**Russian Influence Tradecraft in the Central Sahel (2019-2025)**

*This report provides an evidence-based assessment of how influence methods evolved in Mali, Burkina Faso, and Niger. Applying the European External Action Service EEAS) Foreign Information Manipulation and Interference (FIMI) framework to distinguish coordinated manipulation behaviors from routine political messaging and to connect observed evidence to practical response options. [3]*

*Baseline window*: January 1, 2019 to December 31, 2022 [3]
*Deep-dive window*: January 1, 2023 to December 31, 2025 [3]

*Prepared for*:
Office of Strategic Communications and Information Security (STRATCOM) (Ukraine)

*Prepared by*:
Jason Jay Smart, PhD & Team

*Date*:
February 17, 2026

Version: 1.1

**INDEX**

## A. GLOSSARY AND ABBREVIATIONS

AI
African Initiative. [1] [2]

AP
Associated Press. [29]

AU
African Union. [8] [9]

AU PSC
African Union Peace and Security Council. [9]

CIB
Coordinated Inauthentic Behavior (Meta platform category). [21] [23]

EEAS
European External Action Service. [2] [3]

ECOWAS
Economic Community of West African States. [10]

EUISS
European Union Institute for Security Studies. [13]

FCDO
United Kingdom Foreign, Commonwealth and Development Office. [1]

FIMI
Foreign Information Manipulation and Interference (EEAS framework term). [3]

IO
Influence operation(s) (term used in threat intelligence and platform reporting). [16] [21] [23] [24]

MINUSMA
United Nations Multidimensional Integrated Stabilization Mission in Mali. [7] [17]

PSC
Peace and Security Council (used here to refer to the AU PSC). [9]

TAG
Google Threat Analysis Group. [24]

ToR
Terms of Reference.

UN
United Nations. [7] [11]

UNSC
United Nations Security Council. [7]

VIGINUM
French service responsible for vigilance and protection against foreign digital interference. [1]

## B. Key Terms (Definitions as Operationalized in This Report)

African Initiative
A documented influence architecture described in the joint VIGINUM-UK FCDO-EEAS technical report and characterized by the EEAS as shifting from public diplomacy styling toward covert influence operations. [1] [2]

Amplification
An increase in reach of narratives through reposting, repetition, cross-outlet reproduction, or distribution behavior. This report treats amplification as potentially organic or coordinated depending on observable indicators. [3] [15] [21]

Attribution
A conclusion about responsibility for an operation or network. This report limits attribution to what authoritative technical reporting or platform enforcement reporting supports and does not infer attribution from narrative similarity alone. [1] [3] [21]

Behavioral indicators
Observable actions consistent with manipulation or interference, including timing patterns, distribution behavior, and network characteristics. These indicators are assessed separately from whether content claims are true or false. [3] [21]

Brand presentation
Outward-facing legitimacy cues, including professional styling and source labeling, that can facilitate diffusion and laundering. In this report, brand presentation is treated as potentially compatible with covert operational behavior. [2]

Closed or semi-closed networks
Channels with limited external visibility that reduce what can be observed through public sources or platform reporting and can extend the persistence of contested claims. [21] [23]

Confidence tiers (Low, Medium, High)
A reporting discipline aligned to the EEAS FIMI approach. Low confidence reflects pattern-based early warning during trigger-event windows without assuming coordination or naming operators. [3] [14] Medium confidence reflects reinforced signals consistent with platform-defined coordination behaviors or repeated analytical findings, while avoiding unproven operator naming. [15] [21] [23] High confidence reflects authoritative technical reporting describing a coherent model or platform enforcement evidence documenting linked assets and network behavior within a platform's services. [1] [21] [23]

Coordinated Inauthentic Behavior (CIB)
A Meta classification for networks that are coordinated and deceptive about identity and/or intent, documented through linked assets and behavioral evidence within Meta services. In this report, it is used as a benchmark for what one major platform treats as coordination when evidentiary thresholds are met. [21] [23]

Deep-dive window
January 1, 2023 to December 31, 2025, used to assess documented method evolution and high-signal institutional anchors. [3]

Ecosystem map
A bounded depiction of nodes and pathways that carry narratives from origin points to wider reach, emphasizing patterns across assets, timing, and distribution rather than single-item content review. [3] [15] [21]

External verification capacity
The ability of independent observers, missions, or credible third parties to confirm contested events and claims during crises. In this report, this capacity is treated as uneven and often constrained. [7] [17]

FIMI (EEAS usage)
An analytical framework that focuses on manipulative behavior and harmful interference effects, prioritizing behavioral indicators and coordination signals. It separates those signals from claim-by-claim truth adjudication. [3]

Hybrid presentation risk
The risk that outward-facing legitimacy cues and professional branding coexist with covert influence activity, complicating detection and enabling laundering through legitimate-seeming channels. [2]

Impact typology (Measurable, Plausible, Uncertain)
A method to avoid over-claiming by separating observable signals and platform-scoped evidence (measurable) from context-consistent effects without causal proof (plausible) and from claims not supported by the evidence base (uncertain). [3] [21] [23] [14] [15] [7] [17] [1]

Institutional frame
The legitimacy language and response positions issued by bodies such as the AU and ECOWAS that become focal reference points for narrative contestation and reframing during crises. [8] [10] [14]

Narrative demand
A surge in audience demand for explanations after political or security ruptures, creating openings for rapid framing before verification stabilizes. [14] [15]

Narrative laundering
The process by which a message gains perceived legitimacy as it moves through successive messengers and formats, often via selective quotation, reframing, and repetition until it circulates as a default interpretation. [3] [15]

Node
A focal point in the ecosystem, such as a branded outlet identity or a cluster of linked assets, from which narratives can be seeded or amplified. [1] [21]

Partial observability
The constraint that open-source research and platform transparency reporting cannot fully reveal closed networks, cross-platform coordination, or offline organization. This constraint requires conservative confidence grading. [21] [23]

Pathway
A sequence through which narratives move from initial appearance into broader reach, including movement from high-tempo online circulation into elite-facing discourse. [15] [8] [10]

Platform transparency reporting
Public reporting by platforms describing investigations, enforcement actions, and observable behaviors within their services, used as evidence with acknowledged scope limits. [21] [23] [24]

Rebranding
The use of outward-facing identity and legitimacy cues to package influence activity in forms that resemble routine public communication while serving covert interference goals. [2]

Rights-safe
An evidence-handling posture that avoids stigmatizing domestic actors without high-confidence evidence, limits personal data handling, and prevents monitoring outputs from becoming a basis for intimidation in constrained environments. [3] [29]

Trigger event
A political or security rupture that predictably accelerates information activity and compresses the time available for verification and response. [14] [7] [8] [10]

Verification gap
The time between the first circulation of a contested claim and the availability of credible independent verification. Under constrained monitoring, this gap can extend narrative persistence. [7] [17]

## 1. INTRODUCTION AND SCOPE

This analysis evaluates how Russian state actors have evolved their influence tradecraft across the Central Sahel, specifically within Mali, Burkina Faso, and Niger [3]. To identify these tactical shifts, the study compares a baseline period from 2019 through 2022 against a deep-dive window from 2023 through 2025 [3]. Researchers utilized the Foreign Information Manipulation and Interference (FIMI) framework developed within the European External Action Service (EEAS), the European Union's diplomatic service. The framework supports analysis based on observable behaviors and interference patterns, helping distinguish coordinated manipulation efforts from routine political communication and informing response options when indicators suggest alignment with Russian-linked activity.

From 2019 to 2022, frequent governance and security shocks triggered recurring bursts of narrative activity throughout the Central Sahel [11, 14]. Open-source research into West African disinformation identified specific patterns relevant to Mali, Burkina Faso, and Niger during this period. These include surges tied to trigger events and the use of reusable narrative templates that can be rapidly adapted to exploit local grievances and political divisions [11, 14].

For the 2023 to 2025 period, the African Initiative is identified as the primary model of rebranded Russian influence architecture. This agency was established by the Russian Ministry of Defense to institutionalize the propaganda assets formerly managed by the Wagner Group, serving as the official media wing for the Africa Corps, Russia's state-controlled successor to mercenary networks. Findings from VIGINUM, the French national agency for monitoring foreign digital interference, and the United Kingdom Foreign, Commonwealth and Development Office confirm that the African Initiative has transitioned from public diplomacy into covert influence operations [1, 2]. This shift highlights a practical distinction between how the brand is presented to the public and how the tradecraft operates [2].

The report identifies the UN Security Council's June 30, 2023 decision to end the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) as a major contextual shift. The withdrawal of peacekeepers removed a key source of ground-level observation, making independent verification harder and slowing external responses when Russian claims circulate. [7]

It also treats the July 26, 2023 coup in Niger and the subsequent actions by the African Union and the Economic Community of West African States (ECOWAS) as high-signal trigger events. These shocks provide a clear window for assessing how Russia exploits regional friction points to undermine Western-aligned institutions. [8, 10]

To avoid overstating impact, the approach separates findings into measurable signals, plausible effects, and unresolved claims. It prioritizes platform-defined indicators of coordination when available. [21]

Meta's adversarial threat reporting is the main reference for identifying coordinated inauthentic behavior. The analysis also notes that platform visibility is partial and cannot capture offline

organization, including on-the-ground efforts used by African Initiative to embed Russian influence in Sahelian communities. [21]

## 2. THREAT MODEL: ACTORS, OBJECTIVES, TARGET AUDIENCES, & CHANNELS

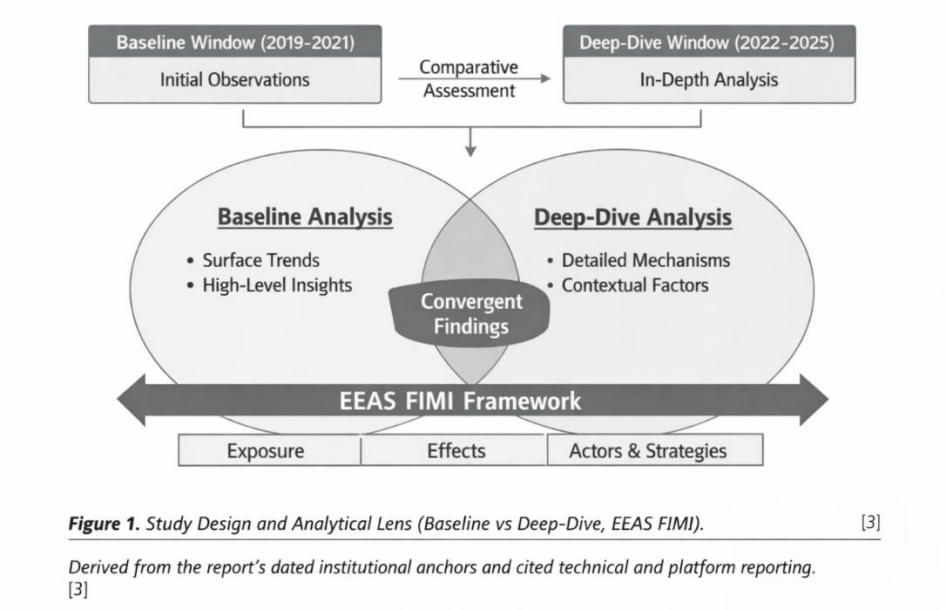



*Figure 1. Study Design and Analytical Lens. Baseline (2019-2022) and deep-dive (2023-2025) comparison framed through the EEAS FIMI approach and the report's core evidentiary anchors. [3] [1] [2] [7] [8] [10] [21] [23] [24]*

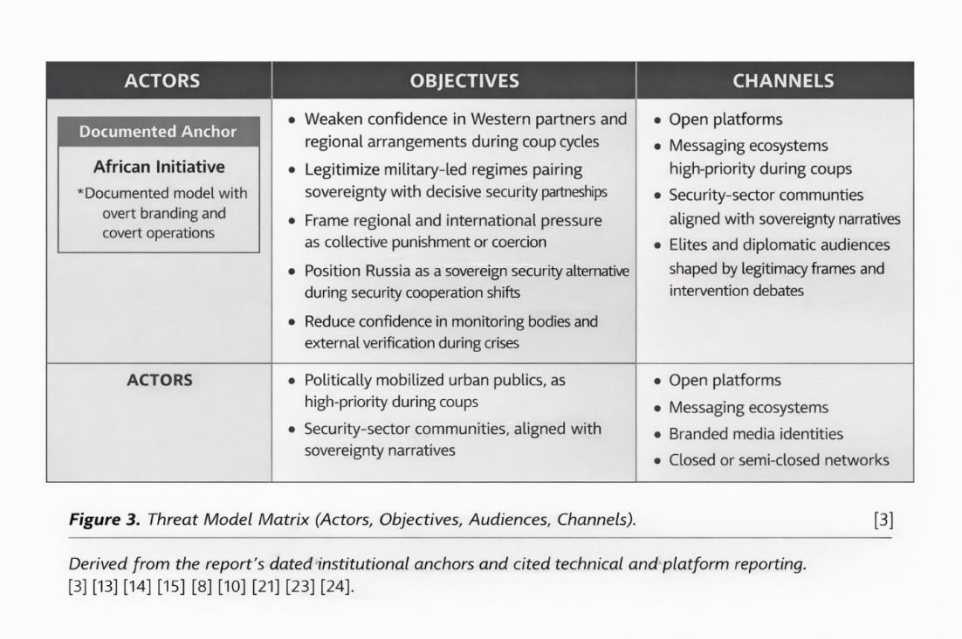
Because this report applies the EEAS FIMI discipline, objectives are framed as hypothesized effects implied by observable behaviors and interference patterns, not as claims of proven persuasion outcomes. They are derived from recurring trigger-event dynamics and the documented use of sovereignty, legitimacy, and verification frames during crisis windows. [3] [14] [15] The list below is used as a working guide for monitoring and response planning. [3]

a. Erode confidence in Western partners and regional arrangements, especially during coup cycles when blame is being assigned. [14, 15]
b. Bolster military-led regimes by pairing sovereignty rhetoric with claims of decisive security cooperation with Russia. [14]
c. Cast regional and international pressure as neo-colonial coercion or collective punishment, deflecting blame from domestic governance failures. [14]
d. Position Russia as the preferred sovereignty and security partner by using shifts in security cooperation to build credibility in local discourse. [13]
e. Undermine trust in monitors and external verification, weakening institutional authority during crises. [3]

Target audiences are grouped to reflect that influence activity is designed for different layers of the public and decision-makers. [3]

a. Politically mobilized urban publics, because they can amplify narratives quickly on social platforms during coups and legitimacy contests. [14]
b. Security-sector communities, because sovereignty and security narratives align with institutional loyalties and lived insecurity. [13]

c. Elite and diplomatic audiences, because legitimacy frames shaped by African Union (AU) and the Economic Community of West African States (ECOWAS), a regional bloc of 15 West African countries created in 1975 to promote economic integration, including trade and free movement; Later taking a major security and political role in the region. responses can be reinforced or eroded through narrative contestation. [8, 10] The July 26, 2023 Niger coup response cycle provides a clear test case. [8, 10] In Mali, the end of MINUSMA reduced independent visibility and increased reliance on external reporting and transnational amplification. [7] The International Peace Institute notes that mission dynamics shape information access and situational awareness constraints. [17]



| ACTORS | OBJECTIVES | CHANNELS |
|---|---|---|
| **Documented Anchor**<br>**African Initiative**<br>*Documented model with overt branding and covert operations | • Weaken confidence in Western partners and regional arrangements during coup cycles<br>• Legitimize military-led regimes pairing sovereignty with decisive security partneships<br>• Frame regional and international pressure as collective punishment or coercion<br>• Position Russia as a sovereign security alternative during security cooperation shifts<br>• Reduce confidence in monitoring bodies and external verification during crises | • Open platforms<br>• Messaging ecosystems high-priority during coups<br>• Security-sector communties aligned with sovereignty narratives<br>• Elites and diplomatic audiences shaped by legitimacy frames and intervention debates |
| **ACTORS** | • Politically mobilized urban publics, as high-priority during coups<br>• Security-sector communities, aligned with sovereignty narratives | • Open platforms<br>• Messaging ecosystems<br>• Branded media identities<br>• Closed or semi-closed networks |

***Figure 3.*** *Threat Model Matrix (Actors, Objectives, Audiences, Channels).* [3]

*Derived from the report's dated institutional anchors and cited technical and platform reporting.*
[3] [13] [14] [15] [8] [10] [21] [23] [24].

*Figure 3. Actor model anchor, operational objectives, audience clusters, and channel environment as defined in the report's evidence base. [1] [2] [3] [13] [14] [15] [8] [10] [21] [23] [24]*

Channels and distribution systems include open platforms, messaging ecosystems, and branded media identities. [21] Closed or semi-closed networks reduce external visibility, limiting what can be measured with confidence using public indicators. [21] Meta reporting shows how operators use social platforms for distribution and blend multiple activity types across linked assets. [21, 23] Because detection is incomplete, attribution should remain conservative when evidence is partial. [23] Google Threat Analysis Group (TAG) bulletins provide secondary support on how major platforms describe influence operations and enforcement. [24] The joint technical report supports a focus on organized models that use a public-facing identity for amplification and recruitment. [1] EEAS analysis supports attention to the overlap between overt communication and covert coordination. [2]

Offline enablers are treated cautiously because they are difficult to observe through public sources and carry political risk. [1] Constraints in the operating environment shape both influence activity and the range of viable countermeasures. [3] In Mali, the end of the

MINUSMA mandate is treated as a structural shift that reduced independent observation and changed monitoring conditions. [7] The International Peace Institute notes that mission dynamics affect information access and situational awareness. [17] Civic space and journalist safety are treated as operational constraints because intimidation or detention narrows the reporting environment and raises the cost of local monitoring. [29] Associated Press reporting on the arrest of prominent journalists in Mali is used as a concrete indicator of this constraint. [29]

## 3. METHODS AND TRADECRAFT EVOLUTION

From January 1, 2019, to December 31, 2022, influence activities in Mali, Burkina Faso, and Niger followed a consistent set of patterns that emerged during every major crisis [14]. Researchers across West Africa identify a standard sequence:

a. A political rupture or security shock triggers immediate uncertainty.
b. Creates a demand for explanations that are rapidly satisfied by amplified messaging across various channels [15].

During this baseline period, most narratives appear reusable. Familiar claims and frames reappear across different countries whenever instability or mass mobilization occurs [14]. Examples from Burkina Faso provided by the Wilson Center ground these patterns in real-world effects, though they require precise phrasing regarding attribution and coordination [18].

In Mali, baseline conditions dictate what influence operations can achieve and what monitors can verify [11]. High insecurity and contested governance often delay independent verification, particularly during fast-moving events where rumors travel faster than evidence [11]. United Nations reporting clarifies the security environment, explaining why claims circulate so quickly and why validating contested events in real time remains difficult [11].

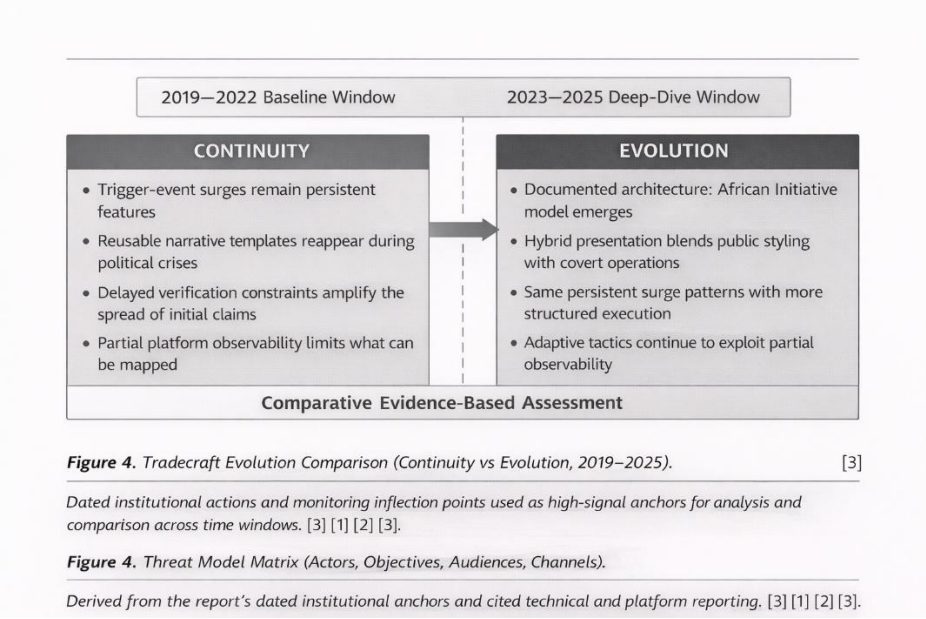



***Figure 4.*** *Tradecraft Evolution Comparison (Continuity vs Evolution, 2019–2025).* [3]

*Dated institutional actions and monitoring inflection points used as high-signal anchors for analysis and comparison across time windows.* [3] [1] [2] [3].

***Figure 4.*** *Threat Model Matrix (Actors, Objectives, Audiences, Channels).*

*Derived from the report's dated institutional anchors and cited technical and platform reporting.* [3] [1] [2] [3].

*Continuities in trigger-event surge dynamics and reusable narrative templates, alongside documented method evolution toward structured, rebranded influence architecture in 2023-2025. [14] [15] [1] [2] [21] [23] [24]*

Platform enforcement data provides a clearer view of coordination once it meets specific evidence thresholds [21]. Meta's adversarial threat reporting defines coordinated inauthentic behavior and details how the company disrupts networks on its services [21]. Meta's recent reporting also highlights tactical adaptation, noting that mixed operator types and shifting behaviors make detection harder [23]. This is a critical point in this analysis as platform visibility

is naturally limited: it cannot fully account for offline organization or coordination that occurs across different platforms [21, 23].

A specific context for the 2023–2025 period is that operations linked to known Russian actors often persist after leadership changes or reputational shocks [16]. Google Cloud threat intelligence suggests that campaigns from these actors continue in modified forms. This justifies a conservative analytic stance: researchers should prioritize looking for continuity and asset reuse rather than assuming a clean break [16]. However, this is not treated as Sahel-specific attribution, nor does it prove that a single operator controls all narratives in Mali, Burkina Faso, or Niger [16].

Across both the baseline and deep-dive windows, the objective is to describe evolution using defensible sourcing and disciplined language [1]. Documentation regarding African Initiative reveals a model that blends public identity with repeatable, organized practices [1, 2]. Meanwhile, Meta's reporting confirms that coordination can be evidenced through observable network behavior and linked assets, even as evolving tactics weaken traditional detection signatures [21, 23]. Baseline research proves that trigger-event surges and reusable templates remain permanent features of the Central Sahel information environment, even as the "packaging" of these operations changes [14, 15].

The Niger coup attempt on July 26, 2023, serves as a high-signal example of how trigger events generate immediate legitimacy messaging [8, 10]. Monitoring through such windows should focus on timing and messenger patterns. Rapid convergence across channels can help distinguish organic repetition from coordinated behavior [21]. The African Initiative report suggests that organized models can successfully mobilize local amplifiers. This increases the likelihood that high-impact messaging appears locally generated while still reflecting a coordinated strategy [1]. The EEAS framing of African Initiative as a bridge between public diplomacy and covert influence serves as a warning: narratives can move through legitimate public channels while being reinforced by hidden amplification [2].

Meta's reporting demonstrates that while coordination is detectable through network behavior, many operations remain only partially visible [21]. This partial visibility becomes more likely as tactics shift toward closed networks or rely on offline organization [23]. Google's Threat Analysis Group (TAG) suggests that while platform transparency provides useful indicators, it does not offer a complete map of influence infrastructure [24]. Finally, the African Initiative report underscores that organized models can blend overt presentation with covert coordination. This creates a clear need for conservative confidence grading when evidence remains incomplete [1].

## 4. ECOSYSTEM MAP: KEY NODES, FRONTS, OUTLETS, AMPLIFIERS, AND INFRASTRUCTURE

Ecosystem mapping involves identifying the specific nodes and pathways that enable influence activities to travel from an origin point to a broad audience in Mali, Burkina Faso, and Niger [3]. The core unit of analysis is the connected system: this includes content sources, branded media identities, amplifiers, and the various channels where narratives are introduced, reframed, and redistributed during crises [15]. The European External Action Service (EEAS) FIMI framework supports this methodology because it prioritizes coordinated behavior and interference effects. These elements are often more visible as recurring patterns in timing and distribution than as isolated pieces of content [3]. While public sources can map certain digital assets and public entities, they rarely provide a full view of offline organization, closed networks, or coordination across multiple platforms [21]. Recent adversarial threat reporting from Meta reinforces the fact that platform visibility is naturally limited to what a company can observe and disclose within its own ecosystem [23].

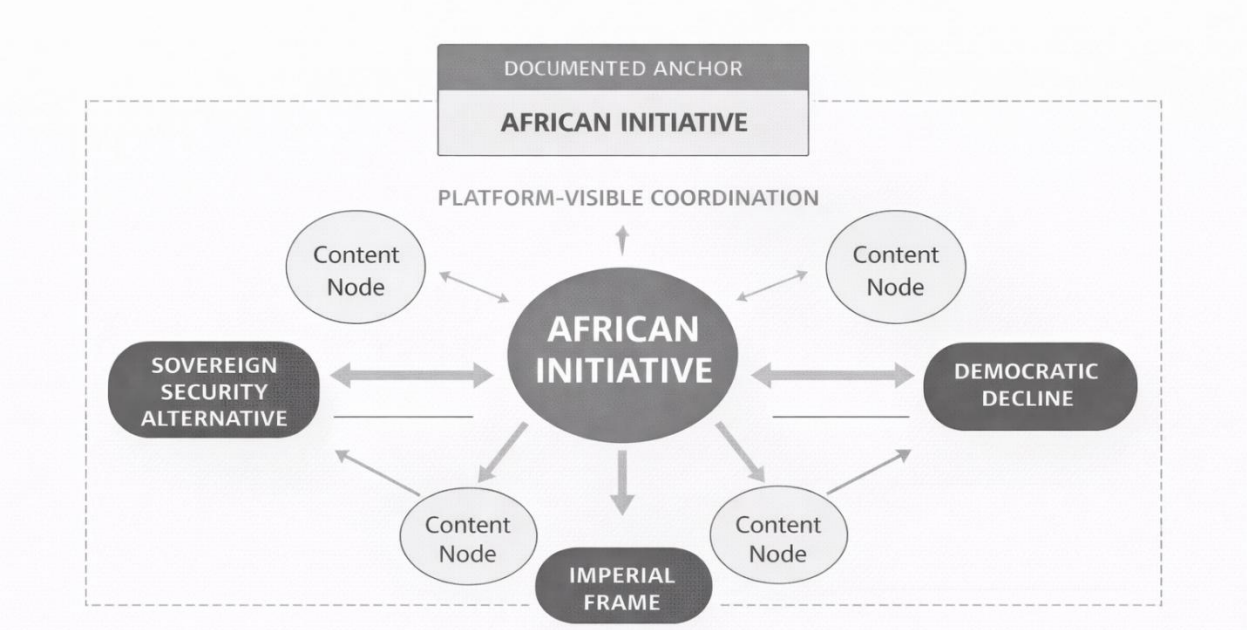



***Figure 5.*** *Ecosystem Map (Bounded Nodes and Pathways).*

Key documented node (African Initiative), platform-visible coordination layer, and principal narrative movement pathways, presented as a bounded system map rather than a comprehensive network map. [1] [2] [3] [21] [23] [7] [17] [8] [10] [15]

*Key documented node (African Initiative), platform-visible coordination layer, and principal narrative movement pathways, presented as a bounded system map rather than a comprehensive network map. [1] [2] [3] [21] [23] [7] [17] [8] [10] [15]*

In the 2023-2025 period, official technical disclosure provides a defensible anchor for treating one branded entity as a structured influence model rather than a generic media label. This report uses African Initiative as that anchor to map nodes, pathways, and observable amplification

behaviors during trigger-event windows. [1] [2] In the deep-dive window from January 1, 2023, to December 31, 2025, the most clearly documented node is African Initiative. This is based on a joint technical report from VIGINUM, the UK Foreign, Commonwealth and Development Office, and the EEAS [1]. This evidence allows researchers to treat African Initiative as a structured influence architecture with a public identity and operational traits that facilitate narrative amplification [1]. The EEAS frames African Initiative as spanning the gap between public diplomacy and covert operations; therefore, the entity functions as much more than a traditional media outlet [2]. While this report uses African Initiative as a primary case for analyzing tradecraft in the 2023–2025 period, it does not suggest that any single node controls the entire Central Sahel information environment [1].

The documentation on African Initiative also explains why branded identity functions as infrastructure rather than simple aesthetics [2]. Effective branding builds legitimacy reduces skepticism among audiences and allows narratives to enter local and cross-border discourse with less friction [2]. The decision by multiple governments to issue a joint assessment suggests they found the evidence of this node's coherence to be significant enough for coordinated disclosure [1]. This makes it a reliable anchor for ecosystem analysis. However, it is still necessary to separate what is documented about the node from what remains unknown regarding its local partnerships or offline command structures in the Sahel [1].

A second layer of mapping focuses on platform-visible coordination. This approach is valuable because it connects ecosystem claims to observable behaviors and linked assets rather than relying on guesswork [21]. Meta’s reporting shows how platforms document coordinated inauthentic behavior through networks of accounts and pages, identifying specific linkages that suggest coordination rather than organic growth [21]. Later reporting highlights that operations are evolving toward mixed operator models and adaptive behaviors. These shifts weaken standard detection markers and require more conservative confidence grading in ecosystem mapping [23].

Mapping based purely on platforms remains limited by design and partial observability [21]. Reports from Meta reflect only what is detectable in their own services; they cannot account for offline organization or the full scope of distribution across different platforms [21, 23]. Additionally, evidence suggests that operators are shifting tactics toward spaces where detection is harder, such as closed networks and less transparent messaging channels [23].

In the Central Sahel, pathways are as critical as nodes because influence depends on how narratives move during fast-paced political events [15]. Research into disinformation surges in Africa shows that trigger events create waves of messaging and sudden demand for narratives across channels [14]. Coup attempts are a recurring trigger; specifically, the Niger coup attempt on July 26, 2023, serves as a primary example for pathway analysis [8]. This event created an immediate contest for legitimacy where regional institutions took formal positions that became the foundation for narratives about sovereignty and foreign intervention [8]. The ECOWAS statement on July 30, 2023, demonstrates how official decisions become narrative scaffolding that is repeatedly excerpted and reframed [10].

1. The first high-value pathway is the movement of narratives from high-tempo online circulation into elite-facing discourse [8]. The African Union's condemnation of the Niger coup shows how the language of constitutional order becomes a central frame for diplomatic decision-making [8]. These official positions can be selectively quoted and reintroduced into local discourse as either external validation or a form of coercion [10]. Research on West African disinformation supports the idea that these reframing moments act as predictable accelerants that move narratives across different audience layers [15].

2. The second pathway moves from branded media identities or influence nodes into local discourse through amplification that mimics organic speech [2]. The EEAS characterization of African Initiative suggests that the overlap between outward messaging and covert reinforcement is a major risk, particularly during trigger events when audiences seek rapid explanations [2]. Technical reporting provides the basis for viewing African Initiative as a node capable of driving such pathways through its documented model [1].

3. A third pathway is defined by constrained visibility and reduced monitoring capacity, which impacts both: 1. Influence dynamics; and 2. The ability to verify information [7]. The decision to end the MINUSMA mandate in Mali on June 30, 2023, marked a significant change in the monitoring environment [7]. Assessments from the International Peace Institute support the claim that mission context and access conditions determine what can be observed and communicated during crises [17]. When visibility is limited, narratives can circulate longer without rebuttal from independent sources, leading to a greater reliance on indirect reporting and transnational amplification [17].

4. The fourth pathway involves platform enforcement acting as a sudden shock to detectable network segments [23]. Disruption often forces operators to change their tactics, platforms, or identities. Meta's reporting on the evolution of these operations suggests that enforcement pressure can accelerate the migration of these actors toward less visible channels [23]. At the same time, earlier reporting confirms that coordinated inauthentic behavior remains a definable category when it is detectable through network linkages and repeated distribution patterns [21].

## 5. NARRATIVE LAUNDERING PATHWAYS (ORIGIN TO MAINSTREAM)

Narrative laundering is the process by which a message acquires perceived legitimacy as it transitions through various messengers and formats [3]. While the core claim remains stable, its presentation shifts to match the credibility of each new carrier [3]. The EEAS FIMI framework identifies the central issue as manipulative behavior and interference effects. These effects operate through timing, coordination, and selective framing rather than through any single piece of content [3]. Research on disinformation in West Africa supports a focus on repetition and reframing across different outlets and audiences. Narratives in this region often travel through a series of successive handoffs rather than starting from a single, identifiable origin point [15].

Pathway A begins with a trigger event, followed by a rapid narrative surge and a contest over the institutional frame [14]. The institutional frame represents the way regional bodies define legitimacy, constitutional order, and permissible responses [14]. The July 26, 2023, coup attempt in Niger serves as a key anchor because it immediately elevated questions of constitutional order and triggered a response from the African Union on the same day [8]. The ECOWAS statement on July 30, 2023, provides a second institutional marker in the response cycle [10]. These institutional reference points are frequently quoted, contested, or reframed. Research indicates that such moments produce concentrated information activity and accelerated competition to define the event and its consequences [14].

In this pathway, laundering typically appears as a chain of handoffs [15]. Institutional signals are pulled into commentary, where their meaning is narrowed or widened to fit a preferred storyline. The reframed version is then repeated until it begins circulating as the default interpretation [15]. Research focused on West Africa shows that the same narrative is often republished in different forms for different audiences. This includes simplified slogans for mass circulation and more formal language for elite-facing discussions [15]. The response cycles of the AU and ECOWAS supply authoritative language that can be repurposed in this manner, as official statements provide short, quotable elements that travel easily across channels [8, 10].

Analysts can observe and code the sequence of these handoffs and the evolution of framing without forcing attribution [3]. It is possible to record when a narrative first appears relative to a trigger event, when it begins borrowing language from the AU or ECOWAS, and when it crosses into broader commentary channels. This can be done without asserting who initiated the narrative in the absence of technical linkages [3]. Meta's adversarial threat reporting illustrates what a platform defines as coordinated inauthentic behavior when it has sufficient evidence. This helps separate pattern recognition from documented coordination [21]. Meta's later reporting also underscores that detection is often incomplete and tactics change; therefore, the absence of enforcement signals does not disprove coordination [23].

Pathway B starts with a branded, public-facing identity that seeds narratives, followed by local amplification that creates the appearance of domestic validation [2]. The joint technical report by VIGINUM, the UK Foreign, Commonwealth and Development Office, and the EEAS identifies African Initiative as a documented model for this mechanism [1]. The EEAS describes African Initiative as transitioning from public diplomacy to covert influence operations. This supports a working distinction between public presentation and the operational behaviors that reinforce

distribution [2]. Branding is critical for laundering because it provides a stable source label that can be cited by others, which implies authority, professionalism, or insider access [2].

This pathway becomes operationally significant when the messaging of a branded node is echoed by local voices or local-appearing accounts. This repetition then circulates as evidence of organic agreement [1]. The technical report on African Initiative provides the documentary basis for treating the model as an influence architecture rather than just a publishing outlet [1]. The EEAS framing highlights how outward-facing legitimacy cues can coexist with covert influence activity. This increases the risk that coordinated diffusion is misread as spontaneous local consensus [2].

Analysts can observe and code the relationship between branding markers, narrative packaging, and the timing of amplification [3]. They can document recurring identifiers tied to the branded node, note the first appearance of specific frames, and track when the same frames appear through other messengers claiming local authority [1, 3]. Claims of operational linkage remain bounded to what is supported by technical reporting [1]. Meta's reporting provides a separate evidentiary stream for on-platform coordination, where linked assets and behavior can support stronger conclusions about coordinated activity within Meta services [21]. Meta's later reporting suggests that researchers should expect adaptation and mixed tactics, which increases the value of using careful chronology and asset tracking during fast-moving events [23].

Pathway C involves constrained visibility that produces delayed verification and a longer narrative half-life [7]. A longer narrative half-life means that contested claims circulate for a greater amount of time before credible corrections reach the same audience [7]. The June 30, 2023, Security Council decision to terminate the MINUSMA mandate marked a clear shift in the international monitoring posture for Mali [7]. Lessons from the International Peace Institute regarding the MINUSMA experience support the idea that mission context and access conditions directly affect information availability and verification capacity [17]. Under these conditions, early claims can persist because the mechanisms providing rapid independent observation are weaker or slower [17].

In this pathway, laundering can occur through ordinary repetition when no rapid, trusted counterweight exists in the same channels where a claim is spreading [17]. The UN record provides the institutional inflection point, and the IPI analysis confirms that monitoring and verification conditions shift alongside mission posture and access [7, 17]. Analysts can observe and code the verification gap and the resulting patterns of persistence [3]. They can log when a claim appears, when credible verification becomes available, and whether that verification penetrates the same channels that carried the initial claim [17]. Meta's adversarial threat reporting shows how some coordinated behavior can be documented on-platform, while also implying that closed networks and offline organization may fall outside of what a platform can see or disclose [21, 23].

## 6. TIMELINE: KEY INFLECTION POINTS AND SIGNAL EVENTS

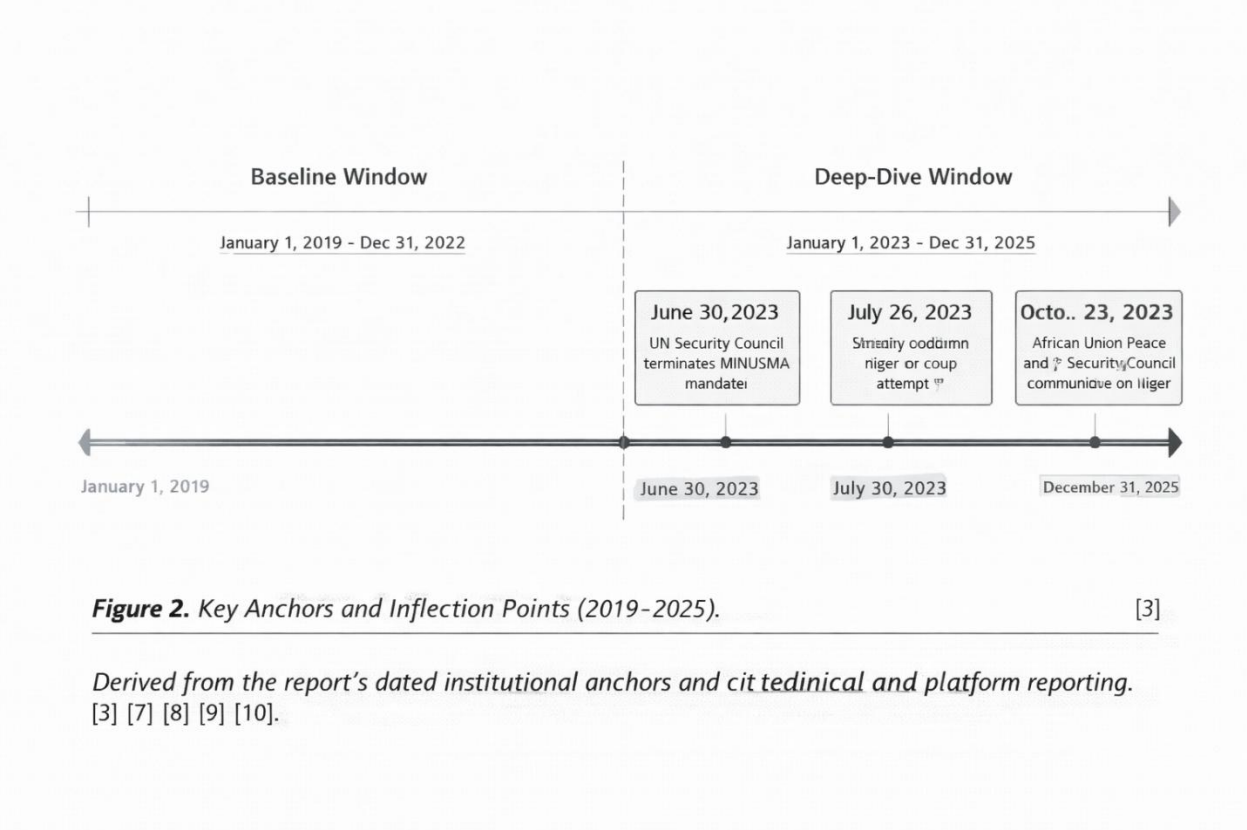



*Figure 2. Key Anchors and Inflection Points (2019-2025). Dated institutional actions and monitoring inflection points used as high-signal anchors for analysis and comparison across time windows. [3] [7] [8] [9] [10]*

From January 1, 2019, through December 31, 2022, the security and governance landscape in Mali created frequent windows where claims regarding responsibility, legitimacy, and external partnerships held immediate political weight [11]. United Nations reporting provides essential baseline context on insecurity and contested governance; this helps explain why independent observation can be inconsistent and why disputed claims often take time to verify during rapid crises [11].

During this same period, research on disinformation surges in Africa suggests that trigger events act as predictable accelerators for information activity [14]. Messaging volume and intensity typically spike following a political or security rupture before settling into repeatable frames [14]. Analysis focused on West Africa describes how narratives travel through continuous repetition and reframing across various channels, noting that similar formats often recur across different national contexts during moments of high uncertainty [15]. Findings from Burkina Faso provide concrete examples of Russian disinformation themes and their documented in-country consequences. These findings ground baseline narrative templates while avoiding the assumption that a single operator or uniform outcome exists across Mali, Burkina Faso, and Niger [18].

By late 2022, the baseline for comparison was a regional information environment characterized by recurring narrative surges around political shocks and uneven verification capabilities [14]. This baseline is used to distinguish continuity from evolution after 2023, accounting for shifts in monitoring conditions and the rise of structured influence architectures documented in official reports [1, 14].

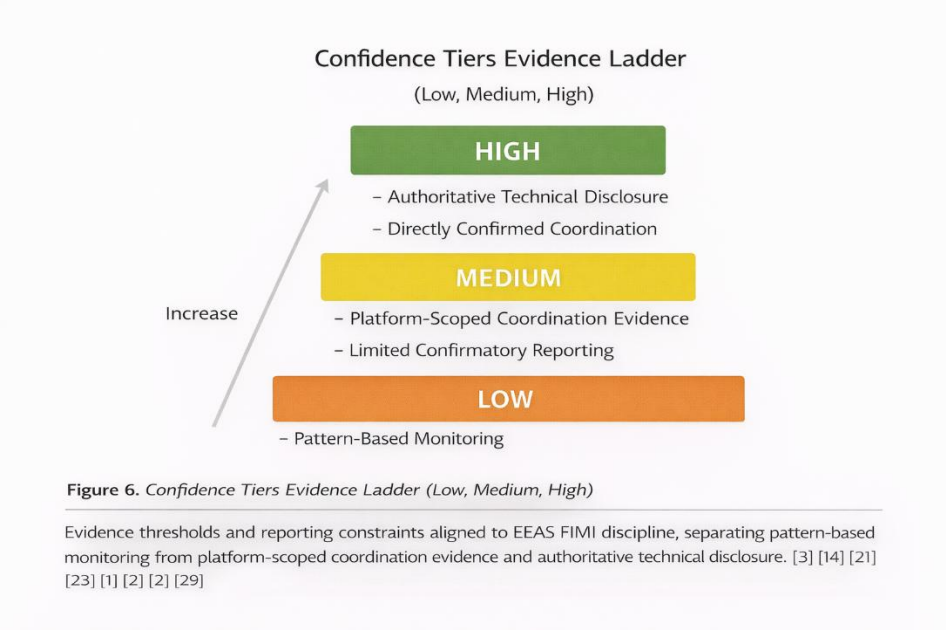
On June 30, 2023, the UN Security Council decided to terminate the MINUSMA mandate in Mali [7]. This represents a major inflection point, as it altered the external monitoring environment and reduced the independent observation typically provided by a major international mission [7]. The International Peace Institute (IPI) notes that mission posture and access conditions fundamentally shape what can be observed and communicated, making this decision directly relevant to post-2023 information conditions in Mali [17].

On July 26, 2023, the Chairperson of the African Union Commission condemned the coup attempt in Niger, anchoring the initial regional legitimacy framing cycle [8]. On July 30, 2023, ECOWAS issued its own statement on the coup, providing a second institutional reference point that shaped regional and international debates on legitimacy and permissible responses [10]. By October 23, 2023, the African Union Peace and Security Council issued a communique dedicated to Niger, indicating sustained formal attention well beyond the initial shock window [9].

These 2023 - 2025 anchors connect a monitoring shift in Mali, a high-tempo trigger sequence in Niger, and a documented influence model [1, 7, 8]. This ensures that later analysis remains grounded in dated institutional actions and documented disclosures rather than generalized assumptions [1, 15].

## 7. INDICATORS AND CONFIDENCE TIERS

Confidence tiers follow the European External Action Service (EEAS) Foreign Information Manipulation and Interference (FIMI) approach as an evidence discipline and reporting standard [3]. This method prioritizes observable behavior, coordination signals, and interference effects rather than primary factchecking of individual claims [3]. Indicators focus on observable actions and linkages - such as timing, distribution behavior, and network characteristics - while keeping coordination signals separate from the truth-value of the content [3]. This distinction is critical because accurate information can be used manipulatively, and false information can circulate without any coordination [3].




*Evidence thresholds and reporting constraints aligned to EEAS FIMI discipline, separating pattern-based monitoring from platform-scoped coordination evidence and authoritative technical disclosure. [3] [14] [21] [23] [1] [2] [29]*

LOW CONFIDENCE serves as an early-warning tier for monitoring and triage during fast-moving events in Mali, Burkina Faso, and Niger [14]. It applies when interference risks are plausible, but evidence is limited to visible content patterns, timing, and early amplification around a trigger event [14]. The anchor for this tier is the Niger coup attempt on July 26, 2023, and the subsequent AU and ECOWAS response cycle, which created a compressed window of narrative competition regarding legitimacy [8, 10]. Evidence at this tier is pattern-based and time-sensitive, including sudden spikes in volume, rapid convergence on specific frames, and the repeated reframing of institutional language [14]. In a Niger-style sequence, a low-confidence signal might include interpretations that quote, contest, or simplify AU or ECOWAS language into emotionally charged forms [8, 10].

At this level, coordination is not assumed and no specific operator is named; similar patterns can arise from organic polarization or opportunistic actors [3]. Analysts may conclude that an event has produced a high-risk environment requiring structured monitoring, but they must not claim

intent or attribution. Rights-safe discipline requires sticking to verifiable observations - such as timestamps and public posts - while explicitly marking all uncertainty [3, 14].

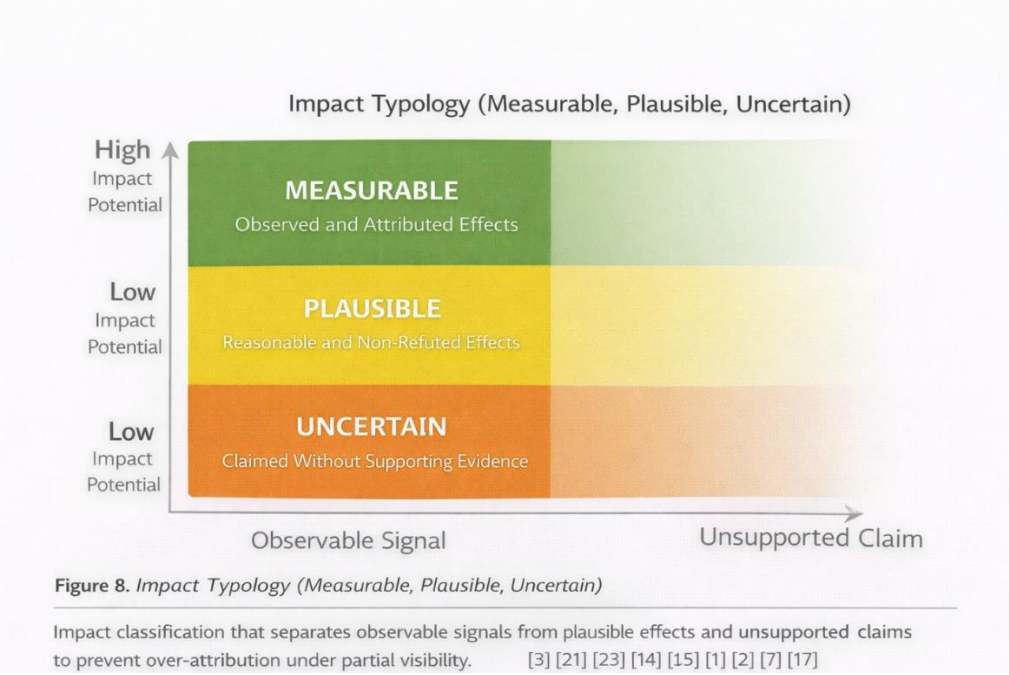
MEDIUM CONFIDENCE applies when pattern evidence is reinforced by signals consistent with platform-defined coordination or well-documented analytical findings [15, 21]. It is used when narrative activity shows structured amplification, repeated reuse of framing across accounts, or behaviors typical of coordinated inauthentic behavior [21]. This tier may still lack a conclusive link to a specific organization, as platform reporting highlights that detection is often incomplete [21, 23]. Qualifying evidence includes behavioral indicators consistent with platform-defined coordination and regional findings documenting recurring narrative templates [15, 21]. Research suggests that trigger-event surges and rapid narrative convergence are recurring patterns that can be compared across different time windows [14].

At medium confidence, analysts may conclude that observed activity is consistent with coordinated influence or structured manipulation and is plausibly part of a broader effort [3]. However, analysts must not claim that a specific state actor directed the activity without technical evidence, nor can they assert that the activity determined political outcomes [3]. Rights-safe discipline requires careful wording and the continued separation of observable indicators from unproven assumptions about funding or offline command structures. Labels such as "Russia-linked" should be used conservatively to avoid stigmatizing domestic dissent or legitimate journalism [3, 21, 23].

HIGH CONFIDENCE is reserved for cases supported by authoritative technical reporting that documents a coherent influence model or clear platform enforcement evidence [1, 21]. The anchor is the joint technical report on the African Initiative, alongside platform reporting that documents coordinated inauthentic behavior through linked assets and enforcement outcomes [1, 21]. The EEAS framing of the African Initiative as a shift from public diplomacy to covert operations supports the view that the model combines overt presentation with covert behavior [2]. High-confidence evidence includes government technical reports describing model characteristics in sufficient detail to support attribution, or platform enforcement data documenting network behaviors and asset linkages [1, 21]. This tier can incorporate convergence from multiple sources while remaining clear that platform evidence is limited to that platform and does not automatically prove offline control [21, 23].

At high confidence, analysts may conclude that a documented model or network exists and operates as described by cited sources [1, 21]. Analysts must not extend these conclusions beyond the documented scope, assert country-by-country reach without explicit supporting data, or treat high confidence as proof of persuasion effects [1, 3]. Rights-safe handling requires stating the nature of the evidence clearly, distinguishing between a documented model and its local application, and ensuring that personal data handling is minimal to protect civic actors and journalists in constrained environments [3, 29].

## 8. IMPACT ASSESSMENT




*Impact classification that separates observable signals from plausible effects and unsupported claims to prevent over-attribution under partial visibility. [3] [21] [23] [14] [15] [1] [7] [17]*

The analysis separates impact into measurable, plausible, and uncertain categories to maintain the discipline of the EEAS FIMI framework. This structure ensures that findings remain grounded in evidence and prevents the analytical error of assuming that the presence of a behavior automatically proves a specific political result [3]. In this model, the highest degree of certainty is reserved for documented coordination signals and distribution patterns. Conversely, persuasion outcomes are treated with caution due to inconsistent monitoring conditions and delayed verification processes [3].

Measurable impacts include instances where sources provide concrete data regarding activity within the information space, even if they do not quantify changes in audience belief [21]. Platform threat reporting offers measurable data through documented network behaviors and enforcement actions taken within a specific service. Although subsequent reports acknowledge that detection is never exhaustive and tactics are constantly shifting, they still provide verifiable indicators of activity [21, 23]. Another measurable category involves surge dynamics. These patterns are tracked through the timing and convergence of narratives during a crisis, allowing analysts to map the sequence of reframing without requiring a definitive attribution of the initial actor [14]. Regional research also allows for the measurement of "narrative handoffs," where stories move through repetition across various channels and outlets [15]. Finally, institutional documentation provides measurable proof that a coherent influence architecture exists. For example, technical reporting on the African Initiative identifies it as a structured model with distinct traits, while the EEAS framing confirms it as a significant operation beyond routine political messaging [1, 2].

Plausible impacts represent effects that align with documented regional patterns and operational goals, though they lack a direct causal link in the current evidence set [14]. One plausible outcome is the gradual erosion of trust in Western partners. This occurs when external actors are repeatedly portrayed as self-interested or ineffective, a process that makes contested claims feel familiar and settled to the public over time [15]. Trigger-event surges can amplify these effects by compressing the time available for factchecking and rewarding the fastest frames before a public record can stabilize [14]. It is also plausible that these operations reinforce the legitimacy of military-led regimes. During transitions, audiences often seek simplified explanations for institutional ruptures. The response cycles from the African Union and ECOWAS in Niger provide a specific vocabulary that operators can target for reframing to support a pro-regime narrative [8, 10, 14]. Additionally, sovereignty-focused messaging plausibly contests regional pressure or sanctions by repackaging complex institutional language into simplified storylines for mass consumption [8, 10, 14, 15].

Uncertain impacts include claims that cannot be responsibly supported by the available source material [3]. The EEAS FIMI framework establishes a clear boundary between observable manipulative behavior and unproven persuasion outcomes. As a result, this report does not claim to quantify direct attitude changes in Mali, Burkina Faso, or Niger resulting from Russian-linked activity [3]. The source set also does not support broad claims about total operational reach. For instance, technical reports on the African Initiative do not suggest that the model is synonymous with every pro-Russia narrative in the region or that it accounts for all narrative surges [1]. Furthermore, there is insufficient evidence to make confident claims regarding offline command structures, financing pipelines, or the full scale of coordination across different platforms beyond what is explicitly documented [1, 21]. Monitoring constraints also introduce uncertainty by limiting what can be validated in real time. In Mali, the June 2023 termination of the MINUSMA mandate serves as a primary example of how a shift in monitoring posture affects the ability to verify information [7, 17]. Finally, maintaining rights-safe boundaries is critical. Influence monitoring can create secondary risks if preliminary findings are treated as formal accusations or if the process exposes civic actors in environments where journalist safety is already compromised [3, 29].

## 9. OPTIONS AND COUNTERMEASURES BY CAPABILITY TIER

Countermeasures must remain proportional to the available evidence. They should focus on behavioral patterns and interference effects rather than policing specific content or viewpoints, staying consistent with the EEAS FIMI discipline [3]. Because access and verification in Mali, Burkina Faso, and Niger are often uneven, the most defensible strategy is to establish pre-defined evidence thresholds, execute a repeatable 24-to-72-hour trigger-event routine, and treat the ecosystem map as a living product revised after every major shock [14, 17].

MINIMUM CAPABILITY

The minimum tier is designed for institutions with limited tools and access. It focuses on disciplined situational awareness for internal use [14]. Operational triggers include coup attempts, sanctions, mission withdrawals, or major security policy shifts [7, 14].

a. Core Outputs: A trigger-event playbook that activates within 72 hours; simple evidence log that tracks chronology and messenger handoffs; and a watchlist of nodes bound strictly to observable data [3, 14].
b. Public Communication: Prioritize rapid factual orientation. Publish primary documents and official decisions in accessible formats. Clearly flag uncertainty where verification is incomplete and avoid line-by-line engagement with viral content to prevent increasing its reach [3].
c. Red Lines: No domestic actor should be labeled as foreign-linked without high-confidence evidence. Monitoring output must be treated as situational awareness products rather than accusations. Speculative network maps must not be published where press freedom is fragile, as careless language can lead to intimidation [3, 29].

INTERMEDIATE CAPABILITY

This tier introduces structured coordination with platforms and coalition partners. It converts confidence into decision points that govern what information can be circulated and to whom [3].

a. Decision Logic: A short decision tree should define what stays internal (low confidence), what is shared with partners (medium confidence), and what qualifies for public attribution (high confidence) [3].
b. Platform Engagement: Maintain standing lines with platform integrity teams. During trigger events, submit behavior-focused referrals requesting context on coordination indicators like synchronized posting or the reuse of identical framing across linked accounts [21, 23].
c. Reference Materials: Use Meta's adversarial threat reporting and Google's Threat Analysis Group bulletins as benchmarks for defining coordinated inauthentic behavior and for setting realistic expectations of platform cooperation [21, 24].
d. Mapping and Red Lines: Focus on nodes and pathways rather than personalities. Log the handoff points where narratives move from niche spaces into the mainstream [14]. Ensure that platform silence is not treated as proof of absence and restrict operator naming to cases supported by technical evidence [1, 2, 21].

ADVANCED CAPABILITY

Advanced capability is for coalition partners with dedicated analytical staff able to integrate technical reporting and long-term monitoring [14]. The central product is an integrated influence picture that treats crisis windows as intense collection sprints [14].

a. Technical Review: Use a standing function to compare observed behavior against documented models like the African Initiative [1]. The EEAS framing of such models can help refine indicator sets for hybrid risks without asserting local reach beyond what is documented [2].

b. Pre-positioned Measures: Build a rapid publication and translation pipeline for official decisions to ensure institutional frames are available before they can be distorted [3]. Support rights-safe, locally led verification capacity that provides time-stamped evidence during crises [3, 29].

c. Red Lines: Platform-scoped linkage does not prove offline command. Documented models should not be generalized into universal attribution for the entire region. Public statements must remain anchored to primary documents and high-confidence evidence [1, 3, 17, 21].

## 10. IMPLEMENTATION PLAN

This plan produces a minimal, repeatable operating system that functions under extreme constraints. The guiding principle is to treat the work as the study of behavior and interference effects rather than content adjudication [3]. Because platform visibility is partial, the plan prioritizes disciplined chronology and conservative confidence grading over rapid public attribution [21, 23].

0 TO 30 DAYS: ESTABLISHING CORE MECHANICS
Focus on building a sprint routine that can operate with minimal staffing [3].

1. Method Note: Define FIMI in EEAS terms, separating coordination indicators from truth-value judgments.
2. Evidence Log: Create a template to capture time, messenger, channel, and visibility gaps [3].
3. Watchpoint List: Limit this to documented nodes like the African Initiative to track method evolution [1, 2].
4. Evidence Protocol: Establish a protocol for secure storage and data retention [3].

The trigger-event workflow must become a fixed routine delivering three products within 72 hours: a Situation and Claims Log, a Pathway Map showing narrative movement, and a Confidence-Tier Brief to guide information sharing [3, 14, 17]. Use the July 2023 Niger sequence to rehearse this institutional framing competition [14].

31 TO 90 DAYS: CADENCE AND INTEROPERABILITY
Build a predictable rhythm for platform engagement and coalition work [3]. Update the ecosystem map after every sprint and preserve visibility gaps rather than filling them with assumptions [3]. Formalize partnership models that do not shift risk onto journalists or civil society, keeping anything above low-confidence data inside closed coalition channels [29]. Partners should agree on a shared vocabulary for confidence tiers and a strict rule: domestic opposition is not treated as foreign-linked without high-confidence evidence [3].

3 TO 12 MONTHS: DURABILITY AND ADAPTATION
Ensure the system survives staff turnover and evolves alongside new tactics [3].

1. Coalition Playbook: Standardize sprint products and rules for all partners [3].
2. Model Library: Summarize documented influence architectures to stay within supported claims [1, 2].
3. Indicator Review: Test whether watchpoints remain useful as tactics evolve, using platform transparency reports as a guide [23, 24].
4. Rotation Training: Focus on rights-safe evidence handling and communicating uncertainty under constrained visibility [3, 17].

Success should be measured by process performance: delivering sprint products on time, maintaining evidence trails, and ensuring all public statements are anchored to high-confidence data [1, 3, 21].

## 11. CONCLUSION: FINDINGS, OPERATIONAL MEANING, AND CHECKLIST

This report establishes a clear distinction between the long-standing characteristics of the Central Sahel information environment and the recently documented shifts in influence tradecraft. By applying the European External Action Service framework, the analysis focuses on observable behaviors and interference effects rather than attempting to adjudicate the truth of individual messages. This method provides a defensible foundation for institutional action in environments where visibility is limited, and the risks of inaccurate attribution are high.

*Finding 1: Structural vulnerability to information surges*
The Central Sahel has proven to be structurally prone to rapid information surges following political or security shocks. Between 2019 and 2022, trigger events consistently generated immediate demands for information that were met with pre-packaged narrative templates tailored to local grievances. For operational teams, this means that major crises should be treated as predictable windows for data collection rather than isolated anomalies. Establishing a 24-to-72-hour response routine is essential to capturing how these narratives move across the region before the public record can be verified.

*Finding 2: Emergence of structured influence architectures*
Since 2023, evidence has emerged of a more structured and organized influence architecture, specifically exemplified by the African Initiative model. Technical disclosures show a shift from traditional public diplomacy toward covert operations that blend professional branding with hidden coordination. This development requires monitoring and response strategies that can identify hybrid threats where legitimate-seeming brand identities are used to mask interference behaviors.

*Finding 3: Complexity of narrative laundering pathways*
Narrative laundering functions as a pathway problem rather than a single-source issue, as messages gain legitimacy by moving through various messengers and formats. In West Africa, narratives often travel through successive handoffs where official statements are selectively reframed to suit specific storylines. Analysts must focus on chronological and behavioral indicators to track these movements. Identifying when a frame first appears and how quickly it converges across different channels provides the most actionable data for intervention.

*Finding 4: Constraints of partial observability*
The ability to verify coordination is fundamentally constrained by the partial visibility provided by digital platforms. While platform reporting identifies some inauthentic behavior, it cannot fully capture offline organization or activities within closed networks. Consequently, the absence of an enforcement signal from a platform does not prove that coordination is not occurring. Confidence grading must remain conservative and explicitly acknowledge these gaps to avoid making unsupported claims about attribution.

*Finding 5: Impact of monitoring shifts on verification*
Changes in the international monitoring posture, such as the termination of the MINUSMA mandate in Mali, significantly affect the speed of information verification. Reduced access to independent observation lengthens the half-life of contested claims, allowing them to circulate

longer without a trusted counterweight. Response plans must manage this uncertainty by protecting rights-safe practices and avoiding the conversion of access gaps into confident assertions.

Overall Significance: The most effective countermeasure is institutional discipline maintained through a repeatable sprint routine.

By preserving evidence and tracking distribution pathways, organizations can create a stable basis for partner coordination and platform engagement. This disciplined approach ensures that public communication remains anchored to verified facts and primary documents even when regional conditions degrade.

MINI-CHECKLIST

- Establish clear evidence thresholds for confidence tiers and link each level to specific rules for information sharing and public attribution.

- Implement a trigger-event routine that delivers an evidence log, pathway map, and confidence-tier brief at the 24-, 48-, and 72-hour marks.

- Prioritize the rapid publication of primary institutional documents to provide a factual anchor for public discourse during a crisis.

- Treat the ecosystem map as a living document that is updated after every major shock to record new nodes and visibility gaps.

- Submit referrals to digital platforms that are focused on verifiable coordination behaviors rather than political viewpoints.

- Adhere to rights-safe safeguards by avoiding the labeling of domestic actors as foreign-linked without high-confidence technical evidence.

## 12. ENDNOTES

[1] VIGINUM; UK Foreign, Commonwealth and Development Office; European External Action Service, “20250612_TLP-CLEAR_VIGINUM_FCDO_EEAS_Technical_Report_African_Initiative_EN.pdf,” 2025-06-12. https://www.sgdsn.gouv.fr/files/files/Publications/20250612_TLP-CLEAR_VIGINUM_FCDO_EEAS_Technical_Report_African_Initiative_EN.pdf

[2] European External Action Service (EEAS), “African initiative: from public diplomacy to covert influence operations,” 2025-07-01. https://www.eeas.europa.eu/eeas/african-initiative-public-diplomacy-covert-influence-operations_en

[3] European External Action Service (EEAS), “2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats,” 2024-01. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

[7] United Nations, Meetings Coverage and Press Releases, “Security Council terminates MINUSMA mandate,” 2023-06-30. https://press.un.org/en/2023/sc15341.doc.htm

[8] African Union, “Chairperson of the African Union Commission condemns the coup attempt in Niger,” 2023-07-26. https://au.int/en/pressreleases/20230726/chairperson-african-union-commission-condemns-coup-attempt-niger

[9] African Union Peace and Security Council, “Communique of the 1180th PSC Meeting held on 23 October 2023 dedicated to the situations in the Republic of Niger,” 2023-10-23 (as shown on page). https://www.peaceau.org/en/article/communique-of-the-1180th-psc-meeting-held-on-23-october-2023-dedicated-to-the-situations-in-the-republic-of-niger

[10] ECOWAS, “ECOWAS Statement on Coup in Niger,” 2023-07-30. https://www.thesierraleonetelegraph.com/wp-content/uploads/2023/07/ECOWAS-STATEMENT-ON-COUP-IN-NIGER-30-JULY-2023.pdf

[11] United Nations Security Council, “Situation in Mali: Report of the Secretary-General (S/2022/731),” 2022-10-03. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2022_731.pdf

[13] European Union Institute for Security Studies (EUISS), “Shifting alliances in West Africa: Measuring Russian engagement to support countermeasures,” 2025 (publication date as shown on page). https://www.iss.europa.eu/publications/briefs/shifting-alliances-west-africa-measuring-russian-engagement-support-counter

[14] Africa Center for Strategic Studies, “Mapping a Surge of Disinformation in Africa,” 2024 (publication date as shown on page). https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-in-africa/

[15] Atlantic Council, Digital Forensic Research Lab, “The disinformation landscape in West Africa and beyond,” 2023 (publication date as shown on page). https://www.atlanticcouncil.org/in-depth-research-reports/report/disinformation-west-africa/

[16] Google Cloud, “Life after death: IO campaigns linked to notorious Russian actors persist,” 2024 (publication date as shown on page). https://cloud.google.com/blog/topics/threat-intelligence/life-after-death-io-campaigns-linked-to-notorious-russian-actors-persist

[17] International Peace Institute, “Emerging Lessons from MINUSMA’s Experience in Mali,” 2024-07. https://www.ipinst.org/wp-content/uploads/2024/07/IPI-E-RPT-Emerging-Lessons-from-MINUSMAweb.pdf

[18] Wilson Center, “The Consequences of Russian Disinformation: Examples in Burkina Faso,” 2025 (publication date as shown on page). https://www.wilsoncenter.org/blog-post/consequences-russian-disinformation-examples-burkina-faso

[21] Meta, “Meta Quarterly Adversarial Threat Report Q1 2023,” 2023-06. https://about.fb.com/wp-content/uploads/2023/06/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf

[23] Meta, “Semiannual Adversarial Threat Report Q2-Q3 2025,” 2025-12 (publication date as shown on page). https://transparency.meta.com/sr/Q2-Q3-2025-Adversarial-threat-report/

[24] Google, Threat Analysis Group, “TAG Bulletin: Q2 2025,” 2025 (publication date as shown on page). https://blog.google/threat-analysis-group/tag-bulletin-q2-2025/

[29] Associated Press, “Mali’s junta arrests prominent journalist for criticizing Niger’s military leader, rights group says,” 2026 (publication date as shown on page). https://apnews.com/article/mali-press-journalism-arrestation-freedom-sissoko-alternance-181552e5b912e1b7fa655804bfe80c75