Enhancing intelligence capabilities against Jihadist and non-state armed groups in West Africa

Johnny Kwadjo

October 2026

African Security Sector Network (ASSN)

Formed in 2003, the **African Security Sector Network (ASSN),** headquartered in Accra (Ghana), is a pan-African network of practitioners and organizations working to promote effective and democratically governed security sectors across Africa.

For more information, please contact the **ASSN** team by email: **info@africansecuritynetwork.org**

or visit the **ASSN** website:
http://africansecuritynetwork.org/assn/

Article available online at:

https://

To cite this article:

Kwadjo (J.), «*Enhancing intelligence capabilities against Jihadist and non-state armed groups in West Africa.*», ASSN, October 2026.

Table des matières

ABBREVIATIONS AND ACRONYMS 4
INTRODUCTION 5
DEFINING THE JIHADIST AND OTHER NON-STATE ARMED GROUPS 5
Nature of other non-state armed actors 5
Security and political effects 6
THE INTELLIGENCE CYCLE AND ITS OPERATION IN THE PREVENTION AND COUNTERING OF VIOLENT EXTREMISM 7
An overview of the intelligence cycle 8
CHALLENGES FACED BY INTELLIGENCE AGENCIES IN COMBATTING VIOLENT EXTREMISM IN WEST AFRICA 8
Enhancing Intelligence Capabilities 10
Integrating Financial Intelligence Across Jurisdictions 10
Leveraging Technology for Predictive Intelligence 10
Conclusions 11

ABBREVIATIONS AND ACRONYMS

SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition
SIGLE : Definition

INTRODUCTION

While the term “Intelligence-led” has become a virtual mantra in propositions about operational activities aimed at effectively confronting, neutralising, defeating, or, otherwise, suppressing the increasing and debilitating activities of jihadists and other non-state armed groups, in the West African sub-region, the evidence appears to point to the contrary.

The apparent and noticeable gaps and challenges still encountered in these efforts attest, quite clearly, to the fact that Intelligence capabilities are not being optimally deployed in this effort to date.

Whether it is in Nigeria, the Sahel, the Horn, or other parts, jihadists and other non-state armed group activity continues with such reckless abandon, suggesting that neither intelligence capabilities nor any other serious counter-measures are at play.

The question, therefore, arises as to how intelligence can best be utilised, or, even retooled to, more effectively, play its expected leading role in the security governance architecture of West African states in their efforts at Preventing and Countering Violent Extremism in the sub-region.

DEFINING THE JIHADIST AND OTHER NON-STATE ARMED GROUPS

To better indicate how intelligence activity could be better utilised in leading operational activities to prevent and counter violent extremism, we may, first, note that jihadists and other non-state armed groups in West Africa (who are the object of the proposed intelligence activities) are, understood, typically, as those hybrid insurgent, criminal and/or political actors who occupy existing security and governance vacuums, creating severe insecurity, displacement and economic disruption across the Sahel and into coastal states.

In West Africa. these groups are known to include franchises and affiliates of Al- Qaeda and the Islamic State, such as Jama’at Nusrat al- Islam wal- Muslimeen (JNIM), the Islamic State Sahel Province (often referred to as ISGS/IS Sahel), and Islamic State West Africa Province (ISWAP), many of which evolved from, or absorbed earlier organizations like Boko Haram.

They are also known to combine what has often been referred to as “ideological narratives” with local conflict dynamics, embedded in disputes over land, resources and governance, rather than operating as purely external terrorist organisations.

These groups have also been known to typically pursue a rural insurgency strategy, using ambushes, Improvised Explosive Divices (IEDs) and targeted assassinations to push state forces out of peripheral areas while setting up parallel governance structures that regulate justice, taxation and social norms in those areas.

Nature of other non-state armed actors

Beyond jihadist organisations, West Africa also has a wide-spectrum of non-state armed actors, including so-called community self- defense militias, vigilante groups, local mercenaries, criminal networks and private security companies.

Since many of these actors emerge in response to state weakness and gaps in policing and justice provision, they position themselves as protectors of communities or economic interests in one form or the other.
Some of these groups attempt to provide some form of localised security and dispute resolution services. And this enables them to engage in small arms proliferation while entrenching themselves

in patronage networks, which, at times, find them collaborating with or mirroring criminal and extremist organisations.

This complex set of security environments has often been described as “hybrid security governance”, in which state and non-state security and justice providers overlap, compete and, sometimes, cooperate, and, thus, blur the line between public security and private or factional protection.

Security and political effects

The growth of jihadists and other armed groups has produced intense violence in Burkina Faso, Mali, Niger, Nigeria and the Lake Chad Basin, emptying villages, displacing hundreds of thousands of people and eroding state control over large rural territories.

As violence and extremist activities move southward from the Sahel, coastal states,such as Benin, Côte d’Ivoire, Senegal and Togo have faced increased cross-border attacks, infiltration and refugee inflows, even where full insurgencies have not yet taken root.

This insecurity has fed into cycles of military coups and fragile transitions, particularly in the central Sahel where military regimes have justified their power grabs as necessary to combat terrorism although they continue to struggle to reverse these jihadist gains.

At the same time, conflict linked to jihadists and non-state armed groups has led to large-scale displacement, disrupted social services and restricted access to health care, education and water across affected regions.

Furthermore, non-state armed groups are known to be heavily involved in illicit economic activities, including smuggling and human trafficking. They also engage in random informal taxation of trade and agriculture to fund their operations, and, in turn, deepen corruption and organised crime networks.

In some areas, these groups provide rough justice, regulate markets, or mediate disputes which sometimes win them local support, but which, nevertheless, simultaneously normalise armed rule and undermine formal institutions.

External security contractors and domestic private security companies add another layer, sometimes filling gaps in protection for elites and businesses, but oftentimes operating with limited accountability and drawing resources and attention away from building effective, inclusive public security sectors.

Overall, the proliferation of jihadists and non-state armed actors shifts West Africa’s security order from centralised state control toward a fragmented system in which violence, governance and economic power are distributed among multiple armed stakeholders, rather than concentrating the monopoly of the use of violence in legitimate state actors.

Jihadist groups in the Sahel expand mainly by embedding themselves in local conflicts and communities, applying a mixture of material incentives, ideology and coercion to recruit followers and control territory. Their influence grows when they are able to portray themselves as protectors or alternative authorities in places where the state is absent, abusive, or unable to deliver basic services.

Exploiting grievances and state weakness
Sahelian jihadist groups systematically tap into local grievances such as marginalisation, discrimination, abuses by security forces and disputes over land and resources to attract recruits, especially the rural youth and herding communities. Weak, corrupt, or predatory state institutions make it easier for these groups to present themselves as more responsive and just than official authorities.

They also leverage the vacuum created by state withdrawal from remote areas, using vast, sparsely governed borderlands to move, train and build cross-border networks. Repeated coups and governance crises in Mali, Burkina Faso and Niger further distract security forces and open space for jihadist expansion.

Providing protection and "governance"
Groups like JNIM and ISWAP deliberately cultivate an image as community defenders, offering protection from rival militias, bandits, or abusive security forces. In some areas, they regulate markets, mediate disputes and enforce their own justice systems, which can appear more predictable than distant state courts.

By setting rules for taxation, movement and social conduct, they build parallel governance structures that bind communities into their orbit. These arrangements also create dependency, making it harder for civilians to disengage even if they disagree with jihadist ideology.

Material incentives and social advancement
Poverty, unemployment and lack of education give recruitment offers strong appeal, since armed groups offer salary, food, status and, sometimes, support for marriage or family expenses. In places like northern Mali and the Lake Chad region, young men can earn better income providing intelligence or fighting for jihadist factions than engaging in available legal livelihoods.
Beyond cash, recruitment can promise social mobility and recognition for marginalised youth, particularly those who feel excluded by traditional or administrative authorities. These dynamics help explain why some people join primarily for economic or social reasons, with ideology becoming more important only after enlistment.

THE INTELLIGENCE CYCLE AND ITS OPERATION IN THE PREVENTION AND COUNTERING OF VIOLENT EXTREMISM

From the brief characterisation of the nature and attributes of the jihadist and non-state armed group menace sketched above, it will appear that the very first step in any strategy aimed at confronting and dismantling them should be a system of acquiring relevant fore-knowledge about their activities.

Such systematically acquired information will have to constitute the foundation upon which all other inputs are assembled in the preparation and deployment of any viable and effective effort at PREVENTION, as well as COUNTERING violent extremism.

It is, therefore, the formal process of turning such acquired information into usable insights, within an organisational structure, which is being referred to here as intelligence production, and the end product, then, as INTELLIGENCE.

Consequently, "intelligence", in this context, refers to information that has been collected, evaluated and analysed so that decision-makers can act on it, in their planning and execution of operations, rather than just the raw data that may be available to them.

An overview of the intelligence cycle

Although various countries develop Intelligence systems in accordance with their own history and needs, standardising the intelligence production process in order to attain more effective analytical outcomes has come to be accepted as a most useful development, over time.

It is, thus, for the achievement of the optimum advantages for analysing such information that the process of "the intelligence cycle" has developed.

The intelligence cycle can, be explained as a repeatable process for turning raw information into finished intelligence and then continuing to update these requirements based on feedback received from the implementation of the previous decisions.

Again, although different organisations may label or split these steps slightly differently, most of them describe a cycle that includes:

- Setting or establishing the requirements; this is where task masters from a planning section will define exactly what information is needed, why it is needed and how it can be obtained, including priorities and resources needed.
- Collecting the required data; this is where agents gather raw information from available sources such as human reports, technical sources, open sources (such as news reports) and databases.
- Processing this data; in this respect, the raw data is converted into a useable form, for example, by translating, decrypting, digitising, or organising it to focus on the task.
- Analysing the processed data; here, analysts evaluate, compare and interpret the processed information to produce assessments, estimates and briefings that answer the original questions.
- Disseminating the results; this is where the finished intelligence is delivered to the people who need it for integration into their own planning and operations.
- Receiving feedback; this is where decision-makers provide their comments on the usefulness or otherwise of the intelligence and, as a result, add new questions or refine the requirements to start a new cycle.

In effect, we may conclude that such an intelligence cycle is useful because, using a structured cycle helps organisations avoid random data collection, ensuring that effort focuses on clearly defined questions and decisions.

Because the cycle repeats, it supports continuous learning: new intelligence leads to new or refined requirements, thus, improving decisions over time.

CHALLENGES FACED BY INTELLIGENCE AGENCIES IN COMBATTING VIOLENT EXTREMISM IN WEST AFRICA

In general, challenges faced by intelligence agencies in regions, such as Nigeria and the Sahel, include:

Difficulties in coping with unclear and informal terrorist financing methods. In Nigeria, for example, groups, such as Boko Haram and the Islamic State West Africa Province (ISWAP), are known to employ diverse funding methods that include foreign donations, running extortion rackets, ransom taking and trade in common products like dried fish.

At the same time, their tendency to rely on informal economies and cash-based systems pose particular challenges for data capture and exploitation in financial intelligence operations. For instance, informal indigenous saving systems (e.g. Esusu, Adashe and Ajo) and barter transactions in

agricultural sectors allow these groups to evade conventional oversight and complicate efforts to track illicit financial flows.

Further complicating the landscape are the high levels of financial exclusion among the adult population. Reports indicate that over 41.6 per cent of adults in Nigeria were estimated to be excluded from formal financial services, with more than 36% being unbanked. Such broad financial isolation drives many individuals to rely on informal and unregulated money transfer systems, thus, hindering the ability of intelligence units to capture critical financial data.

In the Sahel, the threat environment is similarly complex. It has been noted that violent extremist organisations have grown not only due to the inherent ideological fervor but also because of weak governance, economic decline and the worsening effects of climate change.

It has been argued that the apparent collapse of international counterterrorism support and a power vacuum in the region have created fertile ground for extremist organisations. such as JNIM, ISGS and ISWAP, to expand their influence.

Furthermore, the phenomenon of converging security threats (where terrorist organisations cooperate with criminal networks) has exacerbated the difficulties of pinpointing and disrupting illicit financial flows.

Another critical challenge to intelligence-led operations is the fragmentation of intelligence collection and analysis due to rigid, hierarchical structures within the security sector as a whole.

Intelligence agencies and law enforcement entities have historically operated in administrative silos, limiting the free flow of critical information to counter-terrorism agencies and, thus. posing serious challenges, especially given the unpredictable nature of modern terrorism. For example, in Nigeria, the Nigerian Financial Intelligence Unit (NFIU) must navigate complex networks of informal transactions while working with national and international partners, to reconcile disparate data sources.

In short, while technology and new analytical methods offer great promise, traditional structures are still hampered by outdated protocols and inter-agency barriers.

At the same time, the Sahel region, stretching from Senegal to Eritrea, presents a stark contrast to Nigeria in terms of security challenges. Violent extremist organisations in this region (such as JNIM and ISGS have proved quite devastating in their various attacks against civilians.

In some countries,weak governance, economic decline and the adverse effects of climate change further exacerbate conflict and fuel the operations of these non-state armed groups.

A key challenge in the Sahel is the convergence of security and criminal threats.
As extremists cooperate with organised crime networks, traditional intelligence methodologies struggle to keep pace with the rapidly changing threat environment. The lack of robust regional intelligence networks impedes the sharing of timely information, leading to reactive, rather than proactive, counterterrorism measures.

However, recent initiatives, such as the formation of a regional task force after the UN Security Council Resolution 2349, demonstrate that closer cooperation among West African nations can enhance surveillance and targeted operations against terrorist financing.

Enhancing Intelligence Capabilities

Under these circumstances, it would be useful to consider a number of proposals for enhancing the Intelligence capabilities of West African States to enable Intelligence to effectively "lead" the effort to prevent and combat violent extremism in the sub-region.

These may include:

Embracing a Comprehensive, Decentralised Intelligence Model

To enhance intelligence capabilities against jihadists and non-state armed groups, there must be a decisive move toward decentralised intelligence architectures, including:

Developing Fusion Centres and Regional Networks

Establish regional fusion centres that synthesise local, national and international intelligence. These centres can facilitate real-time data sharing and collaborative analysis across borders, thereby, boosting the efficacy of counterterrorism operations.

Implementing Decentralised Data Analytics Platforms

Adopt analytical platforms that enable decentralised analysis.

This approach allows for a localised understanding of threats while maintaining the overall strategic framework set by central authorities above them.

Integrating Financial Intelligence Across Jurisdictions

Financial intelligence is a critical front in the fight against terrorism, and efforts to strengthen this area may include:

Enhanced Use of Digital Financial Tools

Deploy advanced anti-money laundering tools like GoAML, the fully integrated software solution developed by the UN Office on Drugs and Crime (UNODC) specifically for use by financial intelligence units as its strategic response to financial crimes, including money-laundering and terrorism.

When deployed alongside other block chain solutions(a decentralised and distributed ledger system operated on a peer-to-peer network), these could ensure that financial flows are transparent and, therefore, traceable.

Cross-Border Regulatory Cooperation

This is to promote cross-border regulatory frameworks and initiatives dedicated to the sharing of financial intelligence. Such collaboration can significantly reduce the avenues for terrorist financing and enhance transnational financial oversight.

Leveraging Technology for Predictive Intelligence

Advancements in technology provide enormous potential for predictive intelligence. By incorporating machine learning, predictive analytics and real-time monitoring, intelligence agencies can continuously evolve their analytical capabilities.

Steps toward this goal may include:

Establishing Real-Time Data Interchange Pipelines

Create multipoint data pipelines that operate in real time, enabling rapid detection of anomalies in financial, communications, and operational data

Investing in Predictive Modeling

Develop robust predictive models that use historical data, contextual trends and situational analysis to forecast future terrorist activities. This can serve as early warning systems and focus resources effectively to preempt attacks.

Protecting Civil Liberties While Enhancing Security

Any modernisation of intelligence capabilities must delicately balance security imperatives against the need to preserve civil liberties. To do so, agencies should:

Implement Robust Oversight Mechanisms

Establish clear oversight frameworks with strong internal and external accountability measures to ensure that intelligence operations respect privacy and civil rights.

Institutionalise Transparency Protocols

Ensure that all data-sharing protocols are coupled with transparency measures that notify appropriate oversight bodies about the nature and extent of intelligence gathering. This can help foster public trust and create a legal environment that encourages innovation while protecting individual freedoms.

Overall, we may represent the process flow for enhancing intelligence capabilities through technological integration and organisational reform as follows:

a. Data Collection from Multiple Sources
b. Advanced Data Analytics
c. Anomaly Detection & Predictive Modeling
d. Actionable Intelligence
e. Rapid Interagency Sharing
f. Targeted Counterterrorism Operations
g. Feedback & Continuous Improvement

The above should illustrate the cyclical process by which decentralised intelligence networks may operate (from data collection to rapid interagency sharing and continuous feedback loops)

Conclusions

In conclusion, we may note that enhancing intelligence capabilities against jihadists and non-state armed groups requires a multifaceted strategy that spans technological innovation, methodological evolution and deep organisational reforms.

Among the **organisational reforms** required is breaking down traditional intelligence silos through decentralised, horizontal communication models and establishing robust fusion centres that can greatly improve situational awareness and the speed of response.

Another organisational reform needed is a change to **Predictive Intelligence.** In this regard, the agency should aim at transitioning from a reactive to a predictive intelligence model by which it empowers itself to anticipate terrorist activities and act preemptively, thereby, reducing the impact of extremist operations.

Looking ahead, the adoption of these technological and organisational reforms promises to transform intelligence-led operations into agile, dynamic networks capable of countering the complex, evolving nature of jihadists and non-state armed groups.

By uniting innovative technology with robust interagency collaboration and strategic international partnerships, nations in affected regions can establish an intelligence apparatus that is both resilient and adaptable – ultimately strengthening global security in an increasingly unpredictable world.