

TIMBUKTU INSTITUTE

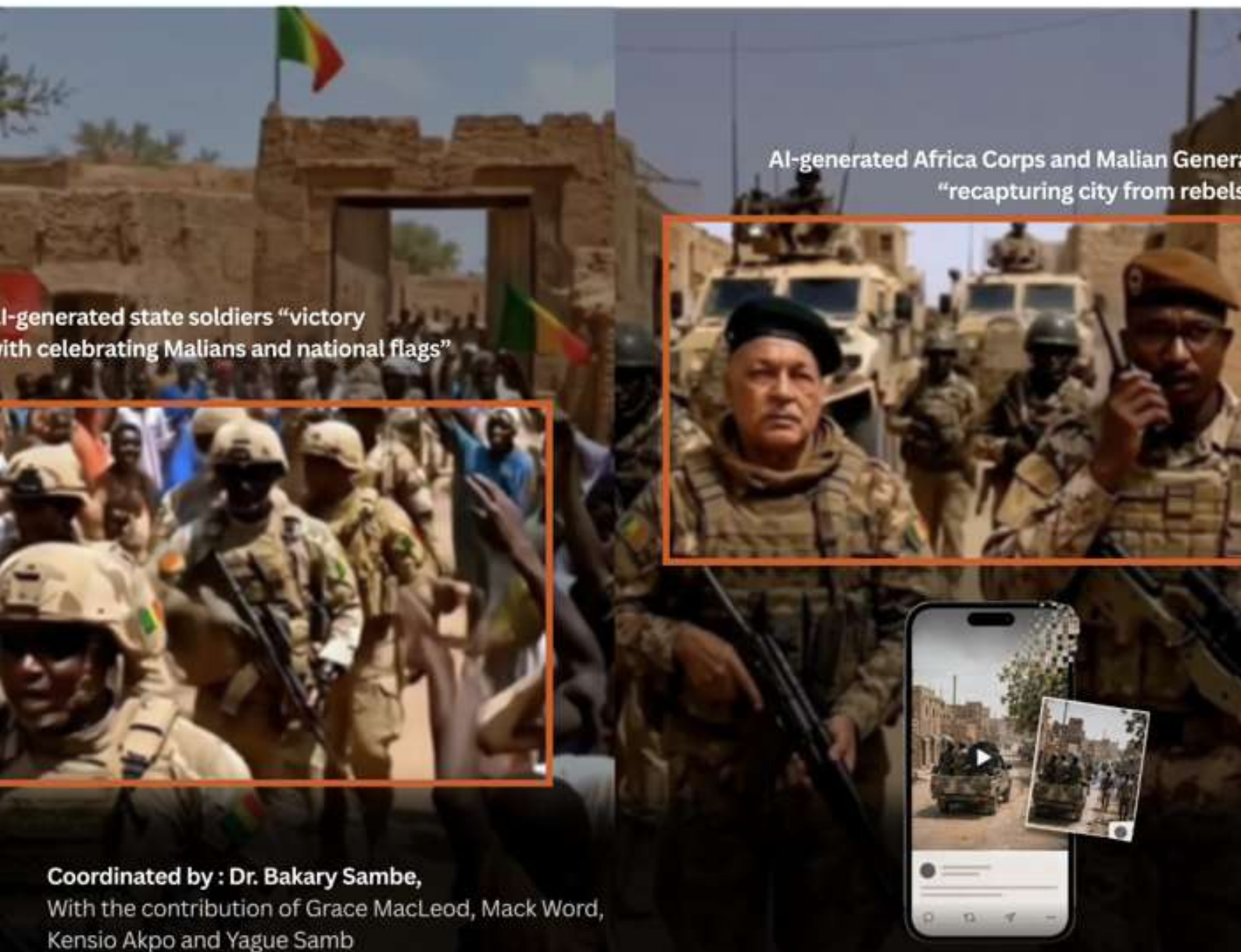
African Center for Peace Studies
www.timbuktu-institute.org

REPORT

• ARTIFICIAL INTELLIGENCE • MALIAN CONFLICT •

ALGORITHMS AT WAR

How Generative AI is Reshaping the Malian Conflict



AI-generated state soldiers "victory
with celebrating Malians and national flags"

AI-generated Africa Corps and Malian General
"recapturing city from rebels"

Coordinated by : Dr. Bakary Sambe,
With the contribution of Grace MacLeod, Mack Word,
Kensio Akpo and Yague Samb

TABLE OF CONTENTS

Executive Summary.....	4
Introduction.....	5
I- DIFFERENTIATED USES OF AI BY ACTORS IN THE MALIAN CONFLICT.....	6
A- JNIM AND THE AI-GENERATED POSTER: LIMITED TECHNICAL SOPHISTICATION, FAR-REACHING IMPLICATIONS.....	7
1- Az-Zallaqa's Role as Relay and Distributor.....	7
2- JNIM and Generative AI: What Immediate Implications for Accelerating Jihadist Propaganda?.....	8
3- Overcoming Language Barriers Through AI: Regional Popularization of Terrorist Propaganda.....	8
B- SYNTHETIC CHARACTERS, REAL INFLUENCE: THE FLA'S DECENTRALIZED USE OF GENERATIVE AI.....	8
1- Creativity, Distribution and Amplification: When the FLA Pools Digital Skills.....	9
2- "Azzghim" on the Trail of Africa Corps: The FLA Challenges the Russian Information Machine.....	10
3- Generative AI in the Malian Conflict: The Rise of Non-State Actors.....	14
C- FROM GRASSROOTS TO STATE APPARATUS: RUSSIA'S AFRICA CORPS AND THE PROFESSIONALIZATION OF AI-DRIVEN DISINFORMATION.....	14
1- Russia and the Use of Generative AI: A State Strategy "Unmasked"?.....	15
D- MANUFACTURING LEGITIMACY: GENERATIVE AI, MEDIA CONTROL AND THE MALIAN REGIME'S INFORMATION STRATEGY.....	15
1-Africa Corps to the Rescue: The Digital Space as an Alternative Battlefield ?.....	17
II- GENERATIVE AI AND THE EVOLUTION OF THE MALIAN CONFLICT: WHAT LIES AHEAD ?.....	17
A- GENERATIVE AI: A GENUINE OPPORTUNITY FOR "GLOCAL" JIHADIST RECRUITMENT ?.....	18
B- A MORE THREATENING USE OF GENERATIVE AI: HOW TO ADDRESS INCREASINGLY UNRESTRAINED AND USER-FRIENDLY AI ?.....	18
C- FROM THE VIRTUAL TO SOPHISTICATED WEAPONS: IS AI REDRAWING THE MILITARY BALANCE OF POWER ?.....	19
D- AI AS A TECHNOLOGICAL ACCELERATOR OF THE MALIAN CONFLICT AND AN UNEVEN FORCE MULTIPLIER.....	19
NOTES & REFERENCES.....	21

TABLE OF FIGURES

FIGURE1 : AI-generated “coming soon” poster from JNIM.....	6
FIGURE 2 : @azzgim on TikTok.....	9
FIGURE 3: Screenshot of an @azzghim TikTok video posted on April 24, 2026, showing a pixel anomaly around the individual's finger.....	10
FIGURE 4 : @tawri.n.azawad on TikTok.....	11
FIGURE 5 : @asnan831 on TikTok.....	12
FIGURE 6 : Post on the Asnan831 TikTok account showing visual anomalies in several places, notably in the flag and the child's top button.....	12
FIGURE 7 : Another post on the Asnan831 TikTok account showing visual anomalies, notably a malformed flag and oddly shaped fingers.....	13
FIGURE 8 : A post on the Asnan831 TikTok account shows him posing with Azzghim.....	13
FIGURE 9 : Two screenshots of posts on X, taken from OpenAI's report, showing how Russia uses generative AI to create brief pro-Kremlin news articles.....	16
FIGURE 10 : Diagram of the "AI-Freak" IMS, taken from the joint report by VIGINUM, the FCDO and the EEAS.....	16
FIGURE 11 : Screenshots of the @6tm_officiel post showing FAMa and Africa Corps retaking Kidal.....	17

EXECUTIVE SUMMARY

For more than a decade, the Malian conflict has been characterized by a permanent recomposition of alliances, balances of power and modes of confrontation. The alliance concluded between Jama'at Nusrat al-Islam wal-Muslimin (JNIM) and the Front de libération de l'Azawad (FLA), despite clear ideological divergences, is one of the most recent illustrations of this. In this sense, the coordinated assaults of April 2026 confirmed this evolution of a conflict in which strategic calculations are increasingly taking precedence over traditional divides. That said, this recomposition is no longer playing out solely on the military terrain. It now extends into the information space, where generative artificial intelligence (AI) is, in turn, beginning to change the rules of the game.

Far from being a uniformly adopted technology, generative AI is being mobilized differently depending on each actor's capabilities, resources and objectives. JNIM's use of it remains limited for now, notably through visual materials designed to reinforce already well-established propaganda. The release, in June 2026, of AI-generated posters by its media wing Az-Zallaqa nonetheless points to a development worth monitoring. By considerably reducing production costs and timeframes, AI could enable the group to multiply its content, translate it into local languages and further personalize its recruitment messaging. This shift could thus favor the emergence of a communicational jihadism that is faster, more targeted and better adapted to local realities. On the FLA side and among its support networks, use appears more decentralized. TikTok accounts feature recurring synthetic characters designed to carry narratives favorable to Azawad and hostile to Africa Corps. The appeal of these tools lies as much in their amplification capacity as in the difficulty of establishing their origin. By artificially humanizing a cause and giving the illusion of broad popular support, this content can contribute to the normalization of extremist narratives and create, among vulnerable audiences, forms of proximity conducive to later mobilization.

At the same time, the most sophisticated use appears to be on the side of Russia and its information apparatus. The documented operations surrounding African Initiative and the "AI-Freak" operation show that AI can be integrated into structured disinformation campaigns, combining generated content, fake accounts and optimized distribution. The Malian regime and, more broadly, the members of the Alliance of Sahel States are gradually settling into this ecosystem, using these methods to consolidate their legitimacy and further control the information space. From this point on, the stakes go beyond the mere production of false or misleading content. As AI becomes more accessible, it could also facilitate personalized recruitment, automated translation, anonymization, and even certain targeting and military-support functions. One nuance remains essential, however: the risk lies above all in the growing gap between the sophistication of these tools and the detection and resilience capacities of the population. The more refined the instruments become, the more uncertain the boundary between what is real, fabricated and manipulated becomes, making mastery of the information space a stake of the conflict in its own right.

It would therefore not be far-fetched to suggest that Mali could become a veritable laboratory of AI-assisted information warfare. That said, while the most advanced kinetic uses remain largely prospective for now, the battle of narratives is already underway. In an information space that is increasingly saturated, the ability to distinguish the real from the fabricated is itself becoming a security issue. And for Sahelian states in general, the response can therefore no longer be limited to conventional disinformation-countering mechanisms. It will also need to strengthen digital literacy, detection capacities and prevention strategies in the face of a technology set to durably redraw the contours of the conflicts at hand.

INTRODUCTION

For more than a decade, the Malian conflict has been marked by the interweaving of jihadist, separatist and state dynamics. This complexity of alliance dynamics intensified when, in 2025, Jama'at Nusrat al-Islam wal-Muslimin (JNIM) and the Front de libération de l'Azawad (FLA) concluded an alliance aimed at driving the Russian paramilitary group Africa Corps out of Kidal and weakening the Malian military power and its security apparatus. Their willingness to cooperate despite seemingly incompatible political ideologies reflects military pragmatism and illustrates the dynamic evolution of the Malian conflict landscape, in which strategic calculations now outweigh communal, historical or ideological divides. This dynamic was successfully put to the test during the coalition's coordinated assaults, launched on April 25, 2026, dealing a severe blow to the diplomatically isolated military rulers and their Russian partner.lancés le 25 avril 2026,

However, the recomposition of alliances and balances of power is not the only transformation under way in the Malian conflict. It is also evolving in its modes of confrontation, as actors move into the information field and appropriate new technological tools. Among them, generative artificial intelligence (GenAI) opens a new front, where the production and dissemination of content become instruments of propaganda, mobilization and influence. In this sense, information operations, combined with the recent accessibility of artificial intelligence (AI) and the growing popularity of generative AI (GenAI) models, are shaping the battlefield and rivalries in Mali and redefining the future of conflict resolution in the Sahel. However, rather than a single, uniform wave of technological adoption, the Malian conflict illustrates an environment in which each actor instrumentalizes generative AI according to its degree of technical sophistication, its resource constraints and its strategic objectives.

For its part, JNIM shows limited but notable experimentation with generative AI compared with the refined capabilities of the Islamic State. Using AI as a tool of anonymization in a tense context, the FLA and its support base mainly use AI-generated characters on social media to bolster the Azawad cause and facilitate the recruitment of fighters and militants. As for the Malian military authorities and their Africa Corps allies, they have the resources and expertise needed to integrate AI into broader and even more sophisticated information operations. Through a combination of military and/or paramilitary presence and sophisticated information warfare, Russia's repositioning in the Sahel, during its transition from the Wagner Group to Africa Corps, has been accompanied by an expansion of Russian influence in the region, riding on the rejection of France, which has itself also been fueled by disinformation operations.

A recent Timbuktu Institute analysis, published in May 2026, examined how the Russian information ecosystem turned Moscow's tarnished reputation after the April attacks into a narrative opportunity, through a coordinated media apparatus, going as far as to disseminate sponsored or manipulated reports claiming that France and Ukraine had trained and equipped the JNIM and FLA assailants. These findings form the empirical foundation of this analysis, whose scope is broadened to examine the role of the differentiated uses of generative AI by JNIM, the FLA, Africa Corps and the Malian regime in their information-warfare strategies. This democratization of generative AI, occurring at different scales, raises a central question: "To what extent is artificial intelligence redefining information warfare in Mali, and how, depending on the actors wielding it, is it heightening the volatility and at times unexpected evolution of the conflict?" The analysis thus proceeds by examining the differentiated uses of generative AI by JNIM, the FLA, Africa Corps, the Malian regime and their respective support bases, and assesses the risks that the integration of generative AI poses to Sahelian stability, notably within the ongoing information war. The growing sophistication of generative AI as an instrument of both information and kinetic warfare thus acts as a force multiplier for state and non-state actors alike, making it increasingly difficult for targeted populations to distinguish between fiction, reality and disinformation.analyse récente du Timbuktu Institute, publiée en mai 2026,

I- DIFFERENTIATED USES OF AI BY ACTORS IN THE MALIAN CONFLICT

Generative artificial intelligence is gradually establishing itself as a new instrument of information warfare in Mali, its uses varying according to the capabilities, resources and strategic objectives of the different actors. Its appropriation thus ranges from still-limited experimentation with image-generation tools to the creation of synthetic characters, and on to the integration of AI into more structured disinformation systems.

This diversity of practices above all reveals a new form of competition in which mastery of the technological tool is gradually becoming a lever of influence, mobilization and legitimization. Examining the practices of JNIM, pro-FLA networks, Africa Corps and the Malian authorities thus makes it possible to grasp how each, at its own level, is investing in this new space of confrontation.

A- JNIM and the AI-Generated Poster: Limited Technical Sophistication, Far-Reaching Implications

Among the four actors examined, JNIM shows the most limited observable use of generative AI, its adoption being largely confined to promotional material supporting existing propaganda campaigns. One example of this emerged in June 2026, with the release of posters announcing a series of videos celebrating the success of the group's attacks in Mali in late April 2026, which claimed the life of Malian Defense Minister General Sadio Camara, giving the operation broad communicational and symbolic reach.

JNIM's official media wing, Az-Zallaqa, published an AI-generated propaganda poster (Figure 1) depicting JNIM fighters in various combat situations: some on motorcycles, others armed in the back of trucks, while, notably, the white flag of the Islamic Emirate of Afghanistan flies against a fiery, smoke-filled sky. An inscription in Arabic at the bottom of the image reads:

"As part of the operations series The Manifest Victory (Al-Fath al-Mubîn)

The raids bringing glad tidings of victory will soon be released."

The poster displays various telltale markers typical of AI generation. Buildings and vegetation blend into one another, background details and small objects turn into Rorschach-test-like blotches, and the entire scene is tinged with the excessive smoothing characteristic of AI.



Figure 1: AI-generated "coming soon" poster from JNIM

1- Az-Zallaqa's Role as Relay and Distributor

Az-Zallaqa is responsible for publishing and republishing these AI-generated posters across several social media platforms, such as Signal, ChirpWire and Telegram, in a manner reminiscent of Islamic State (IS) methods. In 2023, IS had drawn up a guide on the secure use of generative AI, and as early as 2024, several AI-generated posters claiming terrorist attacks were documented as having been published by official and unofficial sources linked to IS. Subsequent reports went on to document this organization's use of AI-assisted video production, multilingual translation, and chatbots designed to personalize propaganda and recruitment messages and facilitate the engagement of sympathizers or future recruits.

AI-generated posters should therefore not be seen as a mere creative and visually interesting but isolated curiosity; rather, they should be understood as an indicator of the adoption of a cutting-edge technology and of growing AI capability. The example of the Islamic State (IS) suggests that once an extremist organization develops the technical capacity and organizational will to integrate generative AI into one part of its propaganda apparatus, the adoption of the technology and the possibilities it offers can then spread to other areas. Although, for now, there is little public evidence that JNIM has officially adopted generative AI in its information-warfare strategy beyond promotional materials, the lowering of technical barriers to AI use makes increased experimentation with video generation, translation and other targeted recruitment strategies increasingly likely.

2- JNIM and Generative AI: What Immediate Implications for Accelerating Jihadist Propaganda?

Despite a degree of technical limitation at this early stage, the first direct implication of JNIM's adoption of generative AI will be a significant and immediate acceleration in the production of sophisticated propaganda. The group currently appears to produce its propaganda materials (videos, images and text) through traditional channels. The group reportedly has only internal production teams relying on processes requiring considerable manual effort. Scaling up communications capacity to rival IS would require substantial human-resource management, specialized skills in video and graphic production, and above all extended production timeframes. Producing a professional-quality propaganda video previously could require weeks or months of work. With modern generative AI tools (whether Midjourney, DALL-E, Runway, or others), however, JNIM could considerably reduce these production timeframes to a matter of hours or even minutes.

A simple text prompt — "JNIM fighters attacking a government position, explosions, group flags in the background" — could automatically generate half a dozen professional-grade visuals within minutes.

These visuals could then be assembled into a video, with animation, music and text, producing an acceptable-quality propaganda video in a matter of hours. This dramatic increase in propaganda-production capacity would have a direct implication: an exponential increase in the volume of propagandist content disseminated, growing saturation of social media communication channels, and a more viral presence for the group across the regional information space.

3- Overcoming Language Barriers Through AI: Regional Popularization of Terrorist Propaganda

The second major implication concerns the linguistic and cultural localization of JNIM's recruitment, especially in an unprecedented context of the "endogenization" of jihadism. The group currently disseminates its messages mainly in classical Arabic, which naturally limits their reach among populations for whom Arabic is not their mother tongue or everyday language. The possibilities offered by AI in neural translation could allow JNIM to instantly generate versions of each propaganda message in some fifteen regional languages: Hassaniya, Fulfulde, Bambara, Mooré, Tamasheq, Songhai, Wolof and other linguistic and dialectal variants of the Sahel and West Africa.

The most significant development would be that multilingual translation would allow JNIM to produce differentiated narratives for different populations. A version of the recruitment message aimed at Fulani herders would emphasize the protection of pastoral interests, economic autonomy, and defense against government marginalization. A version aimed at marginalized urban youth would highlight the promise of dignity, economic inclusion, and social status within the JNIM "community."

A version aimed at idealistic religious youth would stress spirituality, the building of a purified Islamic state, and resistance against Western imperialism. Each of these narratives could be produced quickly and in parallel by AI systems, thereby maximizing recruitment effectiveness for each target population segment.

Another strategically crucial implication lies in the possibilities offered by AI dubbing, which would allow JNIM to target and recruit among populations entirely excluded from the written propaganda market. A 10-minute recruitment video, dubbed in Bambara with a native-sounding synthesized voice, showing JNIM fighters in victorious action, recounting stories of camaraderie and restored dignity, could be distributed via Telegram, WhatsApp or even informal radio, and would effectively reach illiterate or semi-literate young people in Mali, Burkina Faso and Niger. These young people might never access JNIM's websites or read its written publications, but could very easily watch a video or listen to a podcast distributed on a messaging platform accessible via a mobile phone — an object that has become ubiquitous across the Sahel, including in rural areas.

B- Synthetic Characters, Real Influence: The FLA's Decentralized Use of Generative AI

Unlike JNIM's propaganda apparatus, the FLA's online information system appears considerably more decentralized. The FLA's online support base seems to be increasingly relying on generative AI to produce realistic, recurring AI characters tasked with spreading pro-Azawad, anti-Africa Corps messages. On TikTok, for instance, pro-FLA messages are disseminated by a network of accounts that frequently repost,

modify and amplify content produced by different actors, relaying one another in turn. This process, adopted by the FLA and its relays, complicates content attribution; it is often difficult to determine whether these AI-generated characters originate from FLA members or from independent sympathizers won over to the broader Azawad cause.

1- Creativity, Distribution and Amplification: When the FLA Pools Digital Skills

The following case studies examine three accounts representative of this phenomenon, illustrating how these synthetic characters are created, distributed, and then amplified on TikTok. The three accounts are linked to one another: @azzghim is a mutual friend of @tawri.n.azawad and @asnan831. If, as analyzed above, these three accounts are fed by AI-generated content, this link suggests the existence of a network or field system of AI-generated TikTok accounts with a level of technological mastery that could be put to use for recruitment and wider propaganda dissemination. For the purposes of this study, these videos were first identified by observing a trend: several pro-FLA/Azawad TikTok accounts were modifying and reposting videos originating from a single account — @azzghim (Figure 2). According to omar-thingsite, a TikTok account research tool, this account was created in July 2024 and had, as of July 9, 2026, 601,000 followers and 304,000 likes.

The account posts videos criticizing and issuing threats against Russian elements involved in Africa Corps activities in Mali. Its bio “التمرد في وجه الظلم واجب لا يمكن ان تنسى دولة مالي هذا اليوم 27/7/2024” (Rebellion in the face of oppression is a duty — the “State of Mali will never forget this day, 27/7/2024

After cross-referencing and a few relevant clues, this bio likely refers to the Tinzaouaten battle of July 2024, during which a Tuareg rebel coalition ambushed joint forces of the Malian Armed Forces (FAMA) and Africa Corps near the Algeria-Mali border. The account's character is that of a presumed Tuareg man, "Azzghim," recognizable by a distinctive black birthmark, or paint mark, above one eye.



Figure 2 : @azzghim on TikTok.

2- "Azzghim" on the Trail of Africa Corps: The FLA Challenges the Russian Information Machine

Most of the account's videos consist of "Azzghim" speaking directly to viewers and followers. His messages specifically target Africa Corps, which he condemns and criticizes for acts such as "violating the property" of the people of Azawad and "making no distinction between young and old" in its violence and numerous abuses in both northern and central Mali.

Azzghim's videos display several warning signs typical of deepfake or AI-generated content. In one video, an image shows the pixels of his finger momentarily disappearing into his hair (Figure 3), and in the second half of the clip, the right side of his hair moves unnaturally in the wind.

In another video, an ear of grain moves inconsistently in the breeze, while Azzghim's curly hair remains completely still. The same video also appears to contain a sudden cut, revealed by the abrupt movement of an Azawad flag in the background, while Azzghim's voice and the rhythm of his movements remain uninterrupted. Although no single element is sufficient to conclusively demonstrate the use of generative AI or deepfake technology, the accumulation of these numerous anomalies takes on its full significance when assessed collectively against recognized indicators of AI-manipulated content.



Figure 3: Screenshot of an @azzghim TikTok video posted on April 24, 2026, showing a pixel anomaly around the individual's finger.

SoSafe, a European security-awareness company, offers a methodology for spotting deepfake videos:

1. Unnatural body movements
2. Strange coloring
3. Odd eye movements
4. Awkward facial expressions/emotions
5. Unnatural teeth/hair
6. Inconsistent audio

Reviewing different videos, the Azzghim account displays all six characteristics. While not conclusive on its own, the recurrence of this pattern across multiple videos reinforces the hypothesis that the account likely relies, at least in part, on AI-manipulated content. The second account studied, @tawri.n.azawad (Figure 4), is devoted exclusively to modifying and reposting @azzghim's content.

It was created in December 2025 and had 207,000 followers and 938,000 likes as of July 9, 2026. This account features several videos and images of the same individual seen on @azzghim, absent from the original account, as well as "edit"-style videos in which Azzghim's content is remixed. The account follows numerous other accounts posting similar content devoted to Azzghim.

The fact that this account focuses exclusively on a single recurring character suggests that it functions less as an independent content creator than as an amplifier within the broader pro-FLA system. By repackaging existing videos and redistributing them to partially different audiences, accounts such as @tawri.n.azawad create the illusion of widespread popular support.

Furthermore, the presence of images and videos not posted on Azzghim's original account raises questions about the origin of this content. @tawri.n.azawad is not the only account of this type identified during this research either; other accounts with a notable audience display the same pattern. If this content originates from a coordinating source, this could indicate an organized production of pro-FLA propaganda.

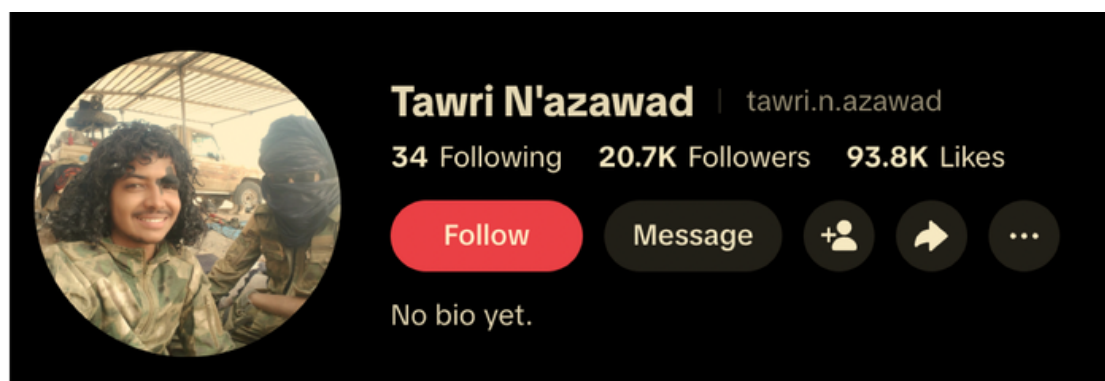


Figure 4 : @tawri.n.azawad on TikTok.

The third account, @asnan831 (Figure 5), features a young teenager claiming affiliation with Azawad. Since most of his TikTok content consists of still images accompanied by background music, it is far more difficult to establish AI-generation markers with certainty. Figure 6, however, presents an example of visual inconsistencies that may indicate a form of image manipulation. In the photo, the red fabric of a flag oddly blends with its white portion, the anatomy of his hand is unclear, and his top button and collar lining appear distorted.

In another post (Figure 7), one notices the strange construction of another flag, a curiously blurred background, and unusually smooth fingers. The account features a single video showing the boy posing alongside @azzghim (Figure 8); all other posts, save one, are still images. The account was created in October 2025 and had, as of July 9, 2026, 4,732 followers and 11,700 likes.

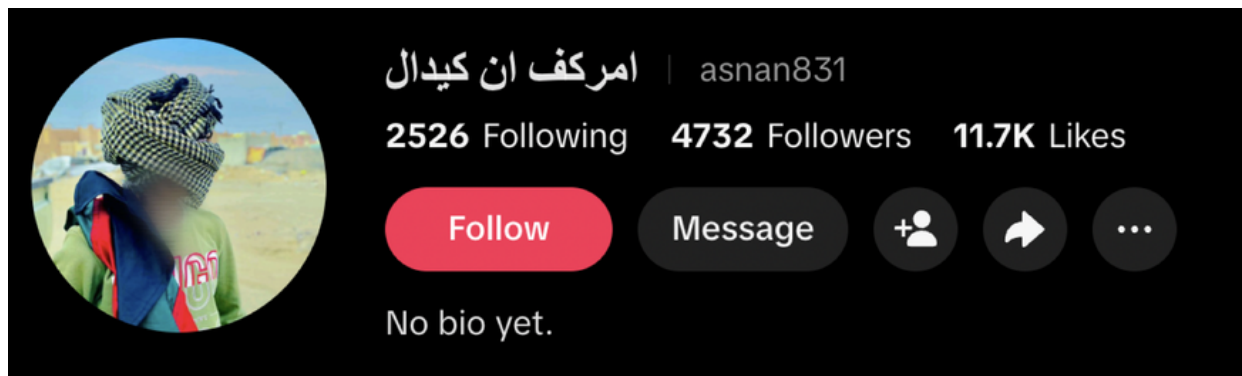


Figure 5 : @asnan831 on TikTok.

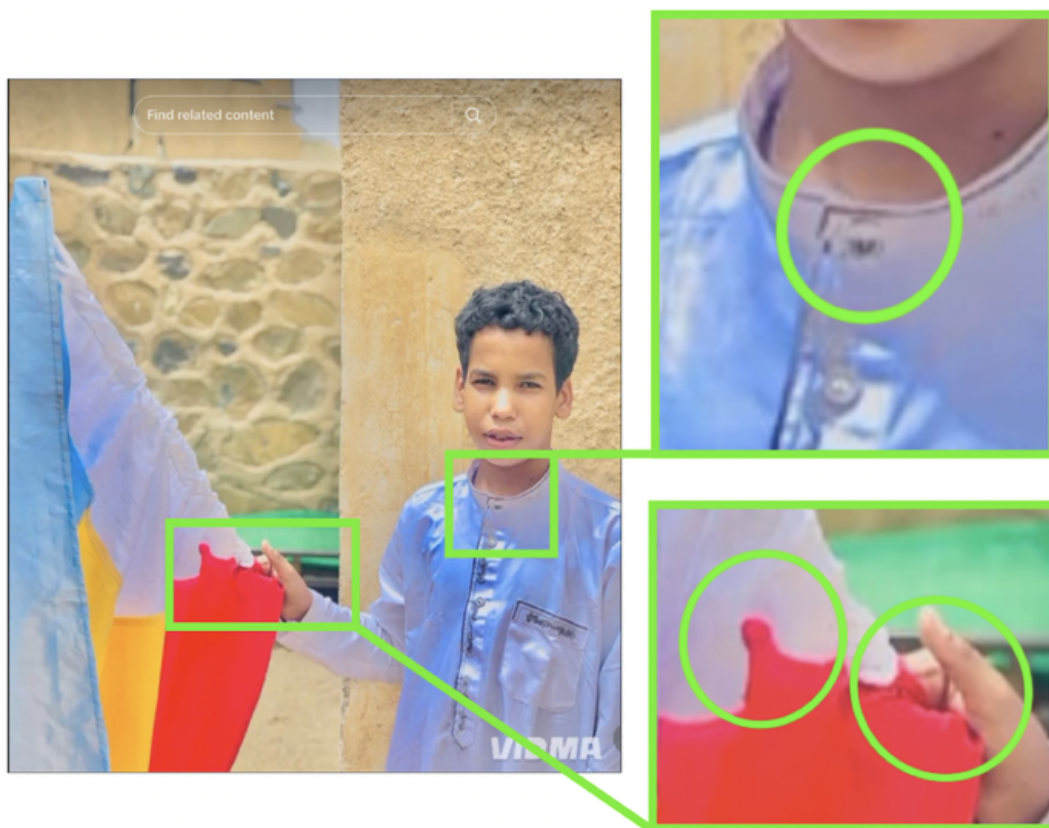


Figure 6: Post on the Asnan831 TikTok account showing visual anomalies in several places, notably in the flag and the child's top button.



Figure 7: Another post on the Asnan831 TikTok account showing visual anomalies, notably a malformed flag and oddly shaped fingers.

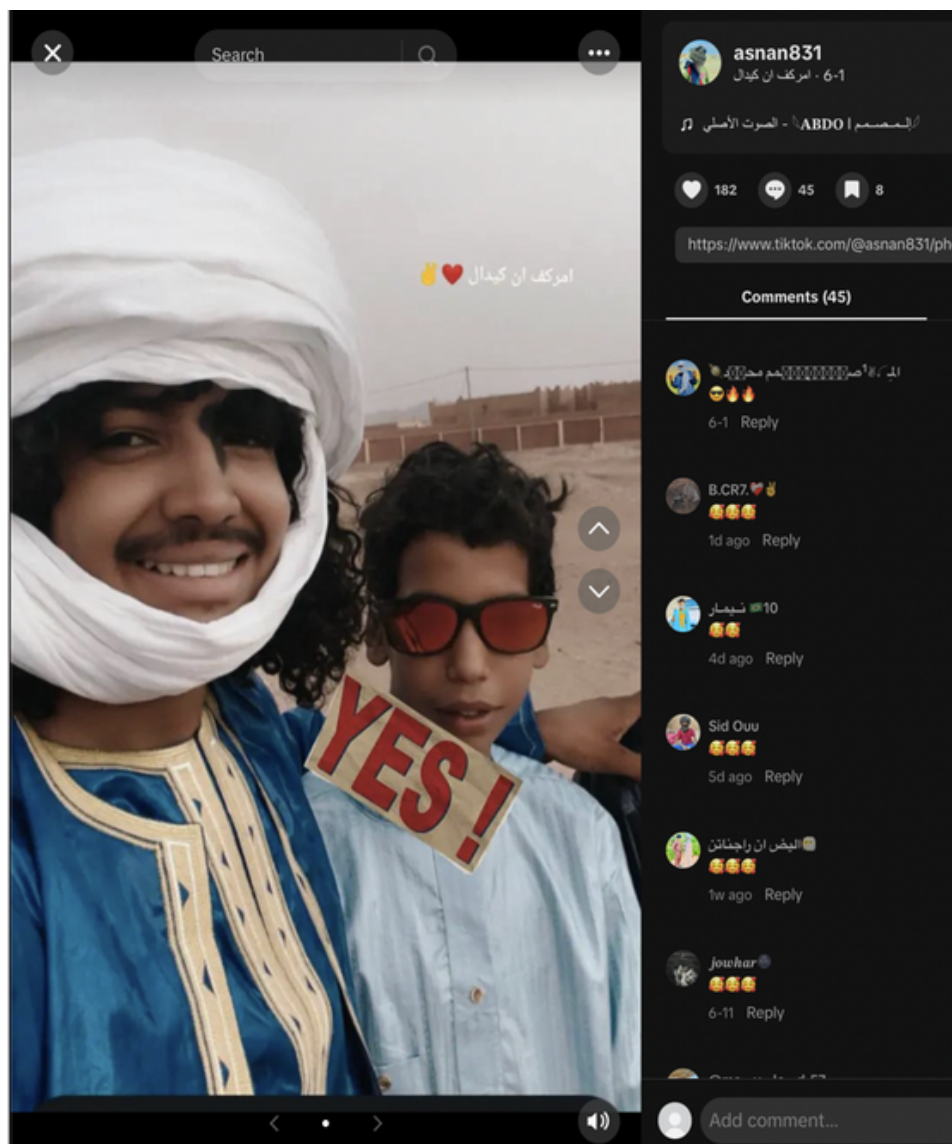


Figure 8: A post on the Asnan831 TikTok account shows him posing with Azzghim.

3- Generative AI in the Malian Conflict: The Rise of Non-State Actors

These case studies illustrate an emerging use of generative AI by non-state actors in Mali: the creation of synthetic characters capable of naturally conveying specific narratives on social media platforms. These AI characters offer several advantages.

On the one hand, they help humanize a movement by presenting convincing "individuals" capable of building familiarity and trust among viewers and other followers. These personas can also be tailored to specific audiences. The AI character of a young teenager may particularly resonate with young viewers already vulnerable to online radicalization, as is the case with the third account studied, Asnan831. Additionally, these accounts offer operational security advantages. After all, it is difficult to locate, capture, arrest or interrogate an extremist who does not exist. Although the content of these three accounts sits at the boundary between

messaging of sympathy and active recruitment, their existence illustrates how advances in generative AI can be exploited in new ways for recruitment, normalization and broader message dissemination.

Whether or not these AI-generated accounts constitute active recruitment mechanisms, repeated exposure to sympathetic messaging can contribute to the gradual normalization of extremist actors and to lowering the psychological barriers to future recruitment, by creating parasocial relationships with vulnerable viewers. Furthermore, given their alliance, it is also possible that as JNIM continues to explore AI-generated propaganda, this phenomenon of AI-generated pro-FLA characters on social media could inspire and accelerate the sophistication and expansion of JNIM's own information operations.

C- From Grassroots to State Apparatus: Russia's Africa Corps and the Professionalization of AI-Driven Disinformation

As the official arm of the Russian state, Africa Corps has extensive expertise in information warfare, as well as the resources needed to continuously increase its sophistication, in line with Russian gray-zone objectives and strategy. In this sense, the paramilitary group maintains official, unofficial and community partnership channels via WhatsApp and Telegram, as well as various other clandestine media channels across several platforms, in order to disseminate its propaganda. Given the considerable resources invested by Russia, the AI-generated propaganda supporting Africa Corps and related information operations in the Sahel is sophisticated.

According to Africa Defense Forum, Africa Corps is merely "one of the likely sources of deepfakes promoting pro-Russian and pro-junta narratives" in Mali. Russian channels aimed at influencing local populations, such as the pro-Russian news agency African Initiative, have historically mixed disinformation with real information, which bolsters their credibility and allows them to deny any involvement. Furthermore, given Russia's track record of deepfakes and AI-assisted disinformation in Ukraine and elsewhere, it is likely that Africa Corps also resorts to this on a larger scale than can currently be verified.

In the 2024 report *AI Extremism: Technology, Tactics, Actors*, Stephane Baele writes:

"Generative AI content has been observed in information operations conducted in West Africa, generally — though not exclusively — as part of processes supported or directly led by Russia and pro-Russian operators. Soto-Mayor, Mare and Onanina (2023), for example, discuss the production of deepfakes by 'digital mercenaries' hired to create disinformation in electoral contexts, aimed at stoking

radical sentiment against political opponents. The investigative journalism collective All Eyes on Wagner (2023) uncovered short nationalist, anti-Western deepfake videos, distributed by inauthentic social media accounts created by the Wagner Group as part of its efforts to reshape the information space in Burkina Faso ahead of its military intervention."

1- Russia and the Use of Generative AI: A State Strategy "Unmasked"?

Unlike the FLA case studies presented above, whose analyses rely on visual markers within individual pieces of content, Russia's use of generative AI in Mali has already been documented in reports from platforms and states alike.

In 2024, OpenAI and Meta identified a Russian operation using OpenAI's models to generate comments, articles and images in English and French, intended for distribution on social media accounts targeting sub-Saharan Africa, including Mali. Meta removed 37 Facebook accounts and 29 pages linked to this network for violating its policy on "coordinated inauthentic behavior." In its report, OpenAI estimated that these images did not appear designed simply to misinform, but rather to "catch the eye, so as to make articles or social media posts more engaging."

A similar technical report, produced jointly by France's foreign digital interference watchdog VIGINUM, the UK Foreign, Commonwealth and Development Office (FCDO), and the European External Action Service

(EEAS), identifies a specific information manipulation set nicknamed "AI-Freak," owing to "its deceptive nature, both in its use of AI-generated content ... and in its unethical search-engine-optimization strategy."

An information manipulation set (IMS) refers to a malicious actor's specific digital footprint, behaviors, tools and tactics, enabling analysts to link isolated online incidents to broader strategic campaigns. It is this analytical framework that revealed that AI-Freak and the Russian operation flagged by Meta and OpenAI were one and the same. Analysts also determined that AI-Freak had been produced by a subcontractor of African Initiative, a media outlet identified as a Russian propaganda platform disseminating anti-Western, pro-Kremlin messages in several languages, thereby serving as Africa Corps' media arm, particularly active in disinformation operations against France in the Sahel.

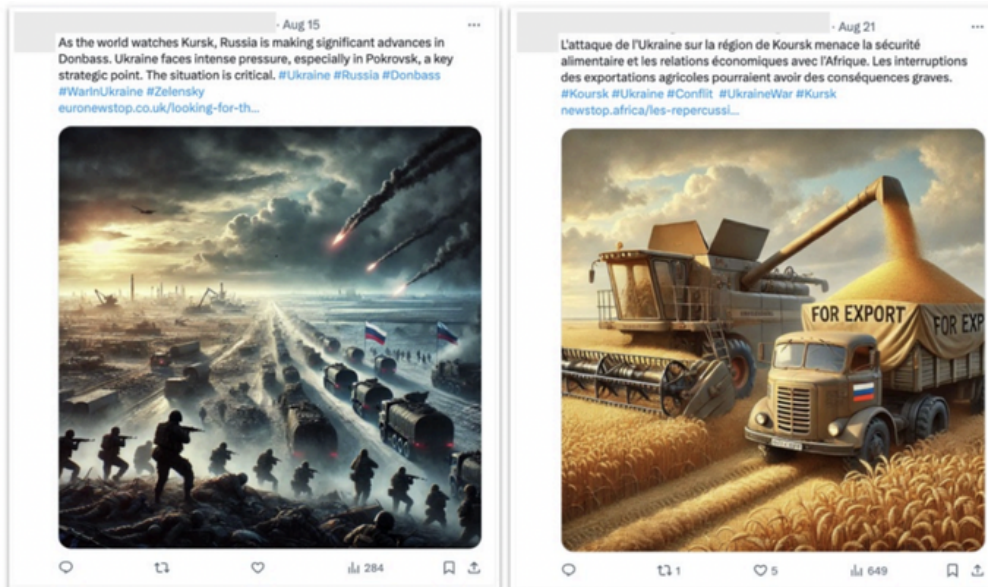


Figure 9: Two screenshots of posts on X, taken from OpenAI's report, showing how Russia uses generative AI to create brief pro-Kremlin news articles.

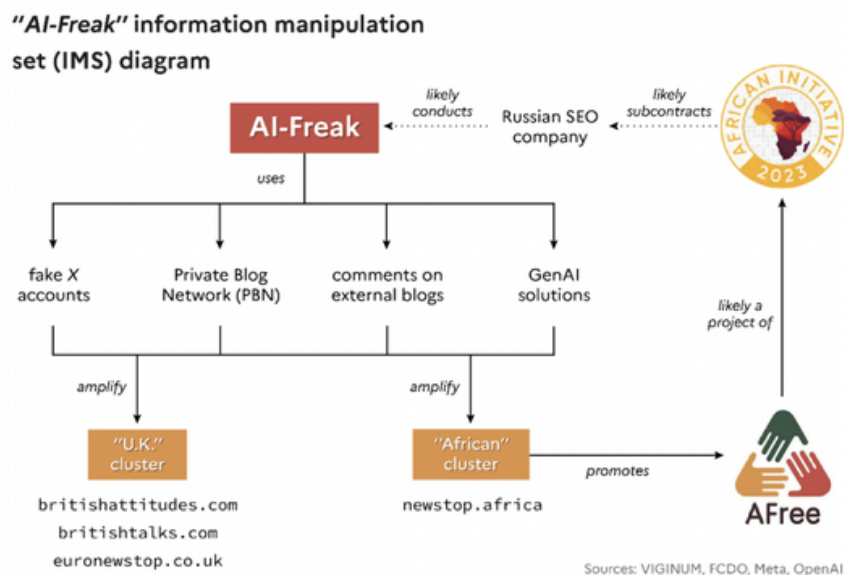


Figure 10: Diagram of the "AI-Freak" IMS, taken from the joint report by VIGINUM, the FCDO and the EEAS.

The report further links African Initiative's founder, Artem Sergeyevich Kureyev, the network of former Wagner Group chief Yevgeny Prigozhin, and the Russian state as a disinformation actor within an information war fueled by geopolitical rivalries in the Sahel. This would therefore not be an isolated event. The Africa Center for Strategic Studies reported that between 2018 and the article's 2024 publication, nineteen Russian disinformation campaigns had targeted Mali, Burkina Faso and Niger, describing these campaigns as being "produced on an industrial scale."

A similar operation was uncovered in April of this year, in which OpenAI's models were used to create a fake academic commentator named Dr. Manuel Godsins, who published

geopolitical commentary incorporating pro-Kremlin propaganda targeting Mali and other sub-Saharan states. Generative AI has become a crucial tactic within Russia's information-warfare strategy. The ability to deny any involvement, combined with the sheer scale of the AI operations conducted by Moscow and its Africa Corps, sets the sophistication of state disinformation apart from that of non-state actors like JNIM and the FLA, and allows Russia and its security partners to readily saturate the information space in pursuit of their strategic objectives.

D- Manufacturing Legitimacy: Generative AI, Media Control and the Malian Regime's Information Strategy

The ruling Malian regime has shown some signs of isolation in recent months, with a growing dependence on support from the Russian state and Africa Corps. The second-largest sponsor of disinformation in the Sahel after Russia, according to a mapping by the Africa Center for Strategic Studies, the Alliance of Sahel States (AES), formed by the ruling regimes of Mali, Burkina Faso and Niger, replicates Russian information-warfare strategies in order to bolster the legitimacy of the current rulers. By drawing on Russian disinformation techniques, the military regimes manage to legitimize their power while designating France, the United Nations, the Economic Community of West African States (ECOWAS) and human-rights organizations as scapegoats — a tactic that feeds anti-Western narratives, particularly among young people.

From this standpoint, Russian support both bolsters regime stability and strengthens its capacity to control the information space.

Through Africa Corps (and previously Wagner), Russia is reported to be pursuing a strategy of using bots and AI-generated content to amplify pro-AES communication online. These regimes then tighten their grip on the media space by leaving little freedom to national journalists and banning recognized international media outlets, thereby steering citizens toward exclusive consumption of content controlled by Russia, the government and their relays.

E- Africa Corps to the Rescue: The Digital Space as an Alternative Battlefield ?

This phenomenon of intensive content production through AI and distribution across various channels is reinforced by other unofficial but pro-AES online accounts. One of them, @6tm_officiel on TikTok, had amassed, as of July 9, 2026, 436,100 followers by posting AI-generated content favorable to the Malian Armed Forces (FAMA), often featuring battlefield successes against JNIM and the FLA.

Other videos posted by this account reached as many as 4.7 million views. The account is linked to an individual based in Bamako, who runs similar accounts on Instagram, Facebook and YouTube. A video (Figure 11), posted on May 17, 2026, shows FAMA and Africa Corps retaking Kidal, after the city's successful capture by JNIM and the FLA during the April attacks.



Figure 11: Screenshots of the @6tm_officiel post showing FAMA and Africa Corps retaking Kidal.

AI-generated content favorable to the military, combined with the Malian regime's gradual adoption of Africa Corps' disinformation methods and resources, poses a new challenge to peace efforts in the Sahel. Used as a mechanism of both political control and manipulation of information and opinion, AI-generated content serves to divert local populations' attention and mislead them about the actual security situation.

As deepfakes become more accessible, it is likely that the Malian regime and other AES members will independently integrate generative AI into state-backed information operations to retain political and public-opinion control, drawing further on the Russian strategy in Ukraine and the Sahel.

II- GENERATIVE AI AND THE EVOLUTION OF THE MALIAN CONFLICT: WHAT LIES AHEAD ?

Each of the actors examined in this report integrates generative AI into its information operations to varying degrees: they instrumentalize bots, their broader support bases and their official channels in order to bolster their credibility and weaken their adversaries with greater effectiveness and efficiency.

As noted above, the fast, visually striking use of AI-generated posters widely disseminated through Az-Zallaqa requires fewer technical skills than traditional graphic design, enabling JNIM to make quality propaganda material go viral in order to boost fighter morale, recruit new insurgents and control the political-ideological narrative.

A- Generative AI: A Genuine Opportunity for "Glocal" Jihadist Recruitment ?

It bears recalling that the Islamic State had already developed AI chatbots to personalize propaganda messages according to the individual psychological vulnerabilities of recruitment targets. With the possibilities that generative AI is beginning to offer, JNIM could plausibly adopt a similar strategy: a Telegram chatbot is already capable of assessing the aspirations, frustrations and convictions of a young person within recruiters' reach, then dynamically and progressively adapting its message to maximize psychological appeal toward violent extremist groups.

From this perspective, this new development could pose complex challenges in the years ahead for countries in the region, which will need to readjust and update their violent extremism prevention and countering policies. Current violent extremism prevention (PEV) strategies, built around the binary push-and-pull-factor paradigm, rely essentially on community outreach, religious counter-narratives and socio-economic inclusion programs. It should be noted that these approaches operate at a collective and generic level, whereas AI-assisted or AI-generated recruitment operates at an individual and increasingly hyper-personalized level. Field actors face colossal challenges, with questions bound to arise in the coming years such as: How can one counter a message dubbed into Mooré, Malinke, Wolof or Fulfulde without multilingual AI production capabilities? How can chatbots designed to automate jihadist propaganda be identified without expertise in algorithmic detection? How can illiterate populations be reached with written prevention messages ?

In other words, one of the major implications of this communicational shift will be a growing strategic gap between the stagnation of traditional strategies and the increasingly automated sophistication of a threat that is paradoxically delocalized yet impacts local communities ever more closely, against a backdrop of relatively stagnant resilience capacities in Mali and across the region.

At the same time, the generative AI used by the dubious online personas allegedly affiliated with the FLA offers an additional layer of operational security in terms of anonymity and digital camouflage, while also serving as a recruitment and communication tool. Accounts featuring children and teenagers easily reach a younger audience and can contribute to the recruitment and radicalization of disillusioned youth. AI-powered bots on social platforms such as Telegram or Matrix enable mass messaging and recruitment campaigns without requiring the manpower that JNIM has traditionally needed and lacked compared with IS.

A May 2024 report by the SITE Intelligence Group noted that it remains difficult, for now, to gauge just how much of a boon AI represents for terrorists, given their current reliance on conventional media and content-production processes: "Productions that once required weeks, even months, mobilizing teams of writers, editors, video editors, translators, graphic designers or narrators, can now be produced with AI tools by a single person in a matter of hours."

B- A More Threatening Use of Generative AI: How to Address Increasingly Unrestrained and User-Friendly AI ?

Across the various case studies examined above, it should be noted that artificial intelligence is becoming increasingly user-friendly or "jailbroken," referring to agents capable of bypassing control mechanisms to operate offline. Although many AI companies are aware of the dangers posed by their models and build in safety tools, it remains relatively simple to craft prompts designed to bypass the built-in guardrails of large language models (LLMs), or to obtain software enabling offline operation and the complete neutralization of safety filters. AI agents are becoming more accessible and models less costly; as their sophistication increases, it simultaneously becomes harder for both authorities and the public to detect and verify them. The ability to deny involvement serves the interests of the actors involved, each seeking to preserve its own credibility while delegitimizing its adversary.

If JNIM and the FLA are exploiting AI in their propaganda and recruitment efforts, they are likely also using AI tools for other, less visible or less recognizable tasks. Africa Defense Forum recently reported that "JNIM appears to have used loitering drones and AI to quickly and more effectively recalibrate its targeting [against Malian and Africa Corps positions]" during the April 25 attacks. Generative AI also offers a range of possibilities to non-state actors who lack access to advanced operational planning and analysis software. Through fine-tuning, these AI models can provide the readily mobilizable know-how and resources needed to identify targets, facilitate attacks and strengthen operational security.

C- From the Virtual to Sophisticated Weapons: Is AI Redrawing the Military Balance of Power ?

The partnership between the Malian regime and Africa Corps illustrates an even more acute manifestation of this issue. As formally state-backed programs, each has enhanced access to resources and thus a strengthened capacity to refine its operations, increasing the risk of state-backed, AI-generated disinformation, such as execution videos attributed to Africa Corps or deepfakes of junta officials.

It is also worth noting that, given the global AI ecosystem, this issue extends well beyond the scope of information warfare in Mali. Given Russia's access to autonomous weapons and the possibility that such weapons could be integrated into combat operations by the Malian regime and Africa Corps, the spread of AI-centered strategies in the Malian conflict is a serious concern for Sahelian security.

D- AI as a Technological Accelerator of the Malian Conflict and an Uneven Force Multiplier

The risks outlined above point to a broader debate on more advanced and more threatening uses of AI on the horizon. The impact of drones combining intelligence, surveillance and reconnaissance (ISR) capabilities with strike capabilities on the Malian battlefield can be amplified by artificial intelligence, notably through the integration of drones capable of autonomous targeting. With the proliferation of this type of weapon, it has already been observed that "easy access to modifications and offline AI has made it easier for these groups to build drones and carry out attacks."

Likewise, the expansion of artificial intelligence in the public space provides extremist groups with advanced, accessible tools to refine their practices. With the "democratization of AI" — that is, the shift toward increasingly user-friendly interfaces in the public domain — combined with the know-how and resources that affiliates can provide, information warfare in the Sahel could thus be reinforced by the combination of these tools and networks.

Furthermore, AI could also have a negative impact if misused within decision-making models. These models make strategic decisions autonomously in complex environments, drawing on pattern-recognition models previously developed to identify new occurrences of a given element based on patterns spotted in their training data. These decision-making models can, however, easily be repurposed. For example, dual-use models designed to discover new drugs can be modified or reversed to develop biological and chemical weapons. While such models are more advanced and unlikely to pose a threat in the hands of non-state actors in the immediate future, the rapid development and spread of AI calls for close monitoring of these advances going forward. Moreover, although this analysis focuses primarily on generative AI, the dangers posed by other AI models must also be acknowledged, particularly if state and non-state actors alike begin to rely on them more heavily. AI in general offers greater potential to amplify recruitment, communication and operational security, as well as the nature and scale of attacks; decision-making and pattern-recognition models could further accentuate this reality in the future.

As the Malian battlefield becomes a veritable AI laboratory, with different fighters experimenting with its use across various formats and platforms, the rapid rise in its use cannot be ignored. Each actor's ability to deploy AI, and the resulting effectiveness, depends on its level of sophistication, itself derived from its degree of technological advancement, financial resources and experience. Although advanced forms of artificial intelligence pose a lesser degree of risk for non-state actors such as JNIM and the FLA, there is nonetheless a significant advantage to pursuing AI-based strategies. As this study shows, AI represents a new mode of action for combatants, and as each side conducts shaping operations in support of decisive combat operations, each is likely to seek to develop its AI-based capabilities, both in information operations and in kinetic operations. The development of artificial intelligence therefore constitutes a serious threat owing to its potential use as a force multiplier.

While AI-assisted kinetic operations remain, at this stage, a more distant possibility on the Malian battlefield, generative AI is already decisively shaping each side's narratives. As AI continues to blur the boundaries of official sources and becomes harder to distinguish from reality, unsuspecting audiences remain vulnerable to taking narratives at face value and believing in an accelerated disinformation that has become a genuine weapon of war.

As a result, the information space is becoming increasingly saturated even as AI literacy remains low. In a sense, AI could help exacerbate the conflict in the Sahel and hinder or complicate its resolution, with each actor exploiting this technology to its own advantage. Sahelian security strategies must, as a matter of urgency, include efforts to counter the uncontrolled penetration of AI into information warfare, as well as its possible use on tomorrow's battlefields, where it will henceforth combine accelerated, increasingly sophisticated information warfare with a blurring of the boundaries between the state, the non-state and the uncontrolled virtual — with lasting effects on present and future conflicts alike.

Viewed through the lens of generative artificial intelligence, the Malian conflict illustrates a profound shift in informational balances of power across the Sahel. This study highlights a variable-geometry appropriation of GenAI, shaped by each actor's resources, technical expertise and strategic objectives. JNIM, still in a phase of limited but potentially evolving experimentation, uses generative AI mainly for propaganda purposes, while hinting, through the model developed by the Islamic State, at a possible trajectory of intensification toward video production, multilingual translation and hyper-personalized recruitment. The FLA and its support base, for their part, draw on the communicational resources of a more decentralized and diffuse form of AI, embodied by synthetic characters that humanize the Azawad cause while blurring the line between organic sympathizer appeal and coordinated production of communication materials. At the other end of the spectrum, Africa Corps and the Malian regime demonstrate a state-driven, professionalized and systemic adoption of generative AI, extending methods already tested by Russia in Ukraine and elsewhere on the continent, with a capacity for plausible deniability and information saturation unmatched by non-state actors.

The picture painted in this report reveals a common denominator: whatever the level of sophistication, generative AI acts as a force multiplier that lowers technical barriers, accelerates cycles of communicational — and even propagandist — content production, and complicates message attribution. In fact, AI does not yet create new fault lines in Mali, but it amplifies and accelerates those that already exist, whether communal, ideological, geopolitical or otherwise. Through the upheavals it introduces, it makes them harder to detect, counter and defuse. The Malian conflict is thus becoming an open-air laboratory where the civilian and military uses of still-lightly-regulated technologies are being tested in real time, with repercussions that extend well beyond national borders and concern the Sahel region as a whole.

NOTES & REFERENCES

-Although the images and videos analyzed in this report display various indicators of AI generation — including scale inconsistencies, pronounced stylization and reduced coherence in dense areas — we cannot state with certainty, absent professional forensic analysis, that this content is indeed a product of generative artificial intelligence.

-Henk van Ess, "Reporter's Guide to Detecting AI-Generated Content," Global Investigative Journalism Network, September 1, 2025, <https://gijn.org/resource/guide-detecting-ai-generated-content/>. and Rob Laughter, "Is That Image AI? Here Are 14 Telltale Signs to Look For," Medium, May 2, 2024, <https://roblaughter.medium.com/is-that-image-ai-here-are-14-telltale-signs-to-look-for-d40e5cff2d0a>.

-Fabrizio Minniti, "Automated Recruitment: Artificial Intelligence, ISKP, and Extremist Radicalisation," GNET (Global Network on Extremism and Technology), April 11, 2025, <https://gnet-research.org/2025/04/11/automated-recruitment-artificial-intelligence-iskp-and-extremist-radicalisation/>.

-The Soufan Center, "Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts," IntelBrief, October 3, 2024, <https://thesoufancenter.org/intelbrief-2024-october-3/>.

-@azzghim, TikTok video, posted May 22, 2026, archived July 9, 2026, Internet Archive Wayback Machine, <https://web.archive.org/web/20260709151626/https://www.tiktok.com/@azzghim/video/7632411683939503368?lang=en>.

-@azzghim, TikTok video, posted April 24, 2026, archived July 9, 2026, Internet Archive Wayback Machine, <https://web.archive.org/web/20260709151842/https://www.tiktok.com/@azzghim/video/7642809457604447496?lang=en>.

-@asnan831, TikTok video, posted November 7, 2025, archived July 7, 2026, Internet Archive Wayback Machine, <https://web.archive.org/web/20260709142645/https://www.tiktok.com/@asnan831/video/7569944316571995399?lang=en>.

-@asnan831, TikTok video, posted November 10, 2025, archived July 7, 2026, Internet Archive Wayback Machine, <https://web.archive.org/web/20260709152038/https://www.tiktok.com/@asnan831/video/7571236925818932498?lang=en>.

-@asnan831, TikTok video, posted June 1, archived July 7, 2026, Internet Archive Wayback Machine, <https://web.archive.org/web/20260709141143/https://www.tiktok.com/@asnan831/photo/7646317103074561300>.

-Jan-Philipp Stein, Priska Linda Breves, and Nora Anders, "Parasocial Interactions with Real and Virtual Influencers: The Role of Perceived Similarity and Human-Likeness," *New Media & Society* 26, no. 6 (2024): 3433–53, <https://doi.org/10.1177/14614448221102900>.

-"Deepfakes Help Spread False Information in Africa," Africa Defense Forum, September 30, 2025, <https://adf-magazine.com/2025/09/deepfakes-help-spread-false-information-in-africa/>.

-Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: RAND Corporation, 2016), <https://www.rand.org/pubs/perspectives/PE198.html>.

-Stéphane J. Baele and Lewys Brace, *AI Extremism: Technology, Tactics, Actors*, VOX-Pol Reports (Dublin: VOX-Pol Network of Excellence, 2024), 28, <https://hdl.handle.net/2078.5/242669>.

-Meta, *Adversarial Threat Report: Second Quarter 2024* (Menlo Park, CA: Meta, August 2024), <https://transparency.meta.com/sr/Q2-2024-Adversarial-threat-report> and Ben Nimmo and Michael Flossman, *Influence and Cyber Operations: An Update* (San Francisco: OpenAI, October 2024), https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf.

-Ben Nimmo and Michael Flossman, *Influence and Cyber Operations: An Update* (San Francisco: OpenAI, October 2024), https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf, 24.

-VIGINUM, UK Foreign, Commonwealth & Development Office (FCDO), and European External Action Service (EEAS), *Technical Report: African Initiative* (Paris: VIGINUM, June 2025).

NOTES & REFERENCES

-https://euvsdisinfo.eu/uploads/2025/06/VIGINUM_FCDO_EEAS_Technical_Report_African_Initiative.pdf European External Action Service, Building a Common Operational Picture of Foreign Information Manipulation and Interference (FIMI) (Brussels: European External Action Service, 2025), <https://www.disinfo.eu/building-a-common-operational-picture-of-fimi/>

-Africa Center for Strategic Studies, Mapping a Surge of Disinformation in Africa (Washington, DC: Africa Center for Strategic Studies, 2025), <https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-in-africa/>

-Africa Defense Forum, "Kremlin Used AI Fake Author to Pass Off Propaganda," Africa Defense Forum, April 2026, <https://adf-magazine.com/2026/04/kremlin-used-ai-fake-author-to-pass-off-propaganda/>

-See ACSS, Mapping a Surge of Disinformation in Africa <https://africacenter.org/fr/spotlight/cartographie-de-la-vague-de-desinformation-en-afrique/>

-DAIDAC (CJID), Revealed: The AES Shadow Game Fueling Anti-ECOWAS, Anti-Western Disinformation Across West Africa (2025), <https://daidac.thecjid.org/revealed-the-aes-shadow-game-fueling-anti-ecowas-anti-western-disinformation-across-west-africa/>

-@6tm_officiel, posted May 17, 2026, archived July 9, 2026, Internet Archive Wayback Machine, https://web.archive.org/web/20260709152157/https://www.tiktok.com/@6tm_officiel/video/7640810558253550869?is_from_webapp=1&sender_device=pc&web_id=7652355898527335954

-Baldaro, E. (2025). The "Glocal" nature of Jihadist insurgencies?: Conflict, space, land and resources in the Sahel 1. In *Water and Land in the Sahel* (pp. 92-104). Routledge. <https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003429111-6/glocal-nature-jihadist-insurgencies-edoardo-baldaro>

-[Sur la personnalisation des messages selon les profils \(BISI\) : https://bisi.org.uk/reports/isis-adoption-of-generative-ai-tools](https://bisi.org.uk/reports/isis-adoption-of-generative-ai-tools)

-[Sur la prolifération des chatbots extrémistes sur Telegram \(Atlantic Council\) : https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/countering-terrorist-propaganda-in-the-age-of-ai/](https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/countering-terrorist-propaganda-in-the-age-of-ai/)

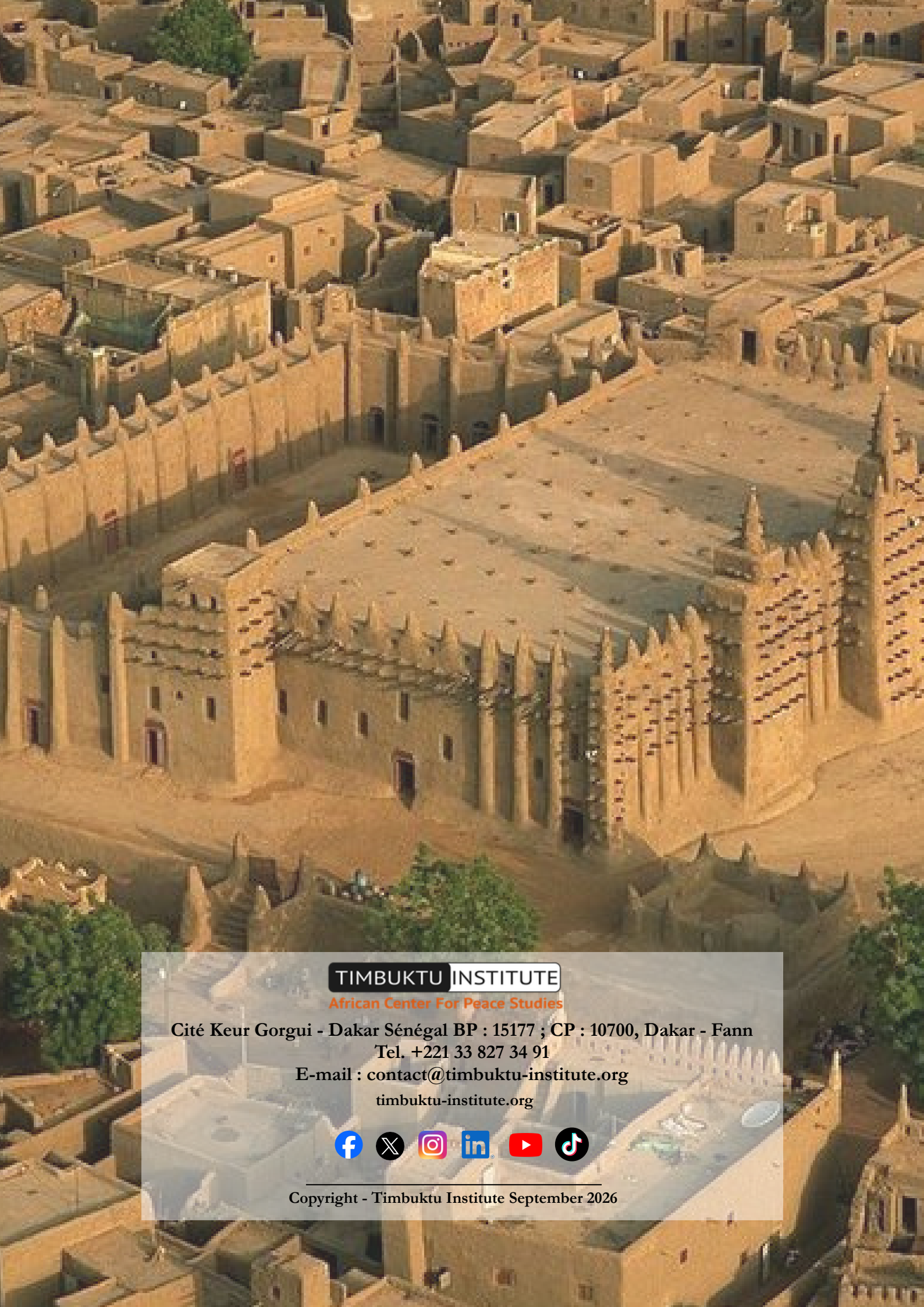
-Africa Defense Forum, "Threats Machine," Africa Defense Forum, February 2026, <https://adf-magazine.com/2026/02/threats-machine/>

-Africa Defense Forum, "Human Skills Are Key to Deploying AI," Africa Defense Forum, June 2026, <https://adf-magazine.com/2026/06/human-skills-are-key-to-deploying-ai/>

-The New York Times, « The World's Leading Deepfake Expert No Longer Trusts His Own Eyes », juin 2026, <https://www.nytimes.com/2026/06/14/us/ai-deepfake-hany-farid.html>

-Ellis, Ben. "Violent Extremism in West Africa." (2026). 12.

-Baele, Stéphane, et al. *AI Extremism: Technology, Tactics, Actors*. VOX-Pol Reports. Dublin: VOX-Pol, 2024. <https://hdl.handle.net/2078.5/242669>. 61.



TIMBUKTU INSTITUTE

African Center For Peace Studies

Cité Keur Gorgui - Dakar Sénégal BP : 15177 ; CP : 10700, Dakar - Fann
Tel. +221 33 827 34 91

E-mail : contact@timbuktu-institute.org
timbuktu-institute.org



Copyright - Timbuktu Institute September 2026