ISA Journal of Business, Economics and Management (ISAJBEM)

Homepage: https://isapublisher.com/isajbem/

Volume 3, Issue 3, May-Jun, 2026 ISSN: 3049-1835

Governing Outsourced Intelligence: Converting External Assistance and Commercial Intelligence into Durable Capability in Nigeria and Kenya

Kunle Olawunmi, Ph.D.

ORCID: 0009-0009-8889-2261

Department of International Relations and Diplomacy, Chrisland University, Abeokuta, Nigeria

Received: 30.05.2026 | **Accepted:** 27.06.2026 | **Published:** 29.06.2026

***Corresponding Author:** Kunle Olawunmi, Ph.D.

DOI: *10.5281/zenodo.21027703*

Abstract **Original Research Article**

African counterterrorism increasingly relies on intelligence capabilities that are neither fully domestic nor fully sovereign. Under acute threat pressure, states draw on foreign intelligence assistance, contractor operated platforms, and commercially sourced data to close capability gaps quickly. Yet the same arrangements that accelerate collection and operational tempo can also entrench strategic dependence, fragment accountability, and widen counterintelligence exposure. This article asks under what governance conditions externally assisted and commercially sourced intelligence can be converted into durable domestic capability rather than reproduced as continuing substitution. It develops a capability conversion framework that integrates scholarship on intelligence governance, outsourcing, security assistance, and hybrid security governance.

Using a structured, focused comparison of Nigeria and Kenya, and relying on tiered open sources, the article traces three mechanisms: institutional absorption, partner and vendor lock in, and exposure through fragmented audit trails and ambiguous data custody. The article argues that conversion is governance contingent. Tactical gains do not by themselves demonstrate durable capability. External and commercial inputs become institutional assets only where domestic systems retain requirements sovereignty, auditable validation routines, and custody discipline over the data, tools, and platforms that shape high consequence security decisions.

Keywords: intelligence assistance, commercially sourced intelligence, capability building, strategic dependence, counterintelligence, Nigeria, Kenya.

Copyright © 2026 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

1. Introduction

What happens when African states fight terrorism with intelligence capabilities they do not fully own, control, or govern? Contemporary counterterrorism across the continent increasingly depends on foreign intelligence assistance, contractor operated platforms, and commercially supplied data assembled to meet urgent operational demands. These arrangements can enhance collection, accelerate targeting, and improve short term

responsiveness. But they can also entrench external dependence, diffuse accountability, and increase counterintelligence vulnerability. The central question, therefore, is whether outsourced and externally assisted intelligence can be converted into durable domestic capability. This article argues that the answer turns on three governance variables: requirements sovereignty, auditability, and custody discipline.

Intelligence governance in contemporary Africa is increasingly organized through distributed security ecosystems rather than self-contained national services. In practice, counterterrorism capability is often assembled through foreign liaison relationships, donor financed assistance, contractor operated platforms, and commercially sourced data and analytic tools. This matters because the reconfiguration changes more than who supplies intelligence support. It also shapes where operational priorities are set, how evidence is validated, and whether domestic institutions can later reproduce what external actors temporarily enable.

This problem sits at the intersection of several literatures. Scholarship on intelligence cooperation shows that external partnerships can close collection gaps and improve operational reach, but may also deepen asymmetries of dependence, complicate accountability, and multiply counterintelligence risk. Work on intelligence oversight similarly demonstrates that effectiveness and legality are not separable goods. Governance arrangements determine whether secret capabilities remain politically controlled, organizationally learnable, and institutionally durable (Aldrich, 2009; Born & Leigh, 2007; Born et al., 2011; Gill, 2020; Aldrich & Richterova, 2018; Leuprecht & McNorton, 2021; Walsh, 2009).

The debate has sharpened further with the rise of commercial intelligence. Recent studies show that commercially sourced intelligence now extends well beyond imagery procurement to include data brokerage, enriched analytics, platformized decision support, and broader public-private collaboration in the production of intelligence value. These developments expand access, speed, and analytic flexibility. At the same time, they blur the boundary between state intelligence authority and market provision, making provenance, auditability, subcontracting, data custody, and legal control central rather than secondary governance issues (Berrefjord & Bjørstad, 2025; Tucker & Robson-Morrow, 2025; Van Puyvelde & Oling, 2025).

African security settings render these questions especially acute. Research on hybrid security governance and counterterrorism in Africa shows that authority is often dispersed across state agencies, external partners, local intermediaries, and private actors. Security assistance does not enter a neutral institutional environment. It is filtered through uneven bureaucratic capacity, donor priorities, fragmented chains of command, and domestic political incentives. External support may therefore generate immediate operational effects without producing durable domestic capability. Existing scholarship has shown how security assistance and external pressure are mediated by domestic political bargains and institutional constraints rather than automatically translated into state capacity (Bagayoko et al., 2016; Reno, 2018; Whitaker, 2010). What remains underexplored is the institutional process through which external and commercial intelligence inputs are converted, or fail to be converted, into lasting intelligence capability.

This article addresses that gap. Existing literatures explain why states accept external intelligence support, why they cooperate under threat pressure, and why commercial actors increasingly populate the intelligence field. They say much less about how externally supplied intelligence support becomes durable domestic capability rather than a recurring substitute for it. The issue is not simply whether external assistance or commercially sourced intelligence is useful in the abstract. The key issue is conversion: whether domestic institutions can absorb these inputs while retaining sovereign control over requirements, reconstructing analytic judgement and intelligence to action processes internally, and governing the data and platform pathways on which consequential security decisions depend.

Nigeria and Kenya provide analytically useful comparison points. Both confront sustained terrorist violence, and both maintain substantial relationships

with external security partners. Yet they differ in the visibility of domestic coordination structures, legal scaffolding, and the pathways through which dependence may emerge. Nigeria offers a sharper open source window into crisis scaled external enablement through contractor operated intelligence, surveillance, and reconnaissance activity, publicly acknowledged partner coordination around kinetic operations, and externally delivered material support. Kenya, by contrast, presents a more legible coordination structure through the National Counter Terrorism Centre, alongside a more formalized trajectory of partnership deepening and a clearer data governance substrate. The comparison is therefore not between a state with assistance and a state without it, but between two pathways through which assistance and outsourced intelligence may be translated into capability, dependence, or both.

The article makes three contributions. First, it brings external intelligence assistance and commercially sourced intelligence into a single analytic field: outsourced intelligence ecosystems. Second, it develops a capability conversion framework centered on requirements sovereignty, auditability, and custody discipline. Third, it uses a structured comparison of Nigeria and Kenya to show that operational enablement and durable capability are not synonymous. Tactical gains may coexist with thin institutional absorption when domestic validation routines are weak, audit trails are fragmented, and control over data and platforms remains external.

The sections that follow review the literature, develop the capability conversion framework, explain the comparative design, and trace the relevant mechanisms across Nigeria and Kenya.

2. Materials and Methods

This study uses a structured, focused comparison of Nigeria and Kenya. The comparative logic is to hold the core problem broadly constant, sustained terrorist pressure combined with meaningful external security cooperation, while observing variation in domestic institutional scaffolding and dependence pathways. Nigeria offers an unusually visible instance of crisis scaled external enablement through contractor operated surveillance activity, acknowledged partner coordination around kinetic action, and opaque material support flows. Kenya offers a more institutionally legible configuration, including a publicly visible coordination architecture, documented partnership deepening with the United States, and a statutory data governance substrate relevant to custody discipline.

The materials used in the study are tiered and conservative. Event facts are drawn primarily from Reuters, Associated Press, and official releases. Institutional architecture is drawn from statutes, official government portals, and publicly accessible policy documents. Scholarly sources are used to frame mechanisms, bound inference, and situate the cases within the literature on intelligence governance, outsourcing, commercial intelligence, counterterrorism, and hybrid security governance.

Within each case, the analysis traces the same governance sequence. It asks where external and commercial inputs enter the intelligence cycle, who owns requirements at those interfaces, how validation and confidence assessment are documented, how data custody is governed, and where pathways to lock in and exposure become visible. The article therefore does not claim to observe the full classified intelligence chain. It identifies high consequence handoffs at which governance either converts external assistance into institutional capability or leaves it as continuing substitution.

The design does not rely on human subjects, classified documents, proprietary vendor contracts, targeting chains, or internal after action reviews. For that reason, the article adopts a conservative inference rule. Where public evidence of requirements control, auditability, or custody governance is thin, it does not infer their absence categorically. It argues only that durable conversion cannot be demonstrated under an open source standard. This limitation is substantively important. Intelligence arrangements that cannot be reconstructed even in limited institutional terms are difficult to evaluate for legality, learning, substitution capacity, and counterintelligence resilience.

3. Conceptual Framework: Capability Conversion Under Hybrid Security Governance

This article treats outsourced intelligence first as a problem of governance, and only second as a problem of procurement. That distinction is crucial. Procurement explains how states acquire external assistance, platforms, data, or analytic services. Governance explains whether those externally supplied functions remain temporary substitutes, become routinized within domestic institutions, or generate new forms of dependence and exposure. The analytical task, therefore, is not simply to identify who supplies intelligence capability, but to explain the conditions under which externally enabled capability is converted into durable domestic capacity.

The first premise of the framework comes from the intelligence accountability literature. Secrecy does not eliminate accountability. It changes its institutional form. Scholarship in this tradition shows that intelligence services require oversight capable of scrutinising legality, mandate compliance, and resource use even where operational details remain shielded from public view. It also shows that intelligence increasingly operates through transnational networks that complicate older assumptions about bounded national control. More recent work pushes the argument further by showing that accountability is not external to performance, but part of the conditions that make intelligence politically legitimate, organizationally learnable, and durable over time (Aldrich, 2009; Born & Leigh, 2007; Born et al., 2011; Gill, 2020; Aldrich & Richterova, 2018; Leuprecht & McNorton, 2021). The implication for this article is straightforward: intelligence capability cannot be assessed by operational output alone. It must also be assessed by whether domestic institutions can explain, review, and reproduce the processes through which intelligence value is generated.

A second and third body of work sharpen this problem by tracing how intelligence functions move beyond the state. Research on outsourcing and liaison shows that private actors and foreign partners may augment state capability, but can also displace essential functions beyond ordinary public chains of supervision. The issue is not privatization in the abstract. It is the relocation of operationally consequential functions across actors governed by different legal authorities, secrecy rules, commercial incentives, and audit practices. Related work on intelligence sharing and liaison reaches a similar conclusion. External partners may close collection and access gaps, yet such relationships also generate informational asymmetries, hierarchical dependencies, and inspection problems for recipient states that cannot fully verify upstream collection or analytic production (Van Puyvelde, 2019; Walsh, 2009; Born et al., 2011).

These difficulties become even sharper in counterterrorism theatres, where urgency and operational tempo reward rapid reliance on externally supplied products. Recent scholarship on commercially sourced intelligence extends the same concern. Commercial intelligence now reaches far beyond imagery procurement to include data brokerage, enriched analytics, platformized decision support, and broader public-private collaboration in intelligence production. Once vendors begin to sit inside the intelligence cycle itself, questions of provenance, reproducibility, subcontracting, cross-border processing, retention, and onward sharing cease to be secondary procurement concerns. They become central questions of intelligence governance (Berrefjord & Bjørstad, 2025; Tucker & Robson-Morrow, 2025; Van Puyvelde & Oling, 2025).

A fourth literature is indispensable for African cases. Research on hybrid security governance shows that authority and security provision in many African settings are distributed across state institutions, external partners, local intermediaries, and private actors rather than monopolized by a single bureaucratic chain. Studies of counterterrorism compliance and security assistance likewise show that external pressure and support are refracted through domestic institutions, political bargains, and uneven administrative capacity rather than automatically translated into state capability (Bagayoko et al., 2016; Reno, 2018; Whitaker, 2010). The result is that external support may improve operational reach while leaving domestic institutional absorption thin or uneven.

The gap appears at the intersection of these literatures. Scholarship on accountability explains why secret capability requires governance. Research on outsourcing and liaison explains how intelligence functions move across organizational boundaries. Work on commercial intelligence explains how private actors increasingly shape collection and analysis. African security governance scholarship explains why external support is mediated by domestic institutional and political conditions. Yet these conversations rarely converge on a single question: under what conditions do external assistance and commercially sourced intelligence become durable domestic capability rather than recurring substitutes for it? That is the question this article addresses.

For that purpose, the article defines an outsourced intelligence ecosystem as an arrangement in which high consequence intelligence functions are delivered through some combination of external partner support, contractor enabled platforms, and commercially sourced data, tools, or analytic services integrated into domestic decision making. The defining feature is not simply the presence of a foreign partner or vendor. It is that critical intelligence handoffs occur across organizational, contractual, jurisdictional, or legal boundaries in ways that shape sovereign control, reviewability, and exposure.

Durable domestic intelligence capability is defined here narrowly as the capacity of national institutions to set and revise requirements, validate and where necessary reproduce intelligence judgements and operationally relevant products, and retain governance over the principal data flows and enabling platforms used in high consequence security decisions. This definition deliberately separates durable capability from operational tempo. A state may conduct more frequent or even more effective operations after receiving external or commercial support and still remain dependent if it cannot independently task, validate, or govern the capability on which those operations rely.

The framework turns on three conversion variables. **Requirements sovereignty** refers to domestic control over what is collected, for what decision purpose, and with what priority tradeoffs. **Auditability** refers to the domestic capacity to reconstruct how analytic judgements and intelligence to action decisions were formed, including the corroboration standards and confidence thresholds applied. **Custody discipline** refers to governance over where data resides, who can access it, under what authority, for how long, and according to which onward sharing rules. This third variable is especially important where commercial datasets and cloud based platforms are involved, because the location, enrichment, retention, and onward transfer of data may otherwise be governed more by contract than by public law.

Commercially sourced intelligence is treated here functionally rather than nominally. At one end are relatively discrete products such as commercial imagery and tracking feeds, which can often be integrated with clearer provenance. In the middle are enriched datasets and analytic services that combine multiple sources and generate probabilistic outputs such as identity resolution, movement patterning, or risk scoring. At the upper end are platformised services that integrate collection, analytics, and alerting workflows and may embed vendor personnel or proprietary decision routines within the user's operational process. Governance risk rises across this spectrum because provenance becomes harder to inspect, reproducibility becomes harder to establish, and vendor leverage over continuity and switching costs increases.

From these conditions flow three mechanisms. **Institutional absorption** occurs when domestic institutions develop repeatable routines through which they own requirements, validate outputs, and reproduce key products without continuous external substitution. **Partner or vendor lock in** occurs when switching costs rise through proprietary systems, training dependence, interoperability pathways, opaque support conditions, or contractor control over indispensable enablers. **Exposure and accountability erosion** occur when multiple interfaces across liaison, contractor, and commercial pathways fragment audit trails, blur data custody, and widen counterintelligence surfaces. Figure 1 should therefore be read as a mechanism map rather than a decorative schematic: outsourced intelligence

becomes durable capability only when governance controls enable institutional absorption faster than lock in and exposure accumulate.

These mechanisms generate five propositions that guide the comparative analysis of Nigeria and Kenya.

- **Proposition 1. Governance, not assistance alone, determines conversion.** External assistance and commercially sourced intelligence are converted into durable domestic capability only where domestic institutions retain sufficient governance control over requirements, validation, and data custody.
- **Proposition 2. Operational enablement without internal validation produces fragile capability.** Where external support increases collection and operational tempo without strengthening domestic routines for validating and reproducing intelligence outputs, the resulting capability remains shallow and dependent.
- **Proposition 3. Dependence can emerge through both emergency substitution and institutionalized integration.** Strategic dependence may arise not only from crisis driven contractorization or urgent external substitution, but also from slower forms of interoperability that embed partner systems, vendor platforms, or external analytic routines into domestic practice.
- **Proposition 4. Commercial intelligence increases exposure unless governed as intelligence rather than procurement.** As commercial providers move from supplying discrete inputs to shaping collection, fusion, analytics, and alerting, governance risks increase unless these functions are subjected to intelligence specific rules of auditability, provenance, and custody.
- **Proposition 5. Under open source conditions, opacity weakens claims of durable capability.** Where public evidence of requirements control, validation routines, and data custody is thin, durable domestic capability should not be inferred from operational performance alone.

Table 1. Capability conversion controls and governance risks in outsourced intelligence ecosystems.

Conversion control	Governance question	Risk when weak
Requirements sovereignty	Who sets collection priorities, decision purposes, and retasking authority?	External agenda drift and shallow domestic ownership.
Auditability	Can analytic judgements, confidence thresholds, corroboration standards, and authorization chains be reconstructed?	Opaque validation, weak learning, and thin oversight.

Conversion control	Governance question	Risk when weak
Custody discipline	Where does data reside, who can access it, for how long, and under which onward sharing rules?	Fragmented audit trails, data exposure, vendor leverage, and counterintelligence risk.
Institutional absorption	Can domestic institutions reproduce the capability without continuous substitution?	Operational tempo may rise while durable capability remains thin.

4. Results and Discussion

4.1 Nigeria: High Tempo Enablement and Thin Conversion Visibility

Nigeria's late 2025 to early 2026 counterterrorism picture provides an unusually clear open source window into how external assistance can scale quickly into an operational ecosystem while leaving the domestic conversion question harder to demonstrate. That pattern is consistent with scholarship on Nigeria's Boko Haram war, which emphasizes chronic intelligence shortfalls, weak fusion across security institutions, and the operational importance of improvised local surveillance arrangements such as the Civilian Joint Task Force (Falode & Faseke, 2023; Agbiboa, 2018). Reuters (2025a) reported that the United States conducted intelligence gathering flights over large parts of Nigeria beginning in late November 2025, using contractor operated aircraft associated with Tenax Aerospace and operating largely from Accra, Ghana.

A second observable interface is the intelligence to action coordination layer. U.S. Africa Command (2025) stated that it conducted airstrikes against Islamic State targets in Nigeria's Sokoto State on 25 December 2025, and described the operation as coordinated with Nigerian authorities. Reuters (2025b) also reported on U.S. strikes against Islamic State militants in northwestern Nigeria around this period, reinforcing that partner enabled intelligence can translate into kinetic effects.

A third interface is resourcing under partnership conditions. Reuters (2026) reported that the United States delivered critical military supplies to Nigeria in Abuja in January 2026 while noting that AFRICOM did not specify the equipment delivered.

4.1.1 Nigeria's outsourced ecosystem map

Based on Tier 1 reporting and official disclosures, Nigeria's outsourced intelligence ecosystem in this period can be represented as three salient nodes linked by high consequence handoffs: partner enabled collection through contractor operated ISR flights, partner enabled action through an acknowledged strike coordinated with Nigerian authorities, and partner enabled resourcing through delivered supplies whose specific content was not detailed publicly (Reuters, 2025a; U.S. Africa Command, 2025; Reuters, 2026). The analytic value of mapping these nodes is diagnostic. Each node and handoff marks a governance junction where the state either enforces or cedes the conversion controls that determine whether assistance becomes durable capability: requirements sovereignty, auditability, and custody discipline.

Table 2. Nigeria's outsourced intelligence ecosystem map: nodes, handoffs, and conversion controls.

Ecosystem node	High consequence handoff	Conversion questions
Partner enabled collection	Contractor operated ISR flights feeding domestic or partner decision channels.	Who sets tasking priorities? Where does collected data reside? Are processing steps visible to domestic authorities?
Partner enabled action	Coordinated kinetic strike linked to intelligence and targeting validation.	Who validates targets and thresholds? Are confidence judgements recorded? Can decisions be reconstructed for lawful oversight?
Partner enabled resourcing	Critical supplies delivered under security partnership, with content not specified publicly.	Does support build substitution capacity? Are enablers proprietary, contractor dependent, or opaque? Do audit trails show capability building or continuing substitution?

4.1.2 Requirements sovereignty in Nigeria's enablement chain

Nigeria's conversion opportunity begins with requirements sovereignty. In an ecosystem where high value collection is contractor operated and embedded in partner pipelines, requirements sovereignty is vulnerable to agenda drift. Under a conservative open source standard, the public record establishes the existence and tempo of the external collection channel, but it does not demonstrate how Nigeria's domestic requirements are articulated and enforced at the interface where partner collection is tasked and products are integrated. This is consistent with the argument that Nigeria's counter-Boko Haram campaign has repeatedly struggled to convert intelligence inputs into anticipatory advantage because collection, analysis, and dissemination remained unevenly integrated across the security apparatus (Falode & Faseke, 2023).

4.1.3 Auditability and validation under partner coordinated action

The presence of partner coordinated kinetic action raises the stakes for auditability. When intelligence coordination translates into strikes, the chain from collection to validation to authorization becomes a capability issue. AFRICOM's public confirmation demonstrates operational integration, but the open record does not reveal the internal confidence and corroboration standards that preceded action (U.S. Africa Command, 2025). This is precisely why auditability must be treated as an internal institutional requirement. It supports learning, enables lawful oversight, and strengthens

counterintelligence detection through reconstructable decision chains.

4.1.4 Custody discipline, commercial adjacency, and counterintelligence exposure

Contractor operated ISR flights entail access surfaces across mission planning, data links, processing, and dissemination channels (Reuters, 2025a). Partner coordinated action implies liaison surfaces, shared situational awareness, deconfliction processes, and targeting coordination (U.S. Africa Command, 2025). Custody discipline constrains interface risk by clarifying where data resides, who can access it, and how onward sharing is governed. Nigeria's Data Protection Act 2023 provides a national custody governance baseline for personal data, increasingly relevant as commercially derived data enters security workflows (Federal Republic of Nigeria, 2023). The wider Nigerian literature also underlines that locally embedded surveillance can improve identification and warning while complicating evidentiary validation, chain of custody control, and accountability when state and non-state intelligence roles blur (Agbiboa, 2018).

4.1.5 Lock in, crisis contractorization, and opaque support flows

Reuters (2025a) described contractor operated ISR flights that were near daily, implying that the external platform was central to operational tempo. Reuters (2026) also noted that AFRICOM did not specify what equipment was delivered as critical supplies in January 2026. The governance question is whether such assistance generates transfer, training, domestic sustainment, and substitution capacity, or whether it becomes a recurrent external replacement for functions that national institutions cannot reproduce alone.

4.1.6 Nigeria's conversion opportunities

Nigeria's opportunity is not to reject external assistance. It is to govern assistance so that short term operational gains convert into durable domestic capacity. Three conversion moves are implementable even under secrecy and resource constraints: codify requirements sovereignty through a formal domestic requirements process with retasking authority; enforce auditable validation through confidence statements, corroboration thresholds, and authorization chains for intelligence to action decisions; and discipline custody at the interface through clear rules on storage, access, retention, and onward sharing for partner, contractor, and commercially derived data. Put differently, the challenge is to move from externally or informally enabled access to intelligence toward routines that domestic institutions can direct, interrogate, and reproduce for themselves (Falode & Faseke, 2023; Agbiboa, 2018).

4.2 Kenya: Institutional Scaffolding for Absorption and Partnership Deepening Risks

Kenya faces persistent threat pressure from al Shabaab and related networks, with recurrent cross border violence and attacks on security personnel and civilians. Associated Press (2025) reported an attack in March 2025 in which Somali militants killed Kenyan police reservists and ransacked a border camp. Kenya also occupies a visible position in U.S. security diplomacy. Reuters (2024a) reported expectations that the United States would designate Kenya as a Major Non-NATO Ally, while Biden (2024a, 2024b) subsequently issued formal documents on intent and designation. Reuters (2024b) also documented the wider set of U.S.-Kenya deals and investments announced during President William Ruto's state visit to Washington.

Kenya's domestic absorption scaffolding is unusually legible. Kenya's Head of Public Service describes the National Counter Terrorism Centre as a multi-agency instrument created in 2004 and established in law by the Security Laws (Amendment) Act 2014, oriented toward coordination in counterterrorism (Government of Kenya, n.d.). Kenya's statutory framework also specifies the NCTC's establishment and responsibilities (Republic of Kenya, 2012, as amended). This visibility aligns with a substantial literature showing that Kenyan counterterrorism has become increasingly institutionalized through legal

reform, interagency coordination, and close partnership with Western security actors, even as those same processes have generated concerns about over-securitization, coercive policing, and externally shaped priorities (Mogire & Agade, 2011; Prestholdt, 2011; Kamau, 2021).

4.2.1 Custody discipline and Kenya's data governance substrate

Kenya's Data Protection Act 2019 establishes the Office of the Data Protection Commissioner and regulates personal data processing (Republic of Kenya, 2019). The Data Protection (General) Regulations provide additional detail relevant to breach related obligations and cross border transfers (Republic of Kenya, 2021). Recent legal scholarship on data privacy in Kenya and Nigeria suggests that the significance of such statutes now extends beyond formal rights protection to the practical governance of digital security systems, cross border data movement, and regulatory enforcement capacity (Juma & Faturoti, 2025).

4.2.2 Lock in risks under institutionalized partnership deepening

Kenya's Major Non-NATO Ally designation pathway illustrates how lock in can be slow moving through continuity and interoperability expectations (Biden, 2024b). That slower pathway is consistent with work on Kenya's counterterrorism trajectory, which shows that long term partnership with the United States has brought resources and status but has also embedded asymmetries in agenda setting and security practice (Prestholdt, 2011; Fisher, 2013).

4.3 Comparative Findings: Capability Multipliers and Dependence Traps

The cross-case comparison supports the article's core claim that outsourced inputs become durable capability only under governance conditions that force institutional absorption. Both Nigeria and Kenya operate under serious terrorist pressure and both engage materially with external partners. Yet the public record does not support the same inference about conversion in each case. What differs is not merely the amount of external support, but the visibility and plausibility of domestic routines for controlling requirements, validating outputs, and governing data and platform custody.

Nigeria illustrates a high tempo enablement pathway in which externally operated or externally coordinated intelligence functions become operationally consequential faster than domestic conversion routines can be demonstrated. The public record clearly establishes collection support, coordination around action, and material resourcing, but it is much thinner on whether domestic institutions can retask collection, independently validate high value products, and reproduce key intelligence functions without continuing external substitution.

Kenya, by contrast, presents more visible absorption scaffolding through the NCTC and a clearer legal administrative environment for coordination and data governance. That does not prove successful conversion. It does, however, make institutional absorption more plausible as an empirical pathway.

The cases also differentiate two forms of dependence. Nigeria more closely approximates fast lock in under crisis contractorization and externally controlled enabling platforms. Dependence emerges because operational tempo becomes tied to capabilities that appear difficult to substitute quickly and whose detailed support conditions remain opaque in the public record. Kenya illustrates a slower pathway in which lock in may emerge through sustained interoperability, strategic partnership deepening, and normalized external reliance. This form of dependence is politically quieter but strategically significant, because continuity can gradually narrow domestic alternatives even in the presence of stronger institutional scaffolding. The contrast also tracks the regional literature: Kenya's risks are more compatible with the gradual interoperability and donor alignment dynamics described by Prestholdt (2011) and Fisher (2013), whereas Nigeria's pattern more closely resembles externally accelerated but

internally thin intelligence adaptation under acute insurgent pressure (Falode & Faseke, 2023).

Exposure and accountability risks rise in both cases once foreign assistance, contractors, and commercial inputs are treated as a single ecosystem rather than separate domains. The more intelligence value depends on interorganizational handoffs, the more easily audit trails fragment and the harder it becomes to reconstruct who handled what data, under which authority, and with what confidence standards. The ODNI policy framework on commercially available information is instructive here, not because it can be transplanted directly into African settings, but because it codifies a principle directly relevant to this article: commercially obtained information requires specific governance standards because intelligence value, privacy, legality, and data custody risk are inseparable in practice (Office of the Director of National Intelligence, 2024).

5. Policy Implications: A Capability Conversion Playbook

The policy implication is not that African states should reject external intelligence assistance or commercially sourced intelligence. In many counterterrorism environments they cannot. The implication is that assistance should be governed against an explicit conversion test. Five controls follow from the analysis:

1. **Requirements sovereignty** should be formalized through domestic tasking authorities that can specify, prioritize, and retask collection.
2. **Auditable validation** should be mandatory for intelligence to action chains through recorded confidence statements, corroboration thresholds, and reconstructable authorization paths.
3. **Commercial intelligence** should be governed as intelligence rather than treated as ordinary procurement, with explicit rules on provenance, subcontracting, storage, retention, and onward sharing.
4. **Counterintelligence safeguards** should be built around the whole ecosystem, not just around domestic agencies, because liaison, contractor, and vendor interfaces all create access surfaces.
5. **Exit design** must be integrated into every major assistance or vendor line so that operational enablement is tied to substitution capacity, training transfer, and institutional learning rather than indefinite external replacement.

6. Conclusion

The Nigeria-Kenya comparison shows that outsourced intelligence is best understood as a problem of capability conversion under hybrid security governance. External assistance and commercial intelligence can expand speed, reach, and analytic depth, but these gains do not by themselves amount to durable domestic capability. Conversion occurs only where domestic institutions retain control over requirements, can reconstruct and challenge intelligence judgements, and govern the data and platforms on which high consequence security action depends. Nigeria's public record points to rapid operational enablement with comparatively thin visibility into conversion routines, making dependence and accountability risks especially acute. Kenya presents stronger institutional and legal scaffolding, but that scaffolding does not remove the longer horizon risks of interoperability driven dependence. The broader implication is clear: the central question for African intelligence governance is no longer whether states receive outside assistance, but whether they can govern the handoffs through which that assistance becomes either durable institutional capability or an enduring dependence trap.

Acknowledgments

No funding was received for this study. The author declares no competing interests. No external grants, institutional research funds, or paid assistance supported the manuscript. Any additional individuals

or institutions to be acknowledged may be inserted before submission.

References

- Aldrich, R. J. (2009). Beyond the vigilant state: Globalisation and intelligence. *Review of International Studies*, 35(4), 889-902. https://doi.org/10.1017/S0260210509990337
- Born, H., & Leigh, I. (2007). Democratic accountability of intelligence services. *DCAF Policy Paper No. 19*. Geneva Centre for the Democratic Control of Armed Forces.
- Born, H., Leigh, I., & Wills, A. (Eds.). (2011). *International intelligence cooperation and accountability*. Routledge. https://doi.org/10.4324/9780203831731
- Gill, P. (2020). Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and National Security*, 35(7), 970-989. https://doi.org/10.1080/02684527.2020.1783875
- Aldrich, R. J., & Richterova, D. (2018). Ambient accountability: Intelligence services in Europe and the decline of state secrecy. *West European Politics*, 41(4), 1003-1024. https://doi.org/10.1080/01402382.2017.1415780
- Leuprecht, C., & McNorton, H. (2021). *Intelligence as democratic statecraft: Accountability and governance of civil-intelligence relations across the Five Eyes security community*. Oxford University Press.
- Walsh, J. I. (2009). *The international politics of intelligence sharing*. Columbia University Press. https://doi.org/10.7312/wals15410
- Berrefjord, V. R., & Bjørstad, T. E. (2025). Commercially sourced intelligence: Friend or foe? *Intelligence and National Security*, 40(3), 391-411. https://doi.org/10.1080/02684527.2024.2437955
- Tucker, K., & Robson-Morrow, M. (2025). Intelligence outsourcing for non-traditional clients: The rise of private sector intelligence providers. *Intelligence and National Security*, 40(3), 412-431. https://doi.org/10.1080/02684527.2024.2437958
- Van Puyvelde, D., & Oling, P. (2025). Public-private collaboration and the digital transformation of intelligence. *Intelligence and National Security*, 40(6), 1015-1030. https://doi.org/10.1080/02684527.2025.2565950
- Bagayoko, N., Hutchful, E., & Luckham, R. (2016). Hybrid security governance in Africa: Rethinking the foundations of security, justice and legitimate public authority. *Conflict, Security & Development*, 16(1), 1-32. https://doi.org/10.1080/14678802.2016.1136137
- Reno, W. (2018). The politics of security assistance in the Horn of Africa. *Defence Studies*, 18(4), 389-409. https://doi.org/10.1080/14702436.2018.1463819
- Whitaker, B. E. (2010). Compliance among weak states: Africa and the counter-terrorism regime. *Review of International Studies*, 36(3), 639-662. https://doi.org/10.1017/S0260210510000641
- Van Puyvelde, D. (2019). *Outsourcing US intelligence: Contractors and government accountability*. Edinburgh University Press.
- Falode, A. J., & Faseke, B. O. (2023). The art of the impossible: Intelligence and Nigeria's Boko Haram War, 2010-2021. *International Journal of Intelligence and CounterIntelligence*, 36(4), 1319-1336. https://doi.org/10.1080/08850607.2022.2121948

- Agbiboa, D. E. (2018). Eyes on the street: Civilian Joint Task Force and the surveillance of Boko Haram in northeastern Nigeria. *Intelligence and National Security*, 33(7), 1022-1039. https://doi.org/10.1080/02684527.2018.1475892
- Reuters. (2025a, December 22). U.S. conducting surveillance flights over Nigeria after Trump intervention threat. https://www.reuters.com/world/africa/us-conducting-surveillance-flights-over-nigeria-after-trump-intervention-threat-2025-12-22/
- U.S. Africa Command. (2025, December 25). U.S. Africa Command conducts strike against ISIS in Nigeria

  Press release

  . https://www.africom.mil/pressrelease/36158/us-africa-command-conducts-strike-against-isis-in-nigeria
- Reuters. (2025b, December 26). US says it struck Islamic State militants in northwest Nigeria. https://www.reuters.com/world/africa/us-launches-strikes-against-islamic-state-militants-northwest-nigeria-trump-says-2025-12-25/
- Reuters. (2026, January 13). US bolsters Nigeria's military with supplies in security partnership. https://www.reuters.com/world/africa/us-bolsters-nigerias-military-with-supplies-security-partnership-2026-01-13/
- Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf
- Associated Press. (2025, March 23). Somali militants kill 6 Kenyan police reservists and ransack a border camp. https://apnews.com/article/kenya-attack-garissa-somalia-alshabab-0fc536e9d951caec7db9263d0f9ffe57
- Reuters. (2024a, May 22). U.S. expected to designate Kenya as major non-NATO ally, source says. https://www.reuters.com/world/us-expected-designate-kenya-major-non-nato-ally-source-says-2024-05-22/
- Biden, J. R., Jr. (2024a, May 23). Message to the Congress on the intent to designate Kenya as a major non-NATO ally. *The American Presidency Project*. https://www.presidency.ucsb.edu/documents/message-the-congress-the-intent-designate-kenya-major-non-nato-ally
- Biden, J. R., Jr. (2024b, June 24). Presidential determination on the designation of Kenya as a major non-NATO ally. *The American Presidency Project*. https://www.presidency.ucsb.edu/documents/presidential-determination-the-designation-kenya-major-non-nato-ally
- Reuters. (2024b, May 23). U.S., Kenya deals and investments announced as Ruto meets Biden. https://www.reuters.com/world/us-kenya-deals-investments-announced-ruto-meets-biden-2024-05-23/
- Government of Kenya, Office of the Head of Public Service. (n.d.). National Counter Terrorism Centre (NCTC). Retrieved January 22, 2026, from https://www.headofpublicservice.go.ke/national-counter-terrorism-centre-nctc/
- Republic of Kenya. (2012, as amended). Prevention of Terrorism Act, Cap. 59B. *Kenya Law*. Retrieved January 22, 2026, from https://new.kenyalaw.org/akn/ke/act/2012/30/eng%402025-06-20
- Mogire, E., & Agade, K. M. (2011). Counter-terrorism in Kenya. *Journal of Contemporary African Studies*, 29(4), 473-491. https://doi.org/10.1080/02589001.2011.600849

- Prestholdt, J. (2011). Kenya, the United States, and counterterrorism. *Africa Today*, 57(4), 3-27. https://doi.org/10.2979/africatoday.57.4.3
- Kamau, J. W. (2021). Is counter-terrorism counterproductive? A case study of Kenya's response to terrorism, 1998-2020. *South African Journal of International Affairs*, 28(2), 203-231. https://doi.org/10.1080/10220461.2021.1924252
- Republic of Kenya. (2019). Data Protection Act, Cap. 411C. *Kenya Law*. Retrieved January 22, 2026, from https://new.kenyalaw.org/akn/ke/act/2019/24/eng%402019-11-15
- Republic of Kenya. (2021). Data Protection (General) Regulations, Legal Notice No. 263 of 2021. *Kenya Law*. Retrieved January 22, 2026, from https://new.kenyalaw.org/akn/ke/act/ln/2021/263/eng%402022-12-31/source.pdf
- Juma, I., & Faturoti, B. (2025). Enforcing data privacy in Kenya and Nigeria: Towards an African approach to regulatory practice. *International Review of Law, Computers & Technology*, 1-25. https://doi.org/10.1080/13600869.2025.2506918
- Fisher, J. (2013). "Some more reliable than others": Image management, donor perceptions and the Global War on Terror in East African diplomacy. *The Journal of Modern African Studies*, 51(1), 1-31. https://doi.org/10.1017/S0022278X12000535
- Office of the Director of National Intelligence. (2024). Intelligence Community policy framework for commercially available information. https://www.dni.gov/files/ODNI/documents/CAI/IC-Policy-Framework-Commercially-Available-Information.pdf