Cascades, Journal of the Department of French and International Studies
Cascades : Revue Internationale Du Departement De Français Et D'etudes Internationales
ISSN (Print): 2992-2992; E-ISSN: 2992-3670
www.cascadesjournals.com; **Email:** cascadejournals@gmail.com
VOLUME 4; NO. 1; APRIL, 2026 ; PAGE 44-51

French Cyber and Intelligence Networks: Tackling Transnational Crime beyond Anglophone Barriers

Tolbert Terdue Abutu
Department of French, Faculty of Arts,
Federal University of Lafia
Email: tolbertabutu@gmail.com
Orcid: https://orcid.org/0009-0004-3318-3090
Mobile phone :07036125310, 09029285468

&

Harrison Gowon UGBIJEH
Department of French,
School of Secondary Education (Language programme)
Federal University of Education,
Kontagora, Niger State,Nigeria.
Email : harrugbi@gmail.com
Orcid: https://orcid.org/0009-0002-8880-2958
Mobile phone: 09035848054

Abstract
The growing entanglement of cyberspace and transnational crime in West and Central Africa underscores the urgent need for robust, multilingual intelligence cooperation. While English remains the dominant language of global cyber operations, the predominance of French across Francophone Africa presents both a barrier and an opportunity for Nigeria and other Anglophone states engaged in countering cybercrime, terrorism financing, trafficking, and illicit digital economies. This article examines the role of French as a strategic linguistic tool in cyber and intelligence networks, emphasizing its potential to bridge operational gaps, enhance real-time information sharing, and strengthen interoperability among diverse national agencies.
Drawing on case studies of regional security initiatives, intelligence-sharing platforms, and counter-cybercrime operations, the study argues that language is not merely a medium of communication but a critical component of cyber-sovereignty and transnational resilience. By situating French within broader debates on cyber-diplomacy, intelligence cooperation, and linguistic geopolitics, the article proposes a framework for integrating language capacity-building into cyber defence strategies.
The analysis concludes that overcoming Anglophone–Francophone linguistic divides is pivotal for dismantling criminal networks that exploit digital borders, and that cultivating bilingual intelligence infrastructures can serve as both a tactical and diplomatic resource in shaping Africa's collective security future.

Keywords: French; Cybersecurity; Intelligence networks; Transnational crime; Anglophone–Francophone divide; Linguistic interoperability.

Introduction

The rapid expansion of digital technologies across Africa has produced both transformative opportunities and profound vulnerabilities. Cyber-enabled transnational crimes, including terrorist financing, cyber fraud, human trafficking, arms trafficking, and illicit online economies, have emerged as defining threats to regional stability

(Interpol, 2021; UNODC, 2022). In West and Central Africa, non-state actors and criminal syndicates increasingly exploit cyberspace to coordinate operations, launder resources, and circumvent border controls (Adeniran & Okeke-Uzodike, 2021). These developments compel African states to extend security frameworks beyond territorial borders into digital spaces where intelligence coordination determines operational success (Taddeo & Floridi, 2018).

Despite the transnational and inherently multilingual nature of cybercrime, intelligence cooperation in Africa remains structurally uneven. English continues to dominate cybersecurity discourse and technical infrastructures (Nocetti, 2015), reinforcing Anglophone-centered operational systems. However, this dominance obscures a critical geopolitical reality: a substantial portion of Africa's security environment is Francophone. Across the Sahel and Central Africa, French remains the dominant working language of governance, military coordination, and intelligence exchange (Charbonneau, 2017).

This linguistic bifurcation produces a structural barrier to effective collaboration. Limited interoperability between Anglophone and Francophone systems slows intelligence exchange, creates asymmetries in operational capacity, and provides exploitable gaps for criminal organizations (Aning & Dzinesa, 2018).
Against this backdrop, this study asks:

1. How does French function as a strategic asset in cyber and intelligence operations?
2. What are the implications of linguistic fragmentation for Africa's cyber defence systems?

This inquiry reframes language not as a communicative accessory but as a determinant of cyber resilience and strategic coordination (Berkman, 2019).

Scope and Limitations

The study is geographically focused on West and Central Africa, where Anglophone–Francophone divisions are most pronounced. While findings may apply to Lusophone and Arabophone contexts, the emphasis on French ensures analytical precision. The study relies on secondary data due to the classified nature of intelligence operations (Yin, 2018). Nevertheless, triangulation across institutional reports and academic literature enhances reliability (Bowen, 2009).

Theoretical Framing: Language and Security Studies

This study is grounded in an interdisciplinary framework that integrates linguistic security studies, cyber-diplomacy, sociolinguistics, and transnational crime theory in order to interrogate the strategic role of language—particularly French—within cyber and intelligence networks in West and Central Africa. Rather than treating language as a neutral communicative tool, this framework positions it as a constitutive element of security architecture, shaping access, coordination, and operational effectiveness.

Language as Security Infrastructure

Language is not neutral; it constitutes a core component of security systems and intelligence infrastructures. Communication structures directly influence the circulation of intelligence, the establishment of institutional trust, and the efficiency of operational coordination among security actors (Bourdieu, 1991; Pennycook, 2017). Within this perspective, language functions as a form of "symbolic capital" that determines who can access, interpret, and act upon security information.

In African security environments, this linguistic dimension becomes particularly salient. Linguistic competence is not simply an auxiliary skill but a prerequisite for participation in joint intelligence operations, cross-border investigations, and multinational task forces (Mazrui & Mazrui, 1998). The absence of shared linguistic frameworks—particularly between Anglophone and Francophone states—therefore produces structural asymmetries in intelligence access and operational participation. In this sense, French operates as a functional infrastructure within Francophone security systems, while its absence within Anglophone systems creates operational discontinuities.

Cyber-Diplomacy and Multilingual Governance

Cyber-diplomacy has emerged as a central pillar of contemporary global security governance, where states negotiate cyber norms, share intelligence, and coordinate responses to digital threats (Taddeo & Floridi, 2018). Within this evolving landscape, multilingual governance is increasingly recognized as a critical enabler of operational coherence and diplomatic trust.

Comparative institutional examples such as NATO and the European Union demonstrate how multilingual frameworks are embedded into cybersecurity governance structures to ensure inclusivity and functional interoperability (Eriksson & Giacomello, 2006). These institutions invest heavily in translation infrastructures, multilingual documentation systems, and bilingual operational protocols to maintain cohesion across linguistic diversity.

In contrast, African cyber governance systems remain largely Anglophone-dominant in practice, despite the continent's linguistic plurality. This dominance limits the effective integration of Francophone actors into shared cyber intelligence infrastructures, thereby reducing the efficiency of regional coordination mechanisms. The absence of institutionalized multilingual cyber governance thus represents a structural constraint on Africa's collective cybersecurity capacity.

Sociolinguistic Power and Postcolonial Asymmetry

Postcolonial sociolinguistic theory provides critical insight into how language hierarchies reproduce structural inequalities within global governance systems (Phillipson, 1992; Bamgbose, 2000). Language is not only a medium of communication but also a site of power, exclusion, and epistemic control.

In the African context, the Anglophone–Francophone divide reflects both colonial legacies and contemporary geopolitical alignments. English dominates global cyber governance, technical standards, and digital security discourse, while French remains the operational language of many national security institutions in West and Central Africa (Banégas, 2020). This dual linguistic order produces asymmetrical access to intelligence networks and fragmented participation in transnational security architectures.

As a result, Francophone states may operate within tightly integrated internal systems, while Anglophone actors risk partial exclusion from these networks due to linguistic incompatibility. Conversely, Francophone systems may face similar limitations when interfacing with global English-dominated cyber infrastructures. This asymmetry reinforces uneven power relations and contributes to fragmented intelligence ecosystems across the continent.

Transnational Crime and Communication Gaps

Transnational crime theory emphasizes the adaptive nature of criminal networks, which exploit jurisdictional fragmentation, institutional weaknesses, and governance gaps to sustain illicit operations (Shelley, 2014). In the digital era, these dynamics are intensified by cybercrime, which enables anonymity, speed, and borderless coordination across multiple jurisdictions (Broadhurst et al., 2014).

Within this context, linguistic fragmentation emerges as a critical enabler of criminal activity. Communication barriers between Anglophone and Francophone enforcement agencies create delays in intelligence fusion, reduce investigative coherence, and weaken real-time response capabilities. Criminal networks strategically exploit these gaps by routing operations through multilingual corridors where coordination is weakest.

Thus, linguistic division does not merely slow down enforcement; it actively shapes the operational geography of transnational crime. Language becomes a structural variable within the crime–security ecosystem, influencing both the visibility of criminal activity and the effectiveness of state response mechanisms.

Methodology

This study adopts a qualitative research design grounded in comparative case analysis and critical discourse analysis to examine the role of French within cyber and intelligence networks across West and Central Africa. Given the complexity of cyber-enabled transnational crime and the institutional sensitivity of intelligence operations, a qualitative approach is particularly suitable for capturing the interpretive, structural, and discursive dimensions of the phenomenon (Creswell & Poth, 2018).
The methodology is designed to move beyond surface-level description to provide an analytical understanding of how language functions as an operational resource within security infrastructures.

Research Design
The study is structured as a multi-case comparative analysis focusing on selected regional security and intelligence cooperation frameworks in West and Central Africa. The comparative approach allows for systematic examination of similarities and differences in linguistic integration across Anglophone and Francophone operational environments (George & Bennett, 2005).
This design enables the study to assess how French language capacity influences intelligence-sharing efficiency, institutional cohesion, and operational outcomes across different security coalitions and cyber defense structures.

Data Sources
The study draws on multiple categories of secondary data to ensure triangulation and analytical depth:

- **Institutional Reports:** ECOWAS, African Union (AU), INTERPOL, and United Nations Office on Drugs and Crime (UNODC) publications on cybercrime, intelligence cooperation, and regional security frameworks.
- **Security Assessments:** Reports from the Multinational Joint Task Force (MNJTF), African cybersecurity monitoring bodies, and INTERPOL's African Cyberthreat Assessment.
- **Scholarly and Policy Literature:** Peer-reviewed academic articles, books, and policy analyses addressing cybercrime, intelligence cooperation, sociolinguistics, and linguistic barriers in Africa.

These sources collectively provide both empirical and conceptual insights into the intersection of language and cybersecurity governance.

Analytical Methods
The study employs a combination of three complementary analytical techniques to ensure methodological rigor and interpretive depth:

- **Comparative Case Analysis:** This method is used to examine variations in cyber and intelligence cooperation across Anglophone and Francophone institutional contexts, allowing for identification of structural patterns and operational divergences (George & Bennett, 2005).
- **Document Analysis:** Institutional documents, policy frameworks, and operational reports are systematically examined to identify how language is addressed—or omitted—within cybersecurity and intelligence strategies (Bowen, 2009).
- **Critical Discourse Analysis (CDA):** CDA is used to interrogate how language, power, and institutional authority are constructed within policy texts and security narratives, particularly in relation to French and English as operational languages (Fairclough, 2013).

Through the integration of these methods, the study is able to connect institutional practice, policy discourse, and operational realities in order to provide a comprehensive understanding of linguistic dynamics in cyber intelligence systems.

Methodological Rationale
The choice of a qualitative, multi-method design is justified by the inherently complex and politically sensitive nature of cyber intelligence operations. Quantitative approaches alone would be insufficient to capture the nuanced role of language in shaping institutional trust, coordination efficiency, and transnational cooperation.

By combining comparative, documentary, and discourse-based methods, the study ensures a robust and context-sensitive analysis of how French functions within Africa's evolving cyber and intelligence landscape.

Analytical Framework, Findings & Discussion

- This section synthesizes evidence drawn from institutional reports, policy documents, and scholarly analyses to examine how linguistic structures—particularly the Anglophone–Francophone divide—shape operational efficiency in cyber intelligence networks across West and Central Africa. The discussion is organized around five interrelated findings that demonstrate that language is not a peripheral issue but a structural determinant of cybersecurity effectiveness.

1. Intelligence delays caused by language barriers

- One of the most immediate operational consequences of linguistic fragmentation is the delay in intelligence transmission and interpretation. Translation bottlenecks, combined with the scarcity of trained bilingual analysts, significantly slow down the circulation of cyber intelligence between Anglophone and Francophone agencies. According to INTERPOL (2021), such delays can extend up to 72 hours in cross-linguistic intelligence exchange processes. In cybercrime environments—where financial transfers, data breaches, and digital concealment occur within minutes—this time lag creates critical vulnerabilities.
- For instance, intelligence originating in English-speaking jurisdictions often requires translation before being actionable in Francophone contexts such as Niger, Chad, or Cameroon. During this interval, cybercriminal networks exploit the delay to reroute funds, erase digital traces, or migrate operations across platforms, thereby reducing traceability and enforcement effectiveness.

2. Greater cohesion in Francophone networks

- A second key finding is that Francophone security coalitions tend to exhibit higher levels of operational cohesion when French is used as the primary working language. This cohesion is largely attributed to shared linguistic structures, administrative traditions, and institutional legacies inherited from colonial governance systems (Charbonneau, 2017).
- Initiatives such as the G5 Sahel illustrate how a shared linguistic framework enhances coordination in intelligence synthesis, operational planning, and field execution. Standardized French terminology reduces semantic ambiguity in threat reporting and command structures. However, this internal cohesion becomes less effective when Francophone systems interface with Anglophone partners such as Nigeria, where linguistic divergence introduces delays, misinterpretations, and coordination inefficiencies.

3. Critical shortage of bilingual analysts

- A third major finding highlights the acute shortage of personnel capable of operating across both linguistic systems. According to the ECOWAS Commission (2020), fewer than 15% of analysts in regional joint task forces possess adequate bilingual proficiency in English and French.
- These bilingual professionals function as essential "linguistic intermediaries," translating not only language but also institutional protocols, technical cyber terminology, and operational intelligence codes. Their scarcity results in fragmented intelligence flows, duplication of analytical processes, and delayed decision-making. In cyber investigations involving malware tracking, phishing networks, or cryptocurrency laundering, even minor translation inaccuracies can compromise evidentiary integrity or misdirect enforcement actions.

4. Criminal exploitation of linguistic gaps

- A particularly significant finding is that cybercriminal networks actively exploit linguistic fragmentation as a strategic operational advantage. According to UNODC (2022), transnational criminal groups—including advance fee fraud syndicates, trafficking networks, and cyber-enabled laundering operations—routinely exploit weak communication channels between Anglophone and Francophone jurisdictions.

- For example, fraudulent financial flows originating in Anglophone countries such as Nigeria are often transferred into Francophone jurisdictions where interoperability between cyber-monitoring systems is limited. Conversely, Francophone-originated cyber communications may evade detection in Anglophone systems due to translation gaps and non-aligned analytical frameworks. This demonstrates that linguistic fragmentation is not neutral; it is structurally embedded in the operational ecology of cybercrime.

5. Weak integration of language policy in cyber strategy

- The final finding reveals a systemic policy gap: cybersecurity frameworks across West and Central Africa disproportionately emphasize technical infrastructure, legal harmonization, and digital surveillance systems while neglecting linguistic interoperability as a strategic pillar.
- Most ECOWAS and African Union cybersecurity initiatives focus on technical capacity-building and regulatory alignment (ECOWAS Commission, 2020). However, structured investment in bilingual training, translation infrastructures, and language-integrated intelligence systems remains minimal. This omission creates a persistent structural vulnerability, as technical systems cannot function optimally without linguistic alignment across operational actors.

Interpretation of Findings

- The findings demonstrate that language is not merely an accessory to communication but a structural determinant of cyber intelligence effectiveness. Intelligence-sharing delays, cohesion gaps, and the deliberate exploitation of linguistic divides by criminal networks collectively reveal that communication itself functions as an operational infrastructure rather than a neutral medium (Bourdieu, 1991; Pennycook, 2017).
- In this context, French emerges as a "strategic equalizer" that enables Anglophone states such as Nigeria to access and integrate more effectively into Francophone intelligence ecosystems. Rather than privileging one linguistic bloc over another, French operates as a bridging resource that enhances regional cyber resilience by facilitating smoother interoperability, faster intelligence circulation, and improved trust among security institutions.

Policy Implications

- The evidence suggests that without the systematic integration of French, Anglophone cyber strategies remain structurally incomplete. Language policy must therefore be reconceptualized as an extension of cyber-sovereignty, intelligence capability, and digital diplomacy rather than being confined to educational or cultural domains.
- Embedding French capacity within national and regional security frameworks would significantly reduce intelligence delays, close exploitable communication gaps, and enhance the operational coherence of multinational coalitions (Mazrui & Mazrui, 1998; Berkman, 2019). This includes institutionalizing bilingual training programs, strengthening translation infrastructures in cyber command centers, and embedding language competencies into cybersecurity recruitment and training policies.
- Ultimately, linguistic interoperability should be treated as a core component of Africa's cyber defense architecture, alongside technical infrastructure and legal frameworks.

Conclusion

This study demonstrates that French is not merely a linguistic medium but a strategic security asset within Africa's cyber and intelligence ecosystems. Beyond its communicative function, French operates as an infrastructural resource that shapes the efficiency, coherence, and reliability of intelligence-sharing across West and Central Africa. The findings consistently show that linguistic interoperability directly influences the speed of intelligence circulation, the level of operational coordination among security agencies, and the overall resilience of regional cyber defense systems.

The evidence further confirms that multilingual integration is not optional but essential for dismantling increasingly sophisticated transnational cybercrime networks. In contexts where cybercriminal actors exploit jurisdictional fragmentation and linguistic divides, the absence of structured bilingual capacity becomes a systemic vulnerability. Conversely, where linguistic bridges exist, intelligence fusion is faster, more accurate, and more actionable, thereby strengthening collective security responses.

Comparative evidence drawn from established security institutions such as NATO and the European Union reinforces this argument. These organizations demonstrate that institutionalized multilingualism enhances operational effectiveness by ensuring that linguistic diversity does not become a barrier to coordination but rather a managed asset within security architecture (Eriksson & Giacomello, 2006). In these contexts, translation systems, bilingual protocols, and multilingual command structures are embedded within operational design, thereby reducing delays and improving cohesion.

Building on these insights, this study advances the concept of linguistic interoperability as a central pillar of cyber security theory in Africa. It reframes language not as a peripheral cultural or educational concern, but as a core infrastructural component of cyber sovereignty, intelligence effectiveness, and transnational security governance. In this sense, French emerges as a critical enabling tool for regional integration, operational efficiency, and strategic resilience in Africa's evolving cyber threat landscape.

Recommendations

1. **Institutionalize French training for Anglophone cyber intelligence officers**
   Structured and continuous French-language training should be embedded within national security academies and cyber intelligence programs in Anglophone states. This will enhance operational readiness, reduce translation delays, and improve real-time collaboration in joint task forces operating across Francophone regions.
2. **Establish bilingual intelligence units within ECOWAS and AU frameworks**
   Regional security institutions should develop dedicated bilingual cyber intelligence units composed of both Anglophone and Francophone analysts. These units would function as operational bridges, ensuring seamless intelligence fusion, standardized communication protocols, and faster coordinated responses to cyber threats.
3. **Develop AI-assisted translation tools for cyber intelligence communication**
   Investment in artificial intelligence-driven translation systems tailored to cybersecurity terminology should be prioritized. Such tools would reduce reliance on human intermediaries, minimize delays in intelligence processing, and improve accuracy in translating technical cyber threat data in real time.
4. **Integrate French into Nigeria's cyber-diplomacy and security policy**
   Given Nigeria's central role in West African security architecture, French language capacity should be formally incorporated into its cyber-diplomacy strategy. This integration would enhance Nigeria's engagement with Francophone partners, strengthen regional leadership, and improve participation in joint intelligence operations.
5. **Strengthen academic–policy collaboration on linguistic cybersecurity**
   Greater collaboration between universities, research institutes, and security agencies should be encouraged to deepen understanding of the relationship between language and cybersecurity. Such partnerships can generate evidence-based policy frameworks and support the development of training curricula on linguistic interoperability in security studies.

Future Research Directions

Future research should extend the analysis of linguistic security beyond the Anglophone–Francophone binary to include other major linguistic systems shaping Africa's cyber and intelligence landscape. In particular, the roles of Portuguese and Arabic warrant systematic investigation, especially within Lusophone Africa (e.g., Angola, Mozambique, Cape Verde) and North African security environments.

Further studies could also examine how emerging digital technologies—such as real-time machine translation, AI-driven intelligence platforms, and multilingual cyber command systems—may reshape linguistic hierarchies in cybersecurity governance. Additionally, empirical fieldwork involving intelligence practitioners

would deepen understanding of how language functions in real operational settings, particularly in joint task forces and cross-border cyber investigations.

Finally, comparative global studies could explore whether Africa's linguistic security challenges mirror or diverge from those in other multilingual regions, thereby contributing to a more comprehensive theory of linguistic interoperability in global cybersecurity governance.

References

Adeniran, A., & Okeke-Uzodike, U. (2021). Cybercrime and regional security in West Africa: Trends, challenges, and responses. African Security Review, 30(2), 157–174. https://doi.org/10.1080/10246029.2021.1905583.

Aning, K., & Dzinesa, G. (2018). Security cooperation in Africa: A reassessment. Routledge.

Bamgbose, A. (2000). Language and exclusion: The consequences of language policies in Africa. LIT Verlag.

Banégas, R. (2020). Francophone Africa and the politics of regional security. Journal of Modern African Studies, 58(3), 355–374. https://doi.org/10.1017/S0022278X20000315.

Berkman, P. A. (2019). Science diplomacy and its role in international cybersecurity. Global Policy, 10(S3), 5–13. https://doi.org/10.1111/1758-5899.12745.

Bourdieu, P. (1991). Language and symbolic power. Harvard University Press.

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology, 8(1), 1–20.

Charbonneau, B. (2017). Intervention in Mali: Building peace between peacekeeping and counterterrorism. Routledge.

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory? International Political Science Review, 27(3), 221–244. https://doi.org/10.1177/0192512106064462.

Fairclough, N. (2013). Critical discourse analysis: The critical study of language (2nd ed.). Routledge.

George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

Interpol. (2021). African cyberthreat assessment report 2021. Interpol.

Mazrui, A. A., & Mazrui, A. M. (1998). The power of Babel: Language and governance in the African experience. University of Chicago Press.

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. International Affairs, 91(1), 111–130. https://doi.org/10.1111/1468-2346.12188.

Pennycook, A. (2017). Posthumanist applied linguistics. Routledge.

Phillipson, R. (1992). Linguistic imperialism. Oxford University Press.

Shelley, L. I. (2014). Dirty entanglements: Corruption, crime, and terrorism. Cambridge University Press.

Taddeo, M., & Floridi, L. (2018). Regulating cybersecurity. Philosophy & Technology, 31(3), 369–373. https://doi.org/10.1007/s13347-018-0325-9.

United Nations Office on Drugs and Crime [UNODC]. (2022). Global report on cybercrime 2022. UNODC.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.