leaders and mobilizers in government-controlled areas in Adamawa and Borno state who have been involved in the reintegration of former Boko Haram members. Since 2021 in particular, following the death of JAS's leader Shekau and intensified fighting between ISWAP and JAS, large numbers of former members have returned and reintegrated into communities. That process has involved cooperation between communities, government authorities, and security forces. Communities have a strong interest in ensuring that returnees have genuinely disassociated, and the social and institutional infrastructure surrounding reintegration meant that former members' conflict histories were generally known to community leaders.

I deliberately avoided recruiting through aid organizations, deradicalization programs, or detention facilities, out of concern that participants in those settings

might not feel free to decline participation or to speak candidly. Instead, I worked through my research assistant, a local researcher with extensive experience studying the conflict in northeast Nigeria, with whom I have collaborated since my doctoral fieldwork in 2018. The research context and selection criteria were shared with community mobilizers, who then identified individuals. In describing the research to potential participants, I kept the framing sufficiently broad, as being about "how Boko Haram and ISWAP operate," to avoid inadvertently revealing details about individuals' prior roles to other community members. Ahead of interviews, my research assistant met with potential participants to confirm they met the selection criteria and to explain the general nature of the research.

Participants were required to meet the following selection criteria: over age 18; former members with no active affiliation or links to any non-state armed group; screened and cleared by the Nigerian military; disengaged for an extended period of several months; and assessed as psychologically stable and healthy to participate. Within this eligible pool, I prioritized individuals who had been members between 2022 and 2025, held commanding authority, or had occupied operational or technical roles likely to have brought them into contact with AI-related activities. I also sought to cover both factions to allow for a comparative analysis. These priorities shaped the sample iteratively. Participants did not receive financial or material compensation for taking part in the research, though logistical costs and refreshments were covered where appropriate.

Interview Process

Data was collected across two rounds of fieldwork in 2025 and 2026, with follow-up interviews conducted with participants who had shown extensive knowledge of the research topic. The first round was more exploratory in nature. I did not enter the

field with certainty that I would find evidence of AI adoption. Rather, my prior research experience in northeast Nigeria, including several fieldwork trips since 2018 and approximately one year spent in the region in total, provided the contextual knowledge and established networks that made this study feasible. The question of whether AI was being used was itself an empirical one that the fieldwork was designed to answer. Interviews in the first round focused broadly on technology adoption and organizational dynamics, with AI emerging as a topic organically as participants described their groups' operational practices. The second round built on the first in that I sought to confirm findings, pursue details that had emerged, and conduct follow-up interviews with participants who had demonstrated particular knowledge of AI-related practices.

Each interview began with questions about participants' backgrounds, how they had become affiliated with the group, and their disassociation process. This served both to establish rapport and to contextualize what followed. Rather than asking about AI directly at the outset, I traced participants' accounts of the group's broader approach to technology and innovation, allowing AI to arise in this context. This reduced the risk of participants calibrating their answers to what they thought I expected, and meant that those with limited exposure to AI could still contribute meaningfully to understanding other dimensions of technology adoption. As trust developed over the course of individual interviews and across repeated meetings, I tailored questions more directly to the specific aspects of AI most relevant to each participant's role and experience. I met with each participant about one to three times, with some individuals interviewed up to six times across both rounds. Interviews lasted 90 minutes on average.

Informed verbal consent was obtained at the start of each interview. Participants were told the purpose of the research and that they were under no obligation to

answer any question or to continue the interview. No names were recorded. Interviews were conducted without recording in the first round. In the second round, participants consented to being recorded, which was done to allow for more precise verification of accounts and to support more detailed analysis. In a small number of cases, individuals who had agreed to participate withdrew before the interview began, mostly out of fear of negative repercussions, which demonstrated that the decision to talk about their experiences was not made lightly.

My research assistant served as my interpreter throughout. He speaks several local languages and translated primarily from Hausa and Kanuri. All interviews except those with one fully English-fluent participant were conducted primarily in Hausa or Kanuri. Where participants had partial English fluency, this occasionally allowed for clarification or direct follow-up without translation, but the primary medium of exchange remained the local language. Translation introduced complexities beyond the purely linguistic. Finding the right framing and phrasing to ask questions about AI required time and iterative adjustment, particularly given that participants had differential access to and awareness of AI depending on their rank and role. As I developed a better understanding of each participant's background and position, I was better placed to tailor questions to the aspects of their experience most likely to be informative. Translation also meant that interviews were more time-consuming than they would otherwise have been, making it difficult to pursue every line of inquiry in as much depth as I would have liked.

Positionality

My positionality shaped the research in ways that are not always easy to assess with confidence and that are likely to have varied across participants. I benefitted greatly from the trust my research assistant had established with participants and with the

community networks through which they were recruited. His presence provided reassurance to participants who might otherwise have been reluctant to speak with an outside researcher, particularly on a topic as sensitive as this one. Over repeated meetings, I also gained a degree of trust in my own right, and I found that participants became more candid as interviews progressed and as I returned for follow-up conversations. Occasional breaks spent in informal conversation over tea often proved as important for building rapport as the interviews themselves.

As a Western woman, I was an obvious outsider — whether in terms of ethnicity, religion, culture, or language — and this shaped the interview dynamic in ways that cut in different directions. Male researchers or those with local ties might have been perceived as more threatening due to potential associations with Nigerian security agencies. At the same time, my status as a foreigner raised its own suspicions, particularly about why I was interested in the conflict and in the technology dimension specifically. I tried to mitigate this through transparency about the academic nature of the project, answering questions interviewees had, attentiveness to participants' comfort, and adjustments when questions seemed to cause unease. How my identity was read and what effect it had ultimately depended on individual participants, and I cannot claim to have assessed this with any precision.

Data Storage & Security

No names were recorded at any point during the research. Participant codes are stored separately from all interview data. All data, including recordings from the second round of fieldwork, are stored on encrypted local drives accessible only to me. Physical notes were digitized and password-protected shortly after each interview, and the physical copies destroyed. Given the sensitivity of the research and the potential risks to participants if their identities were disclosed, these measures were

treated as a baseline rather than a ceiling, and any information that could narrow the pool of possible identities has been withheld from all outputs.

Fieldwork Conditions & Constraints

A brief note on the conditions under which this research was conducted seems warranted, in the spirit of transparency about what fieldwork of this kind actually involves. Participants varied considerably, in that some were forthcoming and expansive, others guarded and brief; some showed up late or not at all, others early and unexpectedly. Staying on track across interviews that varied this much in character, while building sufficient trust to discuss sensitive operational details, required constant adjustment and considerable patience. Logistics before, during, and after interviews were often demanding, alongside challenges like heat, power outages, sickness, the need to remain responsive to a shifting security environment, and the administrative complexity of coordinating interviewees across multiple communities. None of this is unusual for research of this kind in conflict-affected settings, but it bears mentioning as context for the practical constraints that shape what is and is not possible in studies like this one.

List of Interviewees

To ensure interviewees' anonymity, participants are identified only by a code, their most recent faction, a broad rank or role category, and the interview round in which they participated. Although some participants had experience in both factions, the denoted faction reflects their most recent affiliation, given that AI adoption occurred within the period covered by participants' most recent organizational experience. Any information that could narrow the pool of possible identities — including name, location, time of disassociation, age, and cross-faction history — has been withheld.

No.	Code	Faction	Rank / Role	Interview Round
1	JAS Commander-1	JAS	Commander	2025
2	JAS Commander-2	JAS	Commander	2025
3	JAS Commander-3	JAS	Commander	2025, 2026
4	JAS Commander-4	JAS	Commander	2025, 2026
5	ISWAP Commander-5	ISWAP	Commander	2025, 2026
6	JAS Commander-6	JAS	Commander	2025
7	ISWAP Commander-7	ISWAP	Commander	2025, 2026
8	JAS Commander-6	JAS	Commander	2025
9	ISWAP Fighter-9	ISWAP	Fighter	2025
10	JAS Technical Specialist-10	JAS	Technical Specialist	2025
11	JAS Fighter-11	JAS	Fighter	2025
12	JAS Commander-12	JAS	Commander	2025
13	JAS Fighter-13	JAS	Fighter	2025
14	JAS Fighter-14	JAS	Fighter	2025
15	JAS Fighter-15	JAS	Fighter	2025
16	JAS Fighter-16	JAS	Fighter	2025
17	ISWAP Commander-17	ISWAP	Commander	2026
18	JAS Commander-18	JAS	Commander	2026
19	JAS Non-combatant-19	JAS	Non-combatant	2026
20	ISWAP Fighter-20	ISWAP	Fighter	2026
21	ISWAP Commander-21	ISWAP	Commander	2026
22	ISWAP Commander-22	ISWAP	Commander	2026
23	ISWAP Commander-23	ISWAP	Commander	2026
24	ISWAP Commander-24	ISWAP	Commander	2026
25	JAS Fighter-25	JAS	Fighter	2026
26	JAS Commander-26	JAS	Commander	2026
27	JAS Commander-27	JAS	Commander	2026