INSTITUTE FOR SECURITY STUDIES

Wiring the insurgency

Inside ISWAP's adaptive technology programme

Taiwo Adebayo



Despite military pressure, the Boko Haram successor faction ISWAP remains resilient because its enabling ecosystem has not been dismantled. An adaptive technology programme is a critical element of that ecosystem. This report explores the networks, finance channels and organisational structures that allow ISWAP's capability to be sustained. Countering ISWAP – and pre-empting its rival faction JAS from closing the capability gap – requires multi-stakeholder responses targeting the architecture of the insurgency threat.

Key findings

- Islamic State (IS) Central's linkages are the variable explaining Islamic State West Africa Province's (ISWAP) technological and organisational trajectory – an advantage that rival faction JAS lacks.
- ISWAP's media department serves as a channel through which technical knowledge and instructions flow from IS. It is also the propaganda pipeline interfacing with IS global media and running a counter-narrative channel.
- ISWAP's drone programme has evolved from a looted technical school to purpose-built workshops that produce and fit commercial drones with improvised explosive devices.
- ISWAP's *rijal–awam* structure embeds covert agents into communities, backed by phone-enabled informants and logistics handlers; it is both an intelligence-gathering system and an agency of a parallel political economy.
- The group prioritises operational security, including the use of satellite communication devices and the restricted use of local GSM networks.
- ISWAP runs a *ghanimah* pricing system in which captured weapons are surrendered by fighters for payments by IS. This points to a key motivational variable, other than ideology, for the frequent attacks on military positions.
- The use of artificial intelligence (AI) in operations is unconfirmed, but ISWAP's history suggests the state authorities would need to take proactive steps before that becomes a threat.

Recommendations

For military and counterinsurgency operations:

- Cultivate assets and extract information from ISWAP deserters on the locations of facilities and operatives.
- Strengthen amphibious operations to pressure ISWAP and JAS on the Lake Chad islands, where they generate their revenues and locate their high commands.
- Harden military bases to reduce weapons losses and undermine the *ghanimah* system.
- Disrupt the supplies and trading that enrich the insurgency and finance its acquisition of equipment.
- Accelerate and expand the counter-drone programme.

For information and communications authorities:

- Build a rapid-response communications function that acknowledges losses, countering the credibility gap that ISWAP exploits.
- Engage satellite communication providers to monitor devices' use in conflict-affected areas and create an intelligence trail.
- Engage newsrooms on conflict-sensitive reporting, encouraging discretion in using insurgent propaganda; and engage social media platforms on preventing their systems' use by insurgents.

For financial regulators and financial intelligence units:

- Treat currency exchange networks as a priority and flag large and structu red transactions from the Middle East to the Lake Chad Basin.

For civilian protection and humanitarian actors:

- Integrate technical literacy as an abduction risk factor in programming for communities.

For regional bodies and international partners:

- Treat ISWAP's drone and technology programme as an IS-network problem, and share intelligence with Lake Chad Basin countries.
- Support the Multinational Joint Task Force's (MNJTF) operational capacity, and encourage Niger to rejoin the MNJTF.
- Engage AI companies before the tools become a confirmed threat.

Introduction

Nearly two decades after the Boko Haram insurgency began in Nigeria – its worst-hit country – and spread across the Lake Chad Basin into Cameroon, Niger and Chad, the resilience of its successor factions remains striking. Islamic State West Africa Province (ISWAP) and Jama'tu Ahlis Sunna Lidda'awati wal-Jihad (JAS) have demonstrated a capacity to survive disruption, to reorganise and to adapt, despite military pressure and stabilisation initiatives.[1] ISWAP, especially, has shown a notable capability for technological adaptation as a critical element of its enabling ecosystem, advancing in three areas: communications and propaganda, intelligence gathering, and combat operations.[2, 3]

Over the past 10 years, ISWAP's evolution ranks among the most significant examples of how adaptive technology has been adopted by non-state armed groups in Africa – made more significant by the absence of a foreign state patron. In contrast, groups such as the Iran-backed Houthis in Yemen and the Azawad Liberation Front in Mali, which has reportedly drawn on drone warfare training and tactics from Ukraine,[4] illustrate the accelerating effect that state-backed assistance can have on a non-state armed group's capabilities.

ISWAP does not have an equivalent relationship with any government; it cannot call on a state's military–industrial powers or diplomatic cover. However, what it has instead is the Islamic State (IS) network, providing the insurgent group with technical training, financing and media infrastructure. That substitution is not perfect but is sufficient to sustain a decade of technological adaptation, from bread-wrapped memory cards to satellite phones and combat drones. Yet this evolution is underexplored in terms of who built the capability and how.

ISWAP's evolution ranks among the most significant examples of how technology has been adopted by non-state armed groups in Africa

This report uses the term 'adaptive technology programme' to mean the strategic and tactical modification, adoption or repurposing of civilian, commercial and digital tools to enhance military, logistical and operational capabilities. As the report shows, this description defines ISWAP's technological trajectory more precisely than the existing concepts of 'improvised weaponisation' and 'dual-use technology'.[5]

The report traces the development and sustainability of ISWAP's communications apparatus, linked to the IS global media machinery and how it integrates trapped communities into intelligence-gathering and parallel political economy systems. The research examines the group's shift from initially using drones for the reconnaissance of military positions to leveraging

ARMED GROUPS IN AT LEAST

10

AFRICAN COUNTRIES HAVE USED DRONES FOR ATTACKS, INTELLIGENCE AND PROPAGANDA

the technology at scale for offensive operations. In addition, the study analyses ISWAP's capacity for making locally produced munitions and bomb-laden drones.

None of these developments occurred outside the IS network, which provides access to enabling resources as earlier noted. But ISWAP's capacity is not simply imported; rather, the group has adapted external knowledge and resources to its local operational conditions. This explains the divergence in ISWAP's trajectory compared with that of JAS.

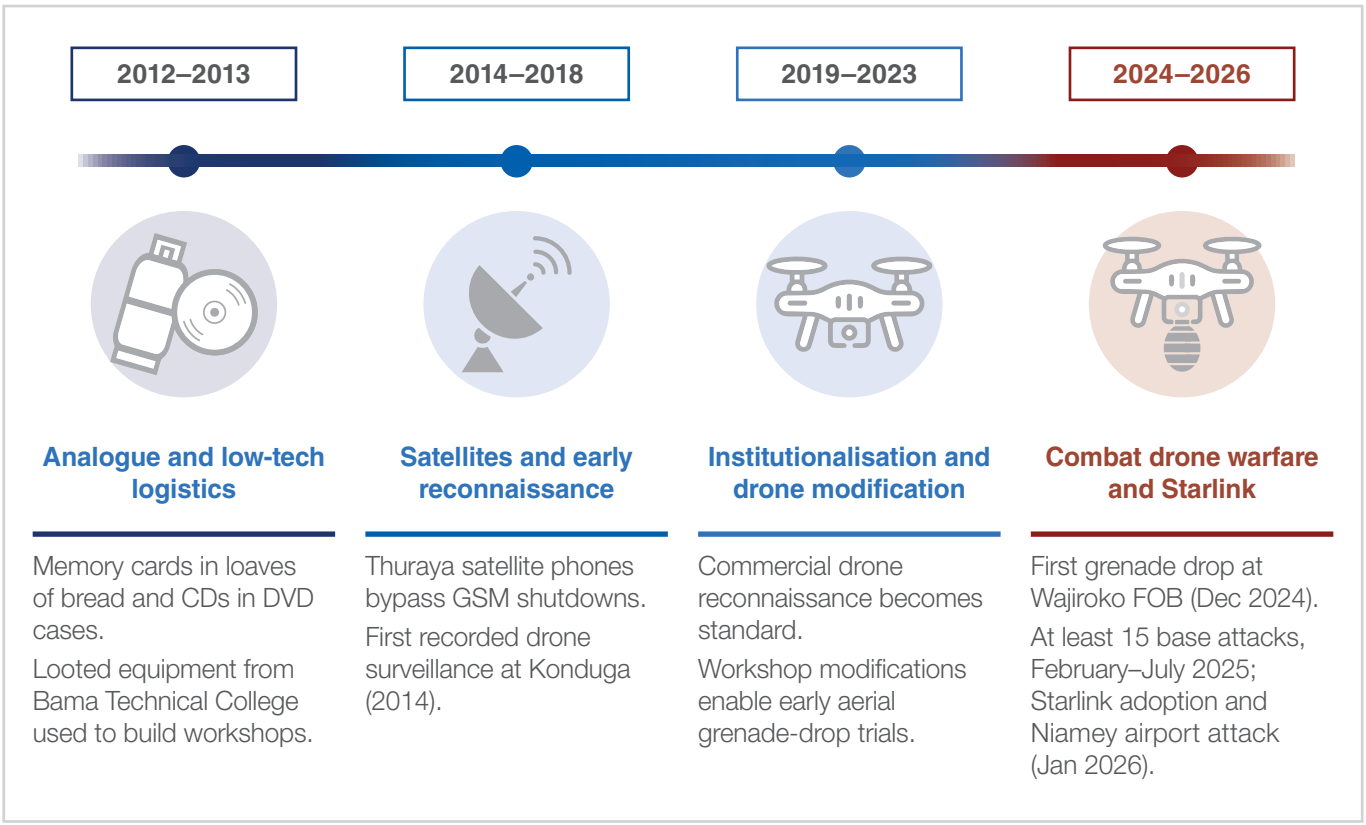
Before their split, both groups, as a unified Boko Haram under Abubakar Shekau, shared access to external assistance from foreign jihadists, including in communications, improvised explosives and the use of drones for reconnaissance. However, since the split, JAS has persisted through a comparatively low-tech and looser organisation, while ISWAP has built a more structured organisation with specialised functions. ISWAP's adaptive technology programme is at the core of its broader organisational professionalisation.

Accordingly, this report asks: how has ISWAP acquired and used technologies for intelligence gathering, communications and combat? And what does this reveal about external linkages in distinguishing ISWAP's trajectory from JAS's?

ISWAP's capacity is not simply imported; rather, the group has adapted external knowledge and resources

By exploring these dynamics, this report offers insights into how Boko Haram, particularly ISWAP, maintains its operational effectiveness and poses a significant challenge to regional stability. This discussion is important for devising counterstrategies against insurgent tactics. This report is part of the Institute for Security Studies' (ISS) Disrupting Armed Groups' Operational Resilience in the Lake Chad Basin project and draws on extensive fieldwork across the region.

Chart 1: Evolution of ISWAP's adaptive technology programme, 2012–2026



Source: ISS interviews; ACLED

Methodology

This report draws on primary interview data conducted in Maiduguri, Borno State, Nigeria with 17 key informant sources between April and September 2026, summarised in Chart 2. Several sources left the insurgency as recently as 2024, 2025 and even 2026, and most of them were pioneers. Other sources were security and intelligence officers and others had experience with Boko Haram through research, trading and social relationships established with members and ex-members before the insurgency.

The sample is small and non-random. It is drawn from existing networks and with the help of local fixers, including those whose relationship with Boko Haram dates back to pre-insurgency years and who received ex-fighters when they fled the insurgency. It is indicative of internal practice, and the interviews were triangulated by cross-checking findings against other testimonies and open-source and previous reporting by the ISS.

Secondary sources were also explored including public news, policy and academic publications. Importantly, the report benefits from several closed-door security briefings and policy engagements that the author participated in between July and October 2026 in N'Djamena, Chad and Abuja , Nigeria. The report also benefits from colleagues who have conducted primary research in Lac Province, Chad and Far North, Cameroon. These professionals shared insights during a data review workshop in N'Djamena, in July 2026 and through continuous virtual conversations up to September 2026.

Chart 2: Key informants

Code	Role or area	Faction history, background or location
P1	Media, editing operative	Pre-split-era Sambisa, ISWAP, briefly held by JAS in 2025, escaped
P2	Combat, ordnance fabrication	Early Boko Haram, student of Mohammed Yusuf, ISWAP, early exposure to drone technology
P3	Drone operator	ISWAP, left 2025
P4	Logistics and procurement	ISWAP
P5	Media, photographer	Early Boko Haram, forcibly recruited from Pulka, switched to ISWAP
P6	Communications operative, self-described 'combatant and journalist'	ISWAP, left 2026
P7	Rank and file fighter	ISWAP, left 2024
P8	Fish trader, civilian	Trades at ISWAP-controlled island markets and Baga Road Market, Maiduguri
P9	Source with inside information on finance department	ISWAP
P10	Counterinsurgency intelligence	Nigeria
P11	Army commander	Nigeria
P12	Counterinsurgency intelligence	Chad
P13	Civilian with contacts in Boko Haram; helped cater to members' families when they were forced out of Maiduguri after the 2009 uprising	Maiduguri
P14	Air force intelligence	Nigeria
P15	Local chief	Maiduguri
P16	Local resident, non-governmental organisation worker and former student of Mohammed Yusuf and classmate of his sons	Maiduguri
P17	Experienced researcher on Boko Haram insurgency	Abuja

Source: ISS interviews

The rise of new technology use by armed groups: a continental trend

ISWAP's technological evolution is only one case of a broader regional trend. Across Africa, armed groups have been steadily integrating commercial and digital technologies into their operations, with drone adoption being the most worrying and disruptive element of that trend. Armed groups in at least 10 countries have used drones for direct attacks, reconnaissance and propaganda: Burkina Faso, the Democratic Republic of the Congo (DRC), Kenya, Libya, Mali, Mozambique, Niger, Nigeria, Somalia and Sudan.[6] ISWAP is the most active drone user among IS affiliates in Africa, but it trails Jama'at Nusrat al-Islam wal-Muslimin (JNIM), the al-Qaeda affiliate in the Sahel region, with over 100 cases since 2023, according to Armed Conflict Location & Event Data (ACLED).[7]

In East Africa and the Horn of Africa, al-Shabaab mirrors ISWAP's method, using drones to scout troops' positions and to coordinate ground attacks (see 'From reconnaissance to weaponisation' below). The group's most documented milestone was the January 2020 assault on the United States (US) military base at Manda Bay, Kenya, where drones gathered real-time intelligence ahead of a ground attack that killed three Americans. Al-Shabaab has not yet publicly claimed a weaponised drone strike but there have been repeated documented deployments for reconnaissance.[8]

ISWAP's communication explicitly counters the Nigerian government's narrative that Boko Haram is degraded

In the DRC, the Rwanda-backed March 23 Movement claimed a drone strike targeting Kisangani Bangoka International Airport's army command centre in March 2026, roughly 400 km from its active frontlines.[9] Further south, the IS affiliate in Mozambique, Ansar al-Sunna, deployed commercially available drones for target identification in Cabo Delgado as early as 2020, which was confirmed by Mozambique's interior minister.[10]

Beyond the policy relevance, there is a broader theoretical reason behind the importance of asking questions about armed groups' adoption and adaptation of technology. Research on the role of digital technology in armed conflicts shows that a technological advantage tends not to last since the disadvantaged side typically finds a workaround within a period of re-adaptation by leveraging openly and commercially available counter-options. In a 2025 Carnegie Endowment study that examined Boko Haram's cellular network history, as one of three case studies alongside Ukraine and Somalia, this pattern is described as a cycle of 'innovation-adaptation' and it explains the protraction of some conflicts.[11]

This report explains the survival of Boko Haram, particularly ISWAP, over many years of innovating strategies against – and adapting to and



ISWAP IS THE MOST ACTIVE DRONE USER AMONG IS AFFILIATES IN AFRICA

disrupting – counterinsurgency operations. The shift to satellite communications and the restricted use of local subscriber identity module (SIM) cards, among other strategies, is a response to the Nigerian government's earlier advantages, for example the 2011 SIM-registration mandate and the Global System for Mobile communications (GSM) network shutdowns since 2013.

Similarly, ISWAP's drone programme is the latest iteration of its innovation-adaptation cycle. The technology is now used in attacks to help insurgents to dislodge military bases, allowing them to capture weapons that are otherwise difficult to access through illicit arms trading.[12] ISWAP projected its drone capability beyond the Lake Chad Basin in January 2026 when it reportedly deployed fighters and armed drones to support the Islamic State Sahel Province's (ISSP) coordinated attack on the Diori Hamani International Airport and Airbase 101 in Niamey, Niger (see 'From reconnaissance to weaponisation').

Meanwhile, in September 2026, a source (P17) said JAS has acquired drone technology, which it uses in its attacks against ISWAP. A review of data from the ISS' fieldwork in Chad also confirms this acquisition. The emerging development points to JAS moving to close the capability gap between it and ISWAP, complicating regional counterinsurgency operations.

Communications

Organisation of media functions

ISWAP organises its propaganda and communications through a dedicated department called the *Ilan,* which, according to ex-members, is headquartered on a tiny strip near the island of Banowa in Abadam Local Government Area (LGA), Borno State. One of the ex-fighters (P5) who worked there pointed to its location on Google Maps, while others only mentioned it by name. One described Banowa as the office for ISWAP's senior media operatives.

There are subordinate units elsewhere across all the group's *mantiqas*[13] (administrative districts), but it is from the headquarters that final materials such as edited videos of attacks are shared. Using Telegram and WhatsApp social media channels, members send these materials to IS for publication via *Amaq News Agency*, IS's main news outlet.

Apart from propaganda, the *Ilan* functions as the vital bridge between ISWAP and its external networks – 'whether new instructions are coming from *dawlah* Iraq [IS Central],' as P1 said, or the group wants to seek guidance. This function makes the department strategically crucial to ISWAP as the channel through which technical knowledge and instructions flow from IS.

Interviewed ex-fighters were consistent on the objectives of the group's communications functions. As P1 put it: 'The military will say people in the bush are weak, that they don't have anything. So, we want people to know that what they are hearing is different from reality.' Alongside recruitment and, more broadly, promotion of the *dawlah* (Islamic State) project as a growing concern rather than a defeated insurgency, the department has an explicit counter-narrative objective aimed at the Nigerian government's repeated narrative that Boko Haram is degraded.

The counter-narrative function operates in something near real-time and through a separate channel from the formal *Amaq*. The department monitors social and news media, and it sees when the military releases post-battle statements. When it assesses such a statement as a misrepresentation of casualties or equipment losses, its members reach out informally to their contacts in Maiduguri for a rebuttal. One such contact interviewed for this report (P13) said they would typically say, 'Look, they are lying … Wait for photos and videos,' referring to the *Amaq* publications usually distributed 24–48 hours after operations.

At times, when they record significant battlefield gains such as the 11–12 May 2025 assault on the Nigerian Army's 50 Task Force Battalion in Marte, the insurgents proactively use the informal channels. This works because the ISWAP media operatives know that those contacts have access to the journalists and researchers covering the conflict, giving the department a back channel for shaping the story before any formal footage surfaces.

However, they do not actually hand over any footage through the back channel, allowing the materials to pass through the *Ilan* processing to *Amaq* for publication. That is a measure of ISWAP's organisational discipline and procedural control. By contrast, JAS runs a markedly looser system, with its members sharing pictures

with contacts as soon as they have them, without an equivalent processing step.

An interviewee (P1) who had a brief stint with JAS after being taken prisoner during an attack on ISWAP's Dogon Chiku base in 2025 dismissively described JAS's media as 'nothing organised'. A researcher on Boko Haram (P17) said he had received JAS's footage in past years and clarified that ISWAP's outputs are of higher quality. A member who knew P1 and was aware of his media-handling skills advised leader Bakura Doro[14] (Abu Ummaima) and his brother Ba Tijja, JAS's head of media, that he could help with the group's struggling media operations. P1 was then released from JAS's prison in Barwa, Niger, but he fled after a while and now lives in Maiduguri, where he cooperates with officials on bringing fighters out of the insurgency.

The *Ilan* recruits from within the group and trains members on camera handling, editing, file transfers and other media and communication technology basics. But it also targets and forcibly recruits civilian community members with needed skills, a former member (P5) said, himself taken from his Pulka hometown, where he was a professional photographer.

Genealogy

Before tech-enabled communications infrastructure, Boko Haram's earliest propaganda reached the outside world through analogue means, which points to the group's early ingenuity. When Boko Haram relocated to the Sambisa Forest around 2012 under the command of Shekau and began staging attacks, it had no communications infrastructure of its own. Instead, according to interviews, to publicise its operations, fighters recorded details of attacks on a memory card or burned them to compact discs (CDs). Those materials were then sent through commercial drivers at motor parks that served as the arteries of commercial life in northeast Nigeria.

The insurgents passed memory cards tucked inside loaves of bread to bus drivers, presented as packages for delivery to contacts on the other end. CDs were slipped inside the printed covers of Indian film digital video discs (DVDs); to drivers or security operatives at checkpoints, the DVD packages were indistinguishable from commercial entertainment. At the destination, a journalist contact would collect the package. At other times, a fighter would communicate the location of a hidden drop, typically a mosque, and instruct the journalist on where to retrieve the material. The crude logistics remained in use until the group began using the Internet and shifted to email and encrypted messaging.

The current form of ISWAP's *Ilan* descends from that unified Boko Haram era, with interviewed ex-fighters separately mentioning Mohammed Tasiu, from Bauchi in northeast Nigeria, as the pioneer Boko Haram media leader. Tasiu, reportedly educated to degree level, ran a business centre in his Bauchi home city before joining the *Yusufiya* movement in Maiduguri. Interviewees described him as training the group's earliest media operatives in filming, message handling, editing and translation, having himself been further trained by Arab jihadi Abu Ayyub.

The insurgents passed memory cards tucked inside loaves of bread to bus drivers, presented as packages for delivery to contacts on the other end

Two other early media leaders, Abubakar Ukba and Umar Manchari Parisu, followed a similar trajectory. Ukba[15] had received prior training in Algeria under al-Qaeda in the Islamic Maghreb (AQIM),[16] and later trained Parisu himself. Both were killed in the field – Ukba in Bama, Borno State in 2013; Parisu by a military rocket also in Bama, along with his brother and father in 2014. Although interviewees credited Tasiu for their early training, subsequently shaping today's *Ilan*, he never formally joined ISWAP before Shekau ordered his execution in 2016. Shekau accused him of maintaining communications with the breakaway ISWAP actors.

The more consequential pair in lasting influence were brothers Habib Yusuf (al-Barnawi)[17] and Abba Yusuf (Abu Rumaisa). Habib became ISWAP's leader and a member of the global IS *shura* council,[18] and Abba was later head of ISWAP's media department. Both were sons of Boko Haram founder Mohammed Yusuf. They were schooled at El-Taha Islamic Centre, which offers both Islamic and Western education, in Maiduguri before the 2009 uprising.[19] The brothers later learnt computing

in N'Djamena, where they were taken to by their father's comrades after his death, according to civilians in Maiduguri (P13 and P16) and ex-fighters.

Habib's Arabic fluency gave Boko Haram a vital bridge to Arab IS liaisons, who were particularly interested in the two brothers and helped them to sharpen their communication technology skills. Habib, in particular, would receive messages from IS, print them out for Shekau to read and send back the replies. It appears that while Tasiu, Ukba, Parisu and others worked in general media functions, Habib and Abba mainly focused on encrypted messaging and communications with IS liaisons.

Interviewees said this was not by accident. Boko Haram's initial contact with IS was through Habib, Abba and a small number of others. They had reportedly been in conversation with IS before they informed and later persuaded Shekau in 2015 to pledge allegiance to Abu Bakr al-Baghdadi, the late leader of IS.[20]

Following the split, Habib became ISWAP's leader and Abba eventually became the media chief. Abba died in 2024 carrying out a vehicle-borne suicide attack against a Multinational Joint Task Force (MNJTF) contingent consisting of Chadian troops in Kangawar, Lake Chad during Operation Lake Sanity II.[21] Before that incident, as communications chief, he had essentially assumed the role of a bridge between ISWAP and IS, continuing what his brother used to do under Shekau's leadership.

After Abba's death, Bana Modu, a former JAS operator and one of Tasiu's trainees in the pre-split days, took over headship of the media centre. However, in early August 2026, Abdullahi Suleiman replaced Modu, with sources citing trust and competence as reasons for the change. 'He knows how to do things better. He's a graduate, and writes and speaks Arabic,' one source said about Suleiman.

Besides technical ability and graduate-level education, no further biographical and background detail had been learnt about Suleiman at the time of completing this report. The source said Modu is still alive, but this insight could not be independently verified. However, another source (P17) disputed claims that Modu is less fluent in Arabic and less technically capable than Suleiman, noting that other ex-fighters described him otherwise.

Devices and platforms

As proof of capability is a key pillar of ISWAP's media operations, every combat dispatch is reported to include operatives from the media department, who film the action and transfer footage across units. With telecom services largely cut off from Boko Haram–affected areas across the four Lake Chad Basin countries, ISWAP commonly relies on satellite services and devices to access the Internet.[22] These tools include Thuraya satellite phones, Wi-Fi devices and, more recently, Starlink.

ISWAP commonly relies on satellite services and devices to access the Internet, including Thuraya satellite phones, Wi-Fi devices and, more recently, Starlink

An interviewee (P6) who described himself as a 'combatant and journalist' during his membership of ISWAP summarised the scale of satellite communications. 'We have our own laptops, and we use Thuraya and Starlink … the number of the Thuraya is uncountable,' he said. He referred to Thuraya devices as 'Wi-Fi', a description of function since these devices are used as portable satellite hotspots rather than regular handsets. He said they are typically taken along to combat for real-time coordination and quick file transfers.

In addition, the group's toolkit includes drones, camcorders, clip-on microphones, walkie-talkies and data compression and archiving software, according to P6 and as corroborated by other sources.[23] The section 'Workshop and fabrication' below details the supply chain behind the equipment.

The strategic significance of satellite communication technology lies in how it helps the insurgents to beat the counterinsurgency measures of cutting off regular telecom services to Boko Haram–held areas. Members with smartphones, whose use of the devices is controlled, typically bypass the local network – or are required to do so – and connect to satellite Wi-Fi, communicating via the WhatsApp, Telegram and Signal platforms. This happens even in areas that retain some GSM signal because of proximity

to unaffected areas. Members usually purchase SIM cards registered with other people's identities to open accounts on these messaging apps, after which they destroy the physical SIM card. This is part of operational security measures (described in the following subsection).

Meanwhile, the switch to satellite technology also has roots in the pre-split Boko Haram era and was an indirect benefit of the group's external networks. Interviewees credited Baba Hassan, described as linked to al-Qaeda and reportedly released by Nigeria's intelligence service, the Department of State Services, around 2013, with introducing Thuraya phones to the group. This move replaced the earlier practice of physically carrying devices into neighbouring Cameroon in search of network coverage after the Nigerian government suspended telecom services in affected areas.

That period saw a parallel rise in satellite phone usage among ordinary civilians affected by the GSM shutdown, which made it difficult to isolate and target satellite phone traffic to Boko Haram. In June 2013, the military then sought to ban Thuraya phones altogether on the assessment that insurgents were using them, a move that only pushed the purchase and use of the devices into the informal supply chain.[24]

Operational security practices

Operational security differs by faction, which matters for counter-intelligence planning. ISWAP, for example, restricts SIM card use, and defiant members who use these cards conceal it to avoid punishment. When a phone with a local telecom connection is used for any operational necessity or by low-rank fighters where connectivity is available, the SIM is not registered to a member's personal identity. In particular, in the Buhaira *mantiqa* islands, where the high command and top figures are located, smartphones are highly controlled.

JAS, by contrast, is looser, with members freely using SIMs and open social media platforms such as TikTok while ISWAP members use WhatsApp, Telegram and Signal. Therefore, telecom-based tracking is likely to yield materially more against JAS than against ISWAP. The latter also forbids traders at markets under its control from selling SIM cards or even freely making telephone calls.

This is not an abstract precaution, but a measure guided by institutional memory and indicative of an innovation-adaptation cycle. In the early years of the insurgency, Boko Haram used Nigeria's GSM networks without restrictions, coordinating and even detonating phone-triggered explosive devices to stage diversionary 'dummy raids' intended to overstretch security forces.

According to the 2025 Carnegie Endowment report, the mandatory registration of SIM numbers gave the government a counter-advantage, offering security forces an intelligence capability that resulted in the arrest of some Boko Haram members in early 2012.[25] The Nigerian government expanded the move to suspend GSM networks to the Boko Haram–affected states of Borno, Adamawa and Yobe in 2013, further toughening operational coordination for the insurgents.

Boko Haram's retaliation and re-adaptation followed, and ISWAP's current practices stemmed from there. The group started attacking telecom infrastructure such as masts and base stations, apparently to counter the intelligence advantage that the government derived from GSM services.[26] Certain members started physically entering the Cameroonian territory for signal to send messages. Then Thuraya satellite phones were introduced, enabling the insurgents to use Skype. 'You can see me; I can see you,' one ex-fighter (P2) said, describing Skype.

Read against this background, ISWAP's SIM restrictions practice is not a fresh innovation. It is a mature, second-generation correction against a vulnerability that its predecessor, the pre-split Boko Haram, suffered and tried to survive more than 10 years ago.

Rijal–awam dynamic

A human network is the main pillar of ISWAP's intelligence gathering, with devices only facilitating the network itself. In each community under its influence (*awam*), ISWAP embeds an agent (*rijal*) from its state security department called *rijal amni.* The *rijal* is a liaison between their assigned *awam* and ISWAP, and supplies a phone to covert agents in the community to spy on the military.

Where network coverage is unavailable, the fallback is either a motorcycle courier or a memory card physically carried into the bush by a child or woman for the *rijal*

to insert into their own phone to play the recorded audio. The spies also help ISWAP to watch other community members who might be cooperating with the military or the Civilian Joint Task Force (CJTF).[27] ISWAP intensified executions of those so accused in 2026. The spies are not necessarily members of ISWAP, and their cooperation is purchased as much as coerced.

Interviewees described cash payment for cooperative message delivery and the provision of relief materials to communities after incidents such as fires – along with an explicit threat of execution for cooperating with the military. One interviewee (P1) framed this as a contrast with the state: 'ISWAP is too friendly and kind with communities … On the other hand, the military has no such relationship.' According to this source, the reason that the insurgents are often able to carry out attacks on unprepared military positions, even after moving several kilometres across communities from their hideouts to targets, is that the military struggles to obtain intelligence from communities that are coerced or induced to cooperate with ISWAP.

The *rijal–awam* dynamic is consistent with the considerably larger parallel political economy system in which ISWAP exercises judicial and governing powers over what it considers its own *dawlah,* including the civilian communities trapped within it. Functions are distributed across departments, such as shariah courts, *hisbah* (moral police), finance and taxation, *mustashfa* (healthcare) and others, which communities are forced to relate with as a government of sorts.

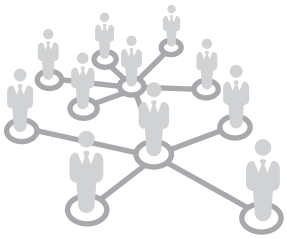
By implication, the insurgents are combining coercion with inducements and services to compete with the state for legitimacy, accentuating their recruitment and revenue logic and making progress in counterinsurgency difficult. Taken together, the *rijal–awam* dynamic is not an isolated intelligence network but a covert security element of a governance system and jihadi state project.

The *rijal* also coordinates logistic functions. For example, the *rijal* distributes cash to community members to separately go to towns such as Geidam and buy petrol in jerrycans. That method avoids easy suspicion that the fuel is for criminal use.

Drones

Origins

Interviewees gave different first-encounter accounts of drones in Boko Haram operations. P1 said the group's first drones were captured from the Nigerian military during a 2014 raid on Gwoza. P2 said the first exposure was to a drone captured from Cameroonian troops after a fight in Kolofata. Both accounts agree on the essentials: 2014 was the approximate exposure point; it was a spoil of war; and Iraqi jihadists helped with training on drone use, first for surveillance rather than combat. The two accounts said fighters were initially confused about what the machine was and photographed it and sent the images to '*dawlah* Iraq' (IS), which then delivered training via Skype.



A HUMAN NETWORK IS THE PILLAR OF ISWAP'S INTELLIGENCE GATHERING

'We then started using [the drone] like a camera … We could see where the enemies were. We were trained on using it by Arabs,' said P1. He recounted a dramatic moment of mutual aerial reconnaissance in Konduga in 2014. 'We were operating near the military,' he said, 'We sent [a drone]; they shot it down. They sent theirs. We shot it down, and we were watching each other.'

As with media skills, of the two Boko Haram successors, it is ISWAP that grew drone capabilities, moving from surveillance and propaganda to combat use. Since at least 2019,[28] ISWAP has been using commercial drones for surveillance, targeting coordination and propaganda. By 2023, the group was already modifying and trialling delivery drones to drop improvised explosive devices (IEDs), according to previous research by the ISS.[29]

From reconnaissance to weaponisation

The weaponisation of commercial drones by ISWAP is recent, but deployment in direct combat has been frequent since the first recorded instance. This happened on 24 December 2024, when the group used four drones to drop locally made grenades in Borno, Nigeria. The target was the army's Forward Operating Base in Wajiroko, Damboa LGA, Borno State, and at least five soldiers were injured.[30] In February 2025, ISWAP launched what it called the 'Camp Holocaust' campaign, which specifically targets poorly resourced military positions across Nigeria and Cameroon. By July of that year, the group had carried out at least 15 successful attacks, according to monitoring by the ISS.[31]

Analysis of the group's tactics reveals the constant use of drones. More attacks have since followed. According to ACLED, between 2024 and February 2026, there were 16 drone incidents, including 10 in direct attacks; the rest were for intelligence and reconnaissance in preparation for ground assault.[32] In January 2026, ISWAP deployed fighters and armed drones to reinforce the ISSP in the coordinated attacks on the Diori Hamani International Airport and Airbase 101 in Niamey, Niger.

According to ex-fighters, the objective of the attacks was to destroy Niger's fleet of drones at the airbase after ISWAP detected that Niamey was monitoring its position in Lake Chad with drones. IS then asked the ISSP to conduct the initial reconnaissance of the airbase, leading to the assaults.[33]

In using drones for attacks, ex-fighters said remote operators guide drones fitted with grenades that were fabricated at the group's workshops (see the following section) over the target. The intention is to gain an aerial view of the 'enemies' and to generate materials for post-battle propaganda. Then the remote control 'is shaken' and explosives are dropped to shock soldiers into disarray. Finally, remote operators coordinate with ground fighters via radio or satellite phones to storm the position with rapid gunfire.[34] Most of those attacks result in heavy losses of state weapons, which ISWAP displays in its propaganda outputs, and help the group to bolster its arsenal.

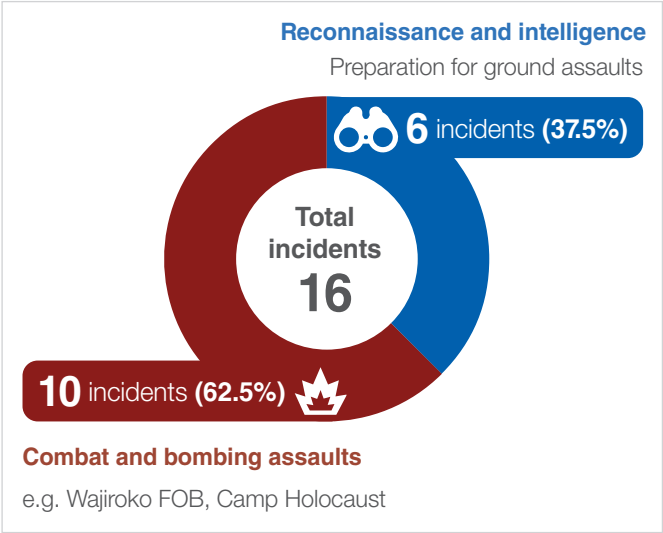
The weaponisation of commercial drones by ISWAP is recent, but deployment in combat has been frequent since the first recorded instance in December 2024

One source (P3), a former drone operator based in Arege, Abadam LGA, Borno, said he belonged to a group of fighters numbering 320, broken into layered sub-groups under a *qaid* (commander). With at least 15 drone operators and eight drones in his group, he said that the ratio is roughly the same for other groups. This highlights a worrying scale and how drone operation is now a specialist role in the insurgent group, with workshops for modification and IED fitting (see the following section).

The use of aerial technology in battlefield operations is a dangerous phase in the insurgency, handing terrorists the advantage to conduct high-impact assaults while minimising their casualties, particularly with military posts remaining under-equipped to defend against such threats.

For a group that is reported as having the highest rate of propaganda outputs among IS affiliates,[35] ISWAP appears to be exercising discretion about its drone programme. The group is not recorded to have brandished or confirmed armed drones in its propaganda materials, unlike JNIM. That silence suggests a further operational security calculation to avoid inviting the countermeasures that publicity could accelerate.

Chart 3: ISWAP drone incidents by mission type, 2024–February 2026



Source: ACLED; ISS interviews

Weapons workshops and fabrication

ISWAP's weapons fabrication programme, including weaponising commercial drones, emerged from an older, more improvised fabrication tradition. P2 traced the origin to the 2013 or 2014 Boko Haram raid on Bama, in which the group stripped the Government Technical College and moved its equipment and tools into the Sambisa Forest. In his account, the group reasoned, 'Yes, we can make things ourselves.' Subsequently, Arab instructors trained fighters in ammunition and IED fabrication as substitutes where standard ordnance was unavailable, P2 said. He continued, 'They told us "If you can't get a real bomb, you can make your own this way."'

He added that fighters were also trained in rigging stolen military vehicles for ramming (vehicle-borne IED) attacks and in constructing suicide vests. In November 2015, the British Broadcasting Corporation (BBC) reported that Boko Haram shared photos of a rocket-making workshop. An inscription on one of the pieces of equipment shows the abbreviation GTCB (for Government Technical College, Bama), appearing to support P2's college raid narrative.[36]

Now, ex-fighters told the ISS that ISWAP has purpose-built workshops in multiple places including Tumbun Magari, which P4 described as a 'garrison town', Tumbun Jakar, Dogon Chiku and Tumbun Allura. Before the December 2024 drone deployment in direct combat, ex-fighters said combat-drone training took place at Tumbun Allura and was conducted by three Arabs: Abu Salma, Abu Jarda and Abu Suleiman. The interviewees could not confirm where the foreign trainers came from.

Explosives are the main outputs of those workshops, including special types that they use to pin to drones with strings. This section deliberately withholds specific technical and procedural steps that interviewees described to avoid producing an open-source, step-by-step account that could be used for illegal, violent purposes. Photos shared by ex-fighters suggest it is Chinese DJI Mavic drones that the group modifies.

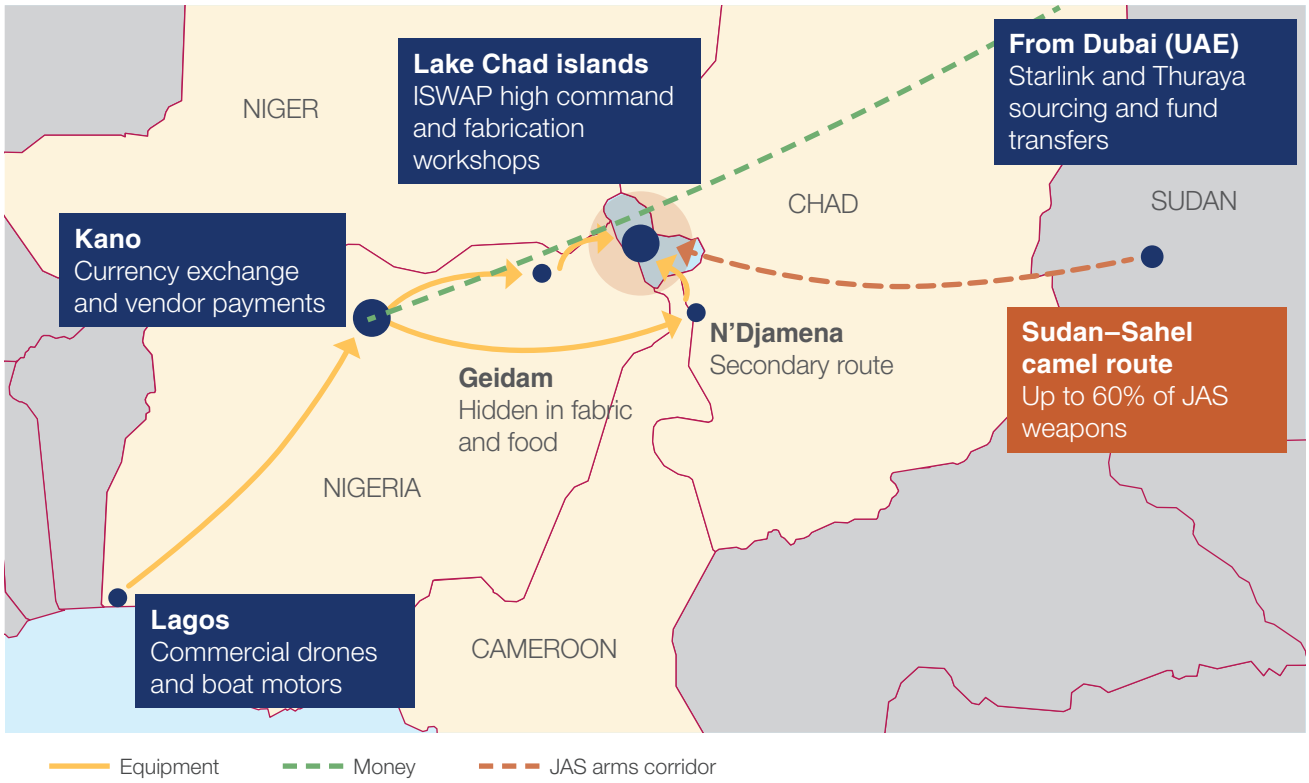
Chart 4: Commercial drone modified by ISWAP



Source: Photo shared by an ex-fighter

Follow-up interviews conducted in August 2026 reveal that ISWAP is continually trying to improve its drone capabilities. To this aim, two new trainers arrived via Libya, Abu Zaid and Abu Fadhil; and a new figure has been appointed to lead the drone operation, Abdurahman Abubakar (Abu Hanifa).

Chart 5: How equipment reaches ISWAP



Source: ISS interviews

Supply chain and financing

The ability to purchase and take delivery of supplies through a network of logistic handlers and channels remains one of the most critical enabling factors for the insurgents. Moreover, the network often intersects with legal economies, making isolation and targeting difficult for governments. Based on interviews, northwest Nigeria's Kano and commercial city Lagos are central to ISWAP's supplies of equipment such as drones, camcorders, boat motors, satellite communication devices and other items that cannot be easily sourced locally. In some cases, certain pieces of equipment, particularly Thuraya and Starlink devices, are moved from Dubai, United Arab Emirates (UAE), where they are reportedly registered, to Kano through currency exchange networks between the two cities.

Interviewees separately credited a Kano-based currency exchange operator named Alhaji Surajo for helping the insurgents to move goods from the UAE to Kano. From Kano, the items would pass through liaisons, tucked into other goods such as bundles of fabrics and food, via towns like Geidam in Yobe State, to villages and local markets where ISWAP members or their agents take delivery. Goods such as DJI Mavic drones, boat motors and media tech items sourced commercially from Lagos follow the same route through Kano. The group also sources these items from N'Djamena, according to ex-fighters.

The involvement of the currency exchange operators in the supply chain is mainly because they help to facilitate payments to vendors and the transfer of cash between IS and ISWAP, interviewees said. Usually, the operators are motivated by the excessive gains they make when they help the insurgents; they typically charge far above market rates. N'Djamena is another point through which ISWAP's supplies are routed, particularly after counter-terrorist financing efforts started targeting the Kano route agents. In August 2025, Chadian police announced the arrest of Muslim Yusuf, son of Boko Haram founder Mohammed Yusuf, in N'Djamena along with five others including logistics and mobility operators.[37]

In 2022, the Nigeria Sanctions Committee listed 13 individuals and three firms with physical addresses in Kano for terrorism financing.[38] Six of them were currency exchange operators and had been convicted and jailed in the UAE in 2021 for helping terrorists to facilitate financial transactions between Dubai and Nigeria. One of them was Surajo Abubakar Mohammed, although it is not confirmed whether he is the same individual that the interviewees named Alhaji Surajo. The ex-fighters could identify the operator only by a single name and the title '*Alhaji*', used by Muslims who have embarked on pilgrimage to Mecca.

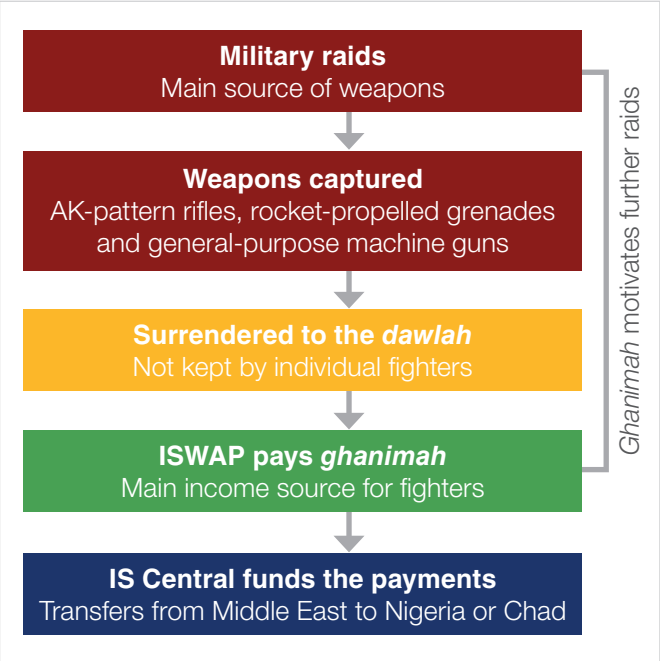
Then, in June 2026, the US imposed sanctions on a Nigerian individual and his three currency exchange firms, saying they 'materially assisted, sponsored, or provided financial, material, or technological support for, or goods and services to or in support of, ISIS-West Africa.'[39]

Weapons sourcing follows a largely distinct pattern. Ex-fighters said ISWAP's weapons, including AK-pattern rifles, rocket-propelled grenades and general-purpose machine guns, are mostly from military raids, rooted in the early Boko Haram method of storming police stations to capture weapons. Captured weapons are then surrendered to the *dawlah,* rather than retained by individual fighters. The ex-fighters said that ISWAP pays for the surrendered battlefield captures, called g*hanimah.*

Those payments are the main source of income for fighters, a key motivation for targeting military positions. IS pays for the surrendered weapons, moving money between the Middle East and Nigeria or Chad, according to ex-fighters and a source with inside information on ISWAP's finances. A senior Nigerian intelligence source confirmed the loss of weapons to terrorists: 'At a time, it was as if we were handing weapons to ISWAP.' Besides spoils, ex-fighters said ISWAP's weapons are also smuggled through N'Djamena.

By contrast, JAS thrives on civilian predation and relies only marginally on captured weapons since it conducts far fewer attacks on military positions. Rather, its leader Bakura Doro is directly responsible for sourcing up to '60 percent' of the group's weapons through Sudan–Sahel illicit arms networks, according to interviewees. P1, who had a brief stay with Bakura, could only describe camel-riding groups from Sudan as Bakura's suppliers.

Chart 6: The *ghanimah* system



Source: ISS interviews

From his Barwa island in Niger, Bakura is, in turn, the principal source of weapons to his JAS structures. These include the Mandara Mountains across Nigeria and Cameroon, led by Aliyu Ngulde; Darrul Ghazwah in the Bama and Banki areas of Borno, led by Alhaji Kale; and northwest and central Nigeria, led by Abubakar Saidu (Sadiku).[40]

Niger's March 2025 withdrawal from the MNJTF, the region's primary coordinating mechanism, benefits insurgent groups whose supply and logistics networks move across the Lake Chad Basin borders. The effect is especially significant because of Niger's geography. The country lies between central Sahel, the Lake Chad Basin and coastal West Africa through Nigeria and Benin. This position makes Niger a key transit corridor from central Sahara, including from Libya and Algeria. As a result, Niger is one of the region's most strategically important border spaces for both insurgent logistics and counterinsurgency coordination.

Slow reactive state response

The Lake Chad Basin countries had slightly earlier exposure to drones than Boko Haram did, even if through foreign military assistance.[41] In May 2014, the US deployed

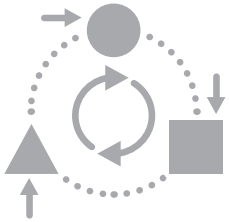
80 troops and a surveillance drone flying from Chad to help locate the Chibok schoolgirls kidnapped by Boko Haram in Nigeria. That was followed more than a year later by a fleet of unarmed American Predator drones sent to Cameroon to conduct surveillance across the Lake Chad region.

If the claims by P1 and P2 that Boko Haram captured drones from Cameroonian and Nigerian forces in 2014 are correct, the countries must have been integrating some drones since 2014. But it was in February 2016 that Nigeria first used an armed drone against the insurgents, according to an official confirmation at the time.[42] The drone was likely from the Chinese CH-3A fleet that Nigeria had acquired in 2014, when the Obama administration was reluctant to directly support Nigeria at the peak of the Boko Haram insurgency over human rights concerns.[43]

Despite their earlier exposure, the militaries of the Lake Chad Basin countries and the MNJTF are now in a reactive mode, having failed to proactively utilise available intelligence to dismantle ISWAP's drone programme before it became a real threat. They allowed ISWAP to raise its capabilities for using drones from propaganda and intelligence to direct combat over many years – even when there were warnings that the group was trialling armed commercial drones.[44]

Speaking at the January 2025 Lake Chad Basin Governors' Forum summit in Maiduguri, the then-commander of the MNJTF, Major-General Godwin Mutkut, acknowledged the threats posed by ISWAP's drones.[45] In addition, he recognised the lack of counter-drone technology, including jamming systems, which leaves security forces and civilians vulnerable to aerial threats. That was just in the wake of ISWAP's first drone deployment for combat, but before the end of that year, the group had used the technology to dislodge military bases multiple times.

Lake Chad Basin countries and the MNJTF are now in a reactive mode, having failed to proactively utilise available intelligence to dismantle ISWAP



ISWAP HAS CONVERTED COMMERCIAL AND ORDINARY CIVILIAN TOOLS INTO INSTRUMENTS OF WAR

In July 2025, the Nigerian Air Force announced specialised training for its personnel on the 612 anti-unmanned aerial vehicle radar system.[46] In addition, the army started fielding the Lithuanian-made EDM4S SkyWiper, a handheld jammer that severs radio link between a drone and its remote operator.[47] Officials (including P10, P11, P12 and P14) mentioned expanded training in detecting and tracking aerial threats, along with intelligence-gathering support from the United States Africa Command team based in an airfield in Bauchi.[48] The officials, however, complained of poor funding and slow procurement processes for equipment needed to accelerate response to the insurgents. During several closed-door security roundtables in Abuja and N'Djamena in 2026, military officials still lamented over the challenge of effective response to the terrorists' drone threat.

AI horizon: unconfirmed but may be close

The Cambridge Programme on AI Science and Policy interviewed 27 former Boko Haram members in northeast Nigeria between 2025 and 2026. The study found that both ISWAP and JAS operatives use frontier artificial intelligence (AI) chatbots. The tools are reportedly used to assist in combat and day-to-day operations, including ISWAP fighters using AI to learn how to breach military defensive trenches and to maintain stolen equipment. The study concludes that AI adoption by these groups 'has been significantly underestimated in both scope and character,' and quoted a former commander, giving the report its title: 'God has helped us, and so will AI.'[49]

However, during interviews, including follow-up sessions in July and August 2026, none of the respondents said ISWAP or JAS currently use AI. Given how candidly and specifically interviewees described other technologies, such as Thuraya, Starlink, drone rigging, IED fabrication and Skype calls with IS Central, the silence on AI, as well as replying 'no' to questions on its use in follow-up interviews, is likely informative. If AI tools were employed as operational infrastructure, the interviewees would likely have mentioned them.

That said, silence does not make the prospect of AI adoption absent or remote, considering the demonstrated adaptability and innovativeness of ISWAP in particular. Furthermore, ISWAP hosts foreign jihadists, including those described as medical doctors and engineers, as well as local members with formal education, including those who teach in its children's schools. These foreigners and local teachers are expected to have some IT exposure.

Therefore, while evidence is scarce that AI is currently institutionalised and deployed as an operational infrastructure, it could be a matter of time. When one ex-fighter wanted to show the author the Starlink device he said ISWAP uses, he Googled it and an AI summary appeared at the top. Any fighter who can use the Google search engine could engage the AI function further. This trend aligns with ISS interviews with ex-fighters on the Cameroonian side of the Lake Chad Basin, who said they learned through Google searches in addition to in-person training.

The crucial point is that, evidenced by its history and ambition, ISWAP can spot a vulnerability in its current position, search for a tool that addresses it, acquire that tool through whatever informal network is available and adapt it for use within a relatively short cycle.

Conclusion and recommendations

While technology is at its core, this report is, in essence, about an organisational culture that enables adaptation, survival and even the outpacing of counterstrategies, assisted by external linkages that distinguish ISWAP's trajectory from its rival JAS's. ISWAP has converted commercial and ordinary civilian tools into instruments of war, seriously tested the capacity of state militaries, and competed with governments for legitimacy and resources.

This is because the insurgent group builds structures: supply networks, the *Ilan*, the *rijal–awam* network, the *ghanimah* pricing system and the drone programme. Therefore, while sustained military pressure has yielded results over the years, such as reducing insurgent territorial control from the peak 2014–2015 scale, the insurgency remains strong and operationally capable, with an entrenched parallel governance system. That is because the structural ecosystem that enables it has not been dismantled.

This report documents one critical dimension of that enabling ecosystem, namely the acquisition, adaptation and institutionalisation of technology across communications, intelligence gathering, and combat. Understanding how that capability was built and continues to be built – by who, through which networks, financed through which channels, sustained through which organisational structures – is a condition for countering it effectively. It is necessary to note that every capability described in this report began as something that the state did not take seriously until it became difficult to neutralise. The same pattern now presents itself with AI.

Countering ISWAP's technology programme – and pre-empting JAS' progress before it closes the capability gap – requires responses that are calibrated to the actual architecture of the threat. The following recommendations are addressed to specific stakeholders and the structural vulnerabilities that each is meant to address.

For military and counterinsurgency operations:

Use defector intelligence systematically. This report is substantially based on interviews with recent defectors, several of whom left between 2024 and 2026. Thousands exited the insurgency through the various defection and reintegration programmes across the four Lake Chad Basin countries. The integration of some ex-fighters into tactical counterinsurgency operations is acknowledged, such as Hybrid Force members and military informants in Borno. But this report argues that ex-fighters are a much more significant intelligence resource for offering specific information on identifying the locations of key insurgent facilities and individuals – a resource that is currently underutilised.

The MNJTF and national operations should establish dedicated debriefing protocols for defectors exiting the insurgency through the deradicalisation programmes: covering technology use, workshop locations, supply routes and personnel. Cooperating sources should be protected adequately enough that others are willing to follow. The information in this report is one illustration of what a structured programme can yield.

Acquire inside assets. With all its operational security practices, ISWAP is vulnerable to compromises among its rank-and-file members, particularly those forcibly recruited or those with grievances from gaps in expectations of benefits and important roles. Following conversations with ex-fighters, it is understood that certain jihadists are aggrieved or ideologically infirm and can defect with some incentives, which may be considered if their defection translates to substantial security outcomes. Some can remain within the insurgent group and offer specific intelligence needed for targeted strikes. For context, the May 2026 strikes were built on intelligence sourced from compromised insiders, acquired by the American team.

Strike the identified facilities. Intelligence-led information should lead to strikes against facilities and key individuals. The US–Nigeria joint strikes of May 2026 demonstrated the kind of impact that this report recommends. But ISWAP's quick operational recovery demonstrates that one-off decapitation strikes yield only temporary disruption. Persistent, intelligence-led targeting of key individuals, including foreign trainers, and physical infrastructure is what generates effective degradation.

Strengthen naval and amphibious presence. The Lake Chad islands are the locations of ISWAP's high command and key facilities, and they also host JAS's leadership, enabling the two groups to plan and coordinate resources. Except for the May 2026 strikes, most of these locations are left undisturbed despite ongoing counterinsurgency operations; this should not continue. In addition to targeted aerial offensives, which erase the advantage that the terrain offers the insurgents against ground troops, naval and amphibious operations should be strengthened in the lake area to put pressure on the insurgents at their core base.

Target the *ghanimah* pricing structure. One of this report's most significant findings is that ISWAP fighters are not motivated by ideology alone when attacking military positions. They are also motivated by income. The *ghanimah* system means that a poorly defended, weapons-heavy military position is both a tactical target and a paycheck. Strengthening military bases with more personnel and increased defence equipment, as well as quick reinforcement and aerial support coordination, would directly reduce the financial incentive that drives ISWAP's targeting pattern.

Invest in counter-drone capability ahead of demonstrated need. The MNJTF commander's January 2025 acknowledgement that his forces lacked counter-drone technology came weeks after ISWAP's first confirmed armed drone use, and months before the group had used the same capability repeatedly. There are current efforts to improve counter-drone capability, but procurement cycles need to be faster. Officials interviewed for this report described 'poor funding and slow procurement processes' as the primary bottleneck. Counterinsurgency budgets should reflect the drone threat as it currently exists.

Map and monitor Boko Haram-active areas and the routes leading there. There should be a state-of-the-conflict assessment to map the areas where the insurgents are active, temporarily putting aside the political risks of acknowledging Boko Haram's territorial influence. The routes leading to those places and the local markets close to them should be monitored against illicit traffic and trading. Research has shown that thousands of traders travel to Boko Haram–controlled

areas for fishing, which provides the insurgents with a huge war chest to procure the equipment they need.

Their continued access to fuel powers the group's mobility and fabrication machinery. Therefore, movements on the identified routes should be monitored, while mitigating the risk of adverse community impact.

Strengthen counter-intelligence at community level. ISWAP's *rijal–awam* system functions because it is embedded in a governance and service structure, alongside coercion. Sustainable counter-intelligence at the community level requires offering genuine alternatives, backed with security to de-risk cooperation with the military and to integrate certain assessed community members into an intelligence and early-warning pipeline. This strategy can enable the identification of ISWAP's spies and logistics handlers to disrupt the group's intelligence-gathering and parallel political economy systems. This is a security task as much as it is a civilian governance and stabilisation one.

For information and communications authorities:

Stay ahead of insurgent narratives. This report documents in granular detail the propaganda work of ISWAP's media department. This includes how it monitors military press releases, assesses them for misrepresentation and deploys back channels to journalists and researchers in near real-time. Countering that system requires rapid-response communication that is visual-rich, transparent and frankly acknowledges losses when they occur, since claiming otherwise is the credibility gap that ISWAP exploits.

Engage social media companies and newsrooms. Regulatory commissions should pursue cooperation with social media and messaging platforms to enhance their systems against extremist propaganda. Similarly, specific engagements with newsrooms on conflict-sensitive reporting are also needed to encourage exercising discretion in using insurgent propaganda usually pushed through informal contacts that newsrooms have taken as sources.

Work with foreign regulatory authorities on satellite communication. The 2013 Thuraya ban pushed procurement and supplies underground. The more productive approach is to engage with foreign governments that have regulatory powers over Thuraya and SpaceX. That would involve having the companies monitor the usage of their devices against use in the conflict-affected areas, thereby countering the practice of diverting devices registered elsewhere with different user information to insurgents. This can also create an intelligence trail and will affect the insurgents' operational security.

Engage local drone dealers and manufacturers. These businesses must be included in the national security conversation to develop a customer due diligence approach and to mitigate the risk of using drones for violent purposes. Local drone manufacturing capacity is emerging in Nigeria, which enhances the opportunity to counter the insurgents. Without tight regulations, however, this also poses the risk of making drones more easily accessible for criminal purposes.

For financial regulators and financial intelligence units:

Counter the financing of terrorism and treat currency exchange networks as a strategic priority. There are already cases of identified operators who have been sanctioned or convicted for Boko Haram financing, but sustained, pattern-level monitoring is required. Sources say IS Central moves substantial funds, often facilitated by currency exchange networks, to its African affiliates, who are incentivised by above-market margins to help move equipment.

Clamping down on those networks will affect ISWAP's ability to access the funds it needs to pay fighters for surrendered captured weapons and operational equipment such as satellite communication devices. Currency exchange operators should be specifically required to flag and report large or structured Middle East–origin transactions moving towards the Lake Chad Basin territories.

For civilian protection and humanitarian actors:

Recognise technical literacy as a specific abduction risk factor in communities. This report documents that ISWAP deliberately and forcibly targets civilians with certain technical skills. P5 was taken from Pulka specifically because he was a professional photographer, and JAS, too, released P1 after he was taken prisoner from ISWAP because of his media skills. Young people with noticeable technical skills in border

communities face a distinct threat that is not currently captured in most conflict sensitivity frameworks. Communities should be made aware of this practice as a protective measure.

For regional bodies and international partners:

Restore MNJTF coordination as a matter of operational urgency. Niger's March 2025 withdrawal from the MNJTF has created a direct operational consequence. JAS leader Bakura operates from the Barwa island of Niger, from where he supplies weapons to his structures across the region. ISWAP has also been expanding its regional reach, thus reinforcing the ISSP, and its supplies follow transborder routes including in Niger, which has withdrawn from the primary coordinating mechanism. The fragmentation benefits the insurgents, who gain the most from ungoverned border spaces. Diplomatic efforts to restore MNJTF cooperation, or to build the bilateral substitutes adequate to cover the Niger border specifically, should be treated as a counterinsurgency operational priority.

Treat ISWAP's drone and technology programme as an IS-network problem. Degrading ISWAP's capabilities requires IS-network intelligence. Intelligence services tracking IS financing and knowledge and technology transfer in the US, Europe and the Middle East hold information that is directly relevant to the threats in the Lake Chad Basin. Intelligence sharing and capacity enhancement assistance towards the Lake Chad Basin counterinsurgency services should be considered an important element of the international fight against terrorism.

Engage AI companies. ISWAP's history of innovation and adoption suggests that the absence of current confirmed AI use is not a reason for complacency. JAS, which lacks the kind of external assistance that is available to ISWAP, may want to lean on AI to close the gap. Before the technology becomes a confirmed operational threat, AI companies should be engaged and required to enhance their systems against misuse for violent purposes. This is also a recommendation for national regulatory agencies.

Notes

1 Lake Chad Basin Commission, Regional strategy for the stabilisation, recovery and resilience of Boko Haram-affected areas in the Lake Chad Basin, 2026, https://cblt.org/download/regional-strategy-for-the-stabilization-recovery-resilience-of-the-boko-haram-affected-areas-in-the-lake-chad-basin-region-rs-srr2-0/.

United Nations Development Programme, Regional Stabilisation Facility for the Lake Chad Basin Region Report 2021–2024, https://www.undp.org/sites/g/files/zskgke326/files/2026-04/rsf_report_final.pdf.

2 Boko Haram is the umbrella name for the networks of violent jihadists in the Lake Chad Basin, formally known as Jama'tu Ahlis Sunna Lidda'awati wal-Jihad (JAS), founded by Mohammed Yusuf in Maiduguri, northeast Nigeria in the early 2000s. Following a 2009 uprising triggered by a police confrontation over the enforcement of a Borno State law requiring motorcyclists to wear helmets, the founder was killed. The movement, also known as Yusufiya, so-named after the founder, turned into a violent insurgency and later spread to Cameroon, Niger and Chad between 2013 and 2015.

3 Led by Yusuf's successor Abubakar Shekau, Boko Haram pledged allegiance to the Islamic State to become Islamic State West Africa Province (ISWAP) in March 2015. But in August 2016, IS backed a breakaway faction led by Abu Musab al-Barnawi (Habib Yusuf, son of founder Yusuf), Mamman Nur and others, citing Shekau's indiscriminate killing of Muslim civilians, which violated IS doctrine. The breakaway faction retained the ISWAP brand, and Shekau's remaining loyalists reverted to the JAS label. Shekau killed himself in June 2021 during a confrontation with ISWAP fighters.

International Crisis Group, JAS vs. ISWAP: the war of the Boko Haram splinters, Africa Briefing N°196, 28 March 2024, https://www.crisisgroup.org/brf/africa/west-africa/nigeria/b196-jas-vs-iswap-war-boko-haram-splinters.

A Dahiru, Imported from Egypt: the extremist ideology that inspired Boko Haram, HumAngle, 31 August 2026, https://www.humanglemedia.com/imported-from-egypt-the-extremist-ideology-that-inspired-boko-haram.

4 The Azawad Liberation Front (Front de Libération de l'Azawad, FLA) is a Tuareg-led coalition operating in northern Mali that has reportedly received drone-warfare training and tactical support from Ukrainian military intelligence.

The Arab Weekly, Ukraine-Russia war tactics seep into Mali's desert as Tuareg get help from Kiev, 7 October 2025, https://thearabweekly.com/ukraine-russia-war-tactics-seep-malis-desert-tuareg-get-help-kiev.

B Phillip, Drones are transforming the Sahel conflict. Here's how, Fronts.co, 6 July 2026, https://fronts.co/article/drones-are-transforming-the-sahel-conflict-heres-how/.

5 As used in the report, the term 'adaptive technology programme' is the author's own conceptualisation. It describes the full strategic and organisational process by which ISWAP has identified, acquired, modified and institutionalised civilian and commercial technologies across all three domains that this report examines. By contrast, 'dual-use technology' refers to the inherent properties of a technology that make it applicable to both civilian and military purposes, but this term does not address organisational adoption or learning by armed groups. 'Improvised weaponisation' refers to the physical conversion of non-weapons materials for combat use and may not encompass communications dimensions.

J Grove, An insurgency of things: foray into the world of improvised explosive devices, International Political Sociology, 10:4, 2016, 332–351, https://doi.org/10.1093/ips/olw018.

OO Awotayo, The DIY age of weapons, Nigerian Defence Academy Journal of Military Science and *Disciplinary Studies*, 4:1, 2026, 15–24, https://fmsisndajournal.org.ng/index.php/new-ndajmsis/article/view/117/40.

P Violakis, Weaponising innovation: how civilian technologies fuel modern warfare, Insights, Rabdan Academy, 16 December 2024, https://www.researchgate.net/profile/Petros-Violakis-2/publication/387867565_Weaponising_Innovation_How_Civilian_Technologies_Fuel_Modern_Warfare/links/678029087934b95644aea1d8/Weaponising-Innovation-How-Civilian-Technologies-Fuel-Modern-Warfare.pdf.

6 K Allen, Drones: a propaganda tool for Africa's armed groups?, ISS Today, 3 June 2025, https://issafrica.org/iss-today/drones-a-propaganda-tool-for-africa-s-armed-groups.

T Adebayo, Lake Chad Basin insurgents raise the stakes with weaponised drones, ISS Today, 17 March 2025, https://issafrica.org/iss-today/lake-chad-basin-insurgents-raise-the-stakes-with-weaponised-drones.

7 In an expert comment, ACLED's analyst for Africa, Ladd Serwat, said, '[ISWAP is] the most prolific IS affiliate in Africa to engage in drone warfare,' with 16 recorded drone incidents since 2024 (10 attacks, six surveillance missions). He continued, 'ACLED records over 100 cases of drone violence by JNIM since the group began using this technology in 2023.'

L Serwat, Reported drone use in the Niamey airport attack is the first-ever by ISSP in Niger, ACLED, 2 February 2026, https://acleddata.com/expert-comment/reported-drone-use-niamey-airport-attack-first-ever-issp-niger.

8 Africa Defense Forum, Attack on Kenya defence forces outpost confirms al-Shabaab drone use, 25 July 2023, https://adf-magazine.com/2023/07/attack-on-kenya-defence-forces-outpost-confirms-al-shabaab-drone-use/.

N Kurt, Weaponised skies: the expansion of terrorist drone use across Africa, Global Network on Extremism and Technology, 30 July 2025, https://gnet-research.org/2025/07/30/weaponised-skies-the-expansion-of-terrorist-drone-use-across-africa/.

9 Reuters, Rebels claim drone attack on Congo's Kisangani airport, 2 March 2026, https://www.reuters.com/world/africa/congos-kisangani-airport-attacked-by-suspected-rebel-drones-authorities-say-2026-03-02/.

10 Club of Mozambique, Mozambique attacks: government says armed groups wear army uniforms and use drones, 27 May 2020, https://clubofmozambique.com/news/mozambique-attacks-government-says-armed-groups-wear-army-uniforms-and-use-drones/.

11 N Allen, Digital technology, strategic adaptation, and the outcomes of twenty-first century armed conflict, Carnegie Endowment for International Peace, 17 June 2025, https://carnegieendowment.org/research/2025/06/digital-technology-strategic-adaptation-and-the-outcomes-of-twenty-first-century-armed-conflict.

12 T Adebayo, Lake Chad Basin's military bases in ISWAP's crosshairs, ISS Today, 14 July 2025, https://issafrica.org/iss-today/lake-chad-basin-s-military-bases-in-iswap-s-crosshairs.

13 ISWAP structures its so-called *dawlah* (state) into provinces called *wilayas*, which are further divided into *mantiqas*, meaning administrative or operational districts. The Buhaira *wilaya* has Tumbuma, Banki and Buhaira *mantiqas*; the Faruq *wilaya* has Sambisa and Timbuktu *mantiqas*; and the Nigeria *wilaya* covers the rest of Nigeria.

14 Bakura Doro, also known by the *nom de guerre* Abu Ummaima, is the current leader of JAS. He is reportedly based in Barwa island in Niger's part of Lake Chad and is the primary arms supplier for JAS structures extending from the Lake Chad Basin to northwest and central Nigeria.

T Adebayo, JAS resurgence deepens Lake Chad Basin's complex security crisis, ISS Today, 11 September 2025, https://issafrica.org/iss-today/jas-resurgence-deepens-lake-chad-basin-s-complex-security-crisis.

15 Ukba was said to be one of the earliest jihadist associates of Mohammed Yusuf. Around 2012, he reportedly helped bring the funds that al-Qaeda donated to Boko Haram, amounting to US$200 000. That money caused disagreement within the group as some wanted it to be used to support the families of slain jihadists and set up businesses to finance the jihad, while Shekau disagreed, preferring arms purchase instead. Those who disagreed with Shekau and also accused him of theological deviation, then broke away to form what is now known as Ansaru in northwest Nigeria.

16 Formally affiliated with al-Qaeda since 2007, AQIM operates across the Sahara–Sahel region and has trained jihadist operatives from across West Africa. As interviewees note, trainees include some early Boko Haram media and communication figures such as Ukba and Baba Hassan.

17 A report says Habib Yusuf died in 2023 after triggering an explosive vest to evade arrest in a Kaduna house that he was hiding in. His reported death has never been acknowledged by IS, nor by any of the Lake Chad Basin countries.

A Salkida, Ideology, blood and war: rethinking the origins of Boko Haram, HumAngle, 23 April 2026, https://www.humanglemedia.com/ideology-blood-and-war-rethinking-the-origins-of-boko-haram.

18 The Islamic State's Shura Council (Majlis al-Shura) is the principal consultative and legislative body of the organisation, responsible for approving major strategic and doctrinal decisions. Habib Yusuf was a member of this council, representing the African affiliates.

19 Boko Haram founder Mohammed Yusuf was extrajudicially killed in police custody following the 2009 Boko Haram uprising that was triggered by a police confrontation over the enforcement of a Borno State law requiring motorcyclists to wear helmets.

20 See note 3.

21 This operation was a joint campaign by the MNJTF in 2024 to clear Boko Haram fighters from the Lake Chad Basin.

22 Interviewees disclosed use of Starlink.

23 M Samuel, ISWAP's use of tech could prolong Lake Chad Basin violence, ISS Today, 13 April 2023, https://issafrica.org/iss-today/iswaps-use-of-tech-could-prolong-lake-chad-basin-violence.

24 O Audu, JTF bans Thuraya phones in Borno, others, says Boko Haram use them for attacks, Premium Times, 19 June 2013, https://www.premiumtimesng.com/news/139116-jtf-bans-thuraya-phones-in-borno-others-says-boko-haram-use-them-for-attacks.html.

25 N Allen, op. cit. (note 11).

26 N Allen, op. cit. (note 11).

27 The CJTF is a civilian vigilante organisation established in 2013 in Maiduguri by residents resisting Boko Haram. It is now state armed and formally operates alongside the Nigerian security forces, providing local intelligence and joining in combat operations.

28 E Searcey, Boko Haram is back. With better drones,, The New York Times, 13 September 2019, https://www.nytimes.com/2019/09/13/world/africa/nigeria-boko-haram.html.

29 M Samuel, ISWAP's use of tech could prolong Lake Chad Basin violence, ISS Today, 13 April 2023, https://issafrica.org/iss-today/iswaps-use-of-tech-could-prolong-lake-chad-basin-violence.

30 T Adebayo, Lake Chad Basin insurgents raise the stakes with weaponised drones, ISS Today, 17 March 2025, https://issafrica.org/iss-today/lake-chad-basin-insurgents-raise-the-stakes-with-weaponised-drones.

31 T Adebayo, op. cit. (note 12).

32 L Serwat, op. cit. (note 7).

33 ISSP, previously known as the Islamic State in the Greater Sahara (ISGS), was formally recognised by IS Central as a distinct province in 2022. It operates primarily in the tri-border area of Mali, Niger and Burkina Faso, and has recently pushed into northwest Nigeria. The January 2026 Niamey attacks represent the first confirmed instance of ISWAP providing operational reinforcement to ISSP, indicating the cross-regional mobility and coordination of the IS affiliates.

T Adebayo, Fragmented security allows terrorists' cross-mobility across Lake Chad and Sahel, ISS Today, 27 July 2026, https://issafrica.org/iss-today/fragmented-security-allows-terrorists-cross-mobility-across-lake-chad-and-sahel.

L Serwat, Reported drone use in the Niamey airport attack is the first-ever by ISSP in Niger, ACLED, 2 February 2026, https://acleddata.com/expert-comment/reported-drone-use-niamey-airport-attack-first-ever-issp-niger.

34 A similar tactic has been recorded in the Sahel.

B Phillip, Drones are transforming the Sahel conflict. Here's how, Fronts.co, 6 July 2026, https://fronts.co/article/drones-are-transforming-the-sahel-conflict-heres-how/.

35 A Palmer, The killing of Abu-Bilal al-Minuki and the U.S. military's deepening involvement in Nigeria, Critical Questions, Centre for Strategic and International Studies, 18 May 2026, https://www.csis.org/analysis/killing-abu-bilal-al-minuki-and-us-militarys-deepening-involvement-nigeria.

36 BBC News, Nigeria's Boko Haram reveals rocket-making factory, 3 November 2015, https://www.bbc.com/news/world-africa-34703173.

37 R Hoinathy, Time to double down after security strikes against Boko Haram leaders, ISS Today, 20 October 2025, https://issafrica.org/iss-today/time-to-double-down-after-security-strikes-against-boko-haram-leaders.

O Dunamis, Boko Haram founder's son, others arrested in Chad, Premium Times, 19 August 2025, https://www.premiumtimesng.com/regional/nnorth-east/815153-boko-haram-founders-son-others-arrested-in-chad.html.

38 Nigeria Securities and Exchange Commission, Circular on designation of ten individuals and three entities by the National Sanctions Committee and addition to the Nigeria sanctions list, 10 November 2022, https://sec.gov.ng/for-investors/keep-track-of-circulars/circular-on-designation-of-ten-individuals-and-three-entities-by-the-national-sanctions-committee-and-addition-to-the-nigeria-sanctions-list/.

39 U.S. Department of the Treasury, Treasury targets ISIS facilitators and disrupts terrorist financial networks, 22 June 2026, https://home.treasury.gov/news/press-releases/sb0537.

40 T Adebayo, JAS resurgence deepens Lake Chad Basin's complex security crisis, ISS Today, 11 September 2025, https://issafrica.org/iss-today/jas-resurgence-deepens-lake-chad-basin-s-complex-security-crisis

41 C Whitlock, Pentagon setting up drone base in Africa to track Boko Haram fighters, The Washington Post, 14 October 2015, https://www.washingtonpost.com/world/national-security/pentagon-setting-up-drone-base-in-africa-to-track-boko-haram-fighters/2015/10/14/0cbfac94-7299-11e5-8d93-0af317ed58c9_story.html.

42 Daily Sabah, For the first time, Nigeria hits Boko Haram targets with drones, 3 February 2016, https://www.dailysabah.com/africa/2016/02/03/for-the-first-time-nigeria-hits-boko-haram-targets-with-drones.

43 Military Africa, Nigeria military drones (UAV) – a complete list, 28 October 2020, https://www.military.africa/2020/10/nigerian-military-drones-uav-current-army-air-force-and-navy-uav-inventory/.

44 E Lionel, Counter-UAV: Africa playing catch-up despite risks of drone threat, Military Africa, 13 April 2023, https://www.military.africa/2023/04/counter-uav-african-militaries-playing-catch-up-despite-presence-of-drone-threat/.

Africa Defense Forum, Militaries lag in counter-drone technology, 18 August 2026, https://adf-magazine.com/2026/08/militaries-lag-in-counter-drone-technology/.

45 The author witnessed and recorded the commander's presentation at the opening ceremony of the 2025 Lake Chad Basin Commission Governors' Forum Summit in Maiduguri, 29 January 2025.

46 N Musa, NAF launches anti-drone training of personnel for counter-terrorism operations in North-East, The Guardian, 28 July 2025, https://guardian.ng/news/nigeria/metro/naf-launches-anti-drone-training-of-personnel-for-counter-terrorism-operations-in-north-east/.

47 Military Africa, Nigerian Army fields Lithuanian C-UAV against insurgents' drones, 18 March 2025, https://www.military.africa/2025/03/nigerian-army-fields-lithuanian-c-uav-against-insurgents-drones/.

48 O Ogunseyin, US trains Nigerian forces in advanced combat, drone operations, The Guardian, 25 August 2026, https://guardian.ng/news/nigeria/national/us-trains-nigerian-forces-in-advanced-combat-drone-operations/.

49 A Juelich, 'God has helped us, and so will AI': how the terrorist group Boko Haram uses frontier AI, Cambridge Programme on AI Science and Policy, University of Cambridge, July 2026, https://casp.ac/reports/ai-enabled-terrorism.

Glossary

Amaq: Meaning 'depths' in Arabic, this is IS's official global news outlet (full name: *Amaq News Agency*). Established in 2014, it functions as the primary channel through which IS publishes attack claims and distributes propaganda and combat footage from IS affiliates including ISWAP.

Awam: This means 'the common people' or 'the public' in Arabic. In ISWAP's governance terminology, *awam* refers to the civilian communities living under or adjacent to ISWAP's areas of influence and control, as distinct from ISWAP members, fighters and officials. The *awam* are simultaneously the subjects of ISWAP's parallel administration, the source of its ground-level intelligence, and the population whose cooperation it purchases and coerces.

Dawlah: Meaning 'the state' or 'the government,' it is used by ISWAP fighters and officials as shorthand for two related things: IS Central in the Middle East (referred to as '*dawlah* Iraq') and ISWAP's own aspirational parallel state project in the Lake Chad Basin. The term carries both a descriptive meaning (the IS organisation) and a political-ideological one (the Islamic state as a governance project to be built).

Ghazwah: This means 'raid' or 'military expedition' in Arabic. In this report, it is the name of a specific JAS territorial structure in the Bama–Banki areas of Borno, led by Alhaji Kale and operating under the command of JAS leader Bakura Doro. It is populated by fighters who fled Sambisa Forest after Shekau's death and refused to pledge allegiance to ISWAP. It operates mostly as a gang of bandits using religious ideology for cover, while routinely robbing and kidnapping civilians for ransom.

Ghanimah: This means 'spoils of war' or 'war booty' in Arabic. In ISWAP's operational context, it refers specifically to the institutionalised system under which fighters are required to surrender weapons captured in military raids to the *dawlah*, which then pays them a fixed price set by IS, which also provides the payout funds.

Ilan (or *Maktabatur Ilan*): This means 'the media office' or 'information bureau'.

Mantiqa: This simply means 'regions' or 'zones'. ISWAP divides its operational territory into administrative zones called *mantiqas*, each with their own subordinate command structures. The Buhaira *mantiqa* covers the Lake Chad islands, where ISWAP's high command and key facilities are concentrated.

Mustashfa: This means 'hospital' or 'healthcare facility' and is how ISWAP describes its health department.

Qaid: This is a 'commander'. In ISWAP's military structure, a *qaid* commands an operational fighting unit described by interviewees as consisting of approximately 320 fighters. A *qaid* reports to a *fiya*.

Rijal amni: 'Security men' or 'security agents'. The formal name for ISWAP's internal state security department, responsible for deploying and managing the network of covert community agents (*rijal*) embedded across areas under ISWAP's influence. The departmentf functions as the intelligence and counterintelligence arm of ISWAP's parallel governance structure.

Rijal–awam: Used in this report to describe the overarching dynamic between ISWAP's covert agents (*rijal*) and the civilian communities (*awam*) they are embedded in. It is simultaneously an intelligence-gathering system, a social control and compliance mechanism, a logistics coordination network and the covert security element of ISWAP's broader parallel governance project.

Shura (as in IS shura council): This means 'consultation'. It is IS's senior consultative and legislative body, responsible for approving major strategic and doctrinal decisions, including the appointment of IS's overall leader.

Yusufiya: The informal name given to the movement of followers of Mohammed Yusuf, Boko Haram's founder, derived from his surname. The Yusufiya was a religious study and social movement centred in Maiduguri in the early 2000s before it became a violent insurgency following the 2009 uprising and Yusuf's death in police custody. The term is used by ex-members to refer to the original pre-insurgency organisation.

About the author

Taiwo Adebayo is a Researcher at the Institute for Security Studies, based at the Regional Office for West Africa, the Sahel and Central Africa. Previously, Taiwo worked as a journalist and editor at *The Associated Press* and *Premium Times*. In 2019, he was part of the team behind the United Kingdom's (UK) Global Challenges Research Fund project with De Montfort University on the humanitarian crisis in northeast Nigeria. He has a Master's degree in international development from the University of East Anglia, UK.

About the ISS

The Institute for Security Studies (ISS) partners to build knowledge and skills that secure Africa's future. The ISS is an African non-profit with offices in South Africa, Kenya, Ethiopia and Senegal. Using its networks and influence, the ISS provides timely and credible policy research, practical training and technical assistance to governments and civil society.

Development partners

Government of the Netherlands

This report is funded by the Government of The Netherlands. The ISS is also grateful for support from the members of the ISS Partnership Forum: the Hanns Seidel Foundation, the European Union, the Open Society Foundations and the governments of Denmark, Ireland, the Netherlands, Norway and Sweden.

© 2026, Institute for Security Studies

Copyright in the volume as a whole is vested in the Institute for Security Studies and the author, and no part may be reproduced in whole or in part without the express permission, in writing, of both the author and the publishers.

The opinions expressed do not necessarily reflect those of the ISS, its trustees, members of the Advisory Council or donors. Authors contribute to ISS publications in their personal capacity.

Cover image: © ISS

ISSN 2617-8184 Print
ISSN 2617-8192 Digital