The role of INTERPOL in Combating Cybercrime in West Africa: Lessons from Nigeria and Ghana

El papel de la INTERPOL en la lucha contra la ciberdelincuencia en África Occidental: lecciones de Nigeria y Ghana

O papel da INTERPOL no combate ao crime cibernético na África Ocidental: lições da Nigéria e de Gana

Tola Benjamin Kehinde[1], Anthonia Adeleke[2] and Olileanya Ezugwu[3]

DOI: https://doi.org/10.47741/17943108.860

Cómo citar/How to Cite/Como citar: Kehinde, T. B., Adeleke, A., & Ezugwu, O. (2026). The role of INTERPOL in combating cybercrime in West Africa: lessons from Nigeria and Ghana. *Revista Criminalidad, 68*(2): 153-170. https://doi.org/10.47741/17943108.860

- Date of receipt: 2025/10/30
- Evaluation date: 2026/06/01

Abstract In West Africa, cybercrime has become one of the most intricate security and governance issues that cross national boundaries and challenge the strength of law enforcement organizations. This paper investigates how INTERPOL can be used to tackle cybercrime in the West African region by comparing lessons learnt in Nigeria and Ghana. It examines the impact of organized policing systems, global collaboration, and institutional change on addressing digital crime in the area. A qualitative research design was employed to collect data with the help of semi-structured interviews with officials of the Economic and Financial Crimes Commission (EFCC), the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), and the INTERPOL Nigeria with the supplementary data of data analysis of regional and international reports. The results indicate that, first, informal inter-agency collaboration, especially via INTERPOL channels and bilateral communications has shown to be the most effective in terms of intelligence exchange

Open Access | Diamond Open Access | CC BY-NC-ND 4.0© por Policía Nacional de Colombia

1. PhD candidate in History and International Studies. Redeemer's University. Ede, Nigeria. kehindeto@run.edu.ng
2. PhD candidate in History and International Studies. Redeemer's University. Ede, Nigeria. adelekean@run.edu.ng
3. PhD Candidate in International Relations. Covenant University. Ota, Nigeria. olileanya.ezugwupgs@stu.cu.edu.ng

and retrieving assets. Second, despite the importance of GIABA in aligning anti-money laundering systems, the lack of a consolidated regional approach to cybercrime is still a hindrance to the efficiency of operations. Third, national regulatory and enforcement institutions such as the EFCC, NITDA, CBN, and Ghana's Financial Intelligence Centre (FIC) have developed specialized cybercrime units and protocols that improve investigative outcomes. The study recommends deepening the existing collaborative frameworks through a regionally coordinated cybercrime task network under GIABA's supervision, linking financial intelligence, digital forensics, and law enforcement expertise across West Africa.

Keywords
INTERPOL; cybercrime; cyber diplomacy; Ghana; Nigeria.

Resumen

En África Occidental, la ciberdelincuencia se ha convertido en uno de los problemas más complejos en materia de seguridad y gobernanza, que traspasa las fronteras nacionales y pone a prueba la capacidad de las fuerzas del orden. Este artículo analiza cómo se puede recurrir a la INTERPOL para hacer frente a la ciberdelincuencia en la región de África Occidental, comparando las lecciones aprendidas en Nigeria y en Ghana. Examina el impacto de los sistemas policiales organizados, la colaboración global y el cambio institucional a la hora de abordar la delincuencia digital en la zona. Se empleó un diseño de investigación cualitativo para recopilar datos mediante entrevistas semiestructuradas con funcionarios de la Comisión de Delitos Económicos y Financieros (EFCC), el Grupo de Acción Intergubernamental contra el Blanqueo de Capitales en África Occidental (GIABA) e INTERPOL Nigeria, complementadas con el análisis de datos extraídos de informes regionales e internacionales. Los resultados indican que, en primer lugar, la colaboración informal entre organismos, especialmente a través de los canales de INTERPOL y las comunicaciones bilaterales, ha demostrado ser la más eficaz en lo que respecta al intercambio de información y a la recuperación de activos. En segundo lugar, a pesar de la importancia del GIABA a la hora de armonizar los sistemas de lucha contra el blanqueo de capitales, la falta de un enfoque regional consolidado frente a la ciberdelincuencia sigue siendo un obstáculo para la eficiencia de las operaciones. En tercer lugar, las instituciones nacionales de regulación y aplicación de la ley, como la EFCC, la NITDA, el CBN y el Centro de Inteligencia Financiera (FIC) de Ghana, han creado unidades especializadas en ciberdelincuencia y protocolos que mejoran los resultados de las investigaciones. El estudio recomienda profundizar en los marcos de colaboración existentes mediante una red de trabajo contra la ciberdelincuencia coordinada a nivel regional bajo la supervisión de la GIABA, que conecte los conocimientos especializados en inteligencia financiera, informática forense y aplicación de la ley en toda África Occidental.

Palabras clave
INTERPOL; ciberdelincuencia; ciberdiplomacia; Ghana; Nigeria.

Resumo

Na África Ocidental, o crime cibernético tornou-se uma das questões mais complexas em matéria de segurança e governança, que ultrapassa fronteiras nacionais e desafia a capacidade das organizações de aplicação da lei. Este artigo investiga como a INTERPOL pode ser utilizada para combater o crime cibernético na região da África Ocidental, comparando as lições aprendidas na Nigéria e em Gana. Ele examina o impacto de sistemas de policiamento organizados, da colaboração global e da mudança institucional no combate ao crime digital na região. Foi

empregado um projeto de pesquisa qualitativa para coletar dados por meio de entrevistas semiestruturadas com autoridades da Comissão de Crimes Econômicos e Financeiros (EFCC), do Grupo de Ação Intergovernamental contra a Lavagem de Dinheiro na África Ocidental (GIABA) e da INTERPOL da Nigéria, complementados pela análise de relatórios regionais e internacionais. Os resultados indicam que, em primeiro lugar, a colaboração informal entre agências, especialmente por meio dos canais da INTERPOL e das comunicações bilaterais, tem se mostrado a mais eficaz em termos de troca de inteligência e recuperação de ativos. Em segundo lugar, apesar da importância do GIABA no alinhamento dos sistemas de combate à lavagem de dinheiro, a falta de uma abordagem regional consolidada para o crime cibernético ainda é um obstáculo à eficiência das operações. Em terceiro lugar, instituições nacionais de regulamentação e fiscalização, como a EFCC, a NITDA, o CBN e o Centro de Inteligência Financeira (FIC) de Gana, desenvolveram unidades especializadas em crimes cibernéticos e protocolos que melhoram os resultados das investigações. O estudo recomenda o aprofundamento das estruturas de colaboração existentes por meio de uma rede de tarefas contra crimes cibernéticos coordenada regionalmente sob a supervisão da GIABA, conectando os conhecimentos especializados em inteligência financeira, perícia digital e aplicação da lei em toda a África Ocidental.

Palavras-Chave
INTERPOL; crime cibernético; diplomacia cibernética; Gana; Nigéria.

Introduction

Digital connectivity has reshaped communication, business, and politics in West Africa, yet it has also spawned new types of crime that are disrupting traditional policing models. Cybercrime has become one of the most essential transnational threats in the region, compromising financial systems, national security, and trust among people in digital technologies. Based on the INTERPOL African Cyberthreat Assessment (2021), West Africa is a hot spot where African economies are losing about four billion US dollars a year to cybercrime. Both Nigeria and Ghana are plagued with diverse cybercrime activities such as financial fraud, online romance scams, identity theft, cyberstalking, and phishing (Abubakari, 2024; Lazarus et al., 2025).

The rising internet usage and digital inclusion of the sub region have far exceeded the creation of cybersecurity and law enforcement infrastructure, and criminal networks take advantage of structural vulnerabilities in regulation, coordination, and investigation. The national governments in the region have reacted to this by establishing legal and institutional mechanisms to deal with these emerging threats. The Economic and Financial Crimes Commission (EFCC) and the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 in Nigeria and the Cybersecurity Authority and Cybersecurity Act of 2021 in Ghana are important examples of policies that attempt to criminalise and prevent cybercrimes. But these systems have had unequal outcomes. A significant number of cybercrime activities start off in a jurisdiction and have a financial and technical presence elsewhere, making national enforcement insufficient in its own right. Criminal actors use transnational digital infrastructures, encrypted communication channels, and schemes of money-laundering that are beyond the scope of investigation of the individual states (Hall & Zeimer, 2023).

Recent criminological research highlights the fact that cyber fraud in West Africa is no longer confined to a specific place but operates through a 'global scamming ecosystem' with an identifiable typology of actors (Button et al., 2025). This ecosystem has been linked to strategic criminal mobility, for instance, the documented cross-border movement of online romance fraudsters and Sakawa actors into Ghana from Nigeria in order to avoid rotating domestic enforcement pressures (Lazarus et al., 2025; Abubakari, 2024).

Consequently, the region of West Africa has emerged as an epicentre of examining the effectiveness of international policing cooperation in addressing cross-border, cross-jurisdiction cyber threats. The reality of enforcement is starkly reflected in the latest operational data; in Nigeria's case, the Economic and Financial Crimes Commission (EFCC) reported a record 4111 convictions in 2024, with advance fee fraud and cybercrime the two most common crimes (Vanguard, 2025). This enforcement intensity has helped to force localized criminal networks into a more structural transformation in cyberfraud operations, which has increasingly forced them to move to another region.

In this regard, the International Criminal Police Organization (INTERPOL) has been playing a strategic role in the exchange of information, coordination of intelligence, as well as joint operations between the law enforcement agencies in West Africa. The organization aims at closing the gaps

between national authorities and improving their overall response to cyber threats through such programs as the African Cybercrime Operations Desk, the INTERPOL Global Complex for Innovation (IGCI), and the West African Police Information System (WAPIS) (Yansaneh, 2020). Such multilateral policing is demonstrated through operations organized within such frameworks, such as Operation Jackal (2022-2023), which exemplify the possibilities and constraints of multilateral policing. Operation Jackal involved the coordination of twenty-five countries by INTERPOL to dismantle West African organized cybercrime rings behind large scale business email compromise schemes (INTERPOL, 2023). The operation resulted in more than two hundred arrests and seizure of illicit assets and digital evidence thus proving the operational relevance of global coordination in addressing transnational crime.

Nevertheless, the overall effectiveness of the campaign of INTERPOL in West Africa is still disputed despite these successes. The existence of differences in infrastructure, insufficient access to the INTERPOL I-24/7 secure communications network, and uneven adherence to data-sharing guidelines tend to put cooperation structures below their capacities (Calcara, 2021). The language diversities of the region, institutional fragmentation and legal differences on the definition of cyber offence also make cross-border investigations more difficult. Also, local political and bureaucratic restrictions often impede the timely cooperation thus resulting in the delays in the investigation and the poor prosecution results.

Scholars have noted that although INTERPOL is an invaluable platform of cooperation, its success is largely influenced by the political goodwill, technical capabilities and legal harmonisation among the member states (Akande et al., 2022; Forest, 2022; Stock, 2023). Nigeria and Ghana provide valuable comparative lessons about the relations between international policing systems and local enforcement capabilities. Nigeria is one of biggest centres of cyber-facilitated fraud, but also has one of the most developed law enforcement systems in the area. The partnership of the EFCC with INTERPOL has enabled high-profile apprehensions and asset. Ghana, on the other hand, has focused on capacity building and institutional changes within its Cybersecurity Authority and demonstrated better coordination with the international community, but still combats challenges in forensic investigation and prosecution (Apau & Koranteng, 2020; Ojewumi et al., 2022).

This paper critically reviews how INTERPOL has helped to fight cybercrime in West Africa by looking at the case of Nigeria and Ghana. It examines the impact of the programmes and activities of INTERPOL on the investigative strengths and capabilities of countries, inter-agency cooperation and policymaking. It also determines the structural constraints that persist in minimizing the operational implications of transnational policing in the region. The paper places the discussion in the context of the criminological framework, which is why it adds to the existing discussions on international police cooperation, sovereignty, and how to govern digital security in the Global South.

Methodology

The study adopts a qualitative and exploratory research design, which focuses on investigating the role of INTERPOL in fighting cybercrime in West Africa, specifically in Nigeria and Ghana. The study uses documentary analysis and empirical data collected through expert interviews to gain a multi-dimensional understanding of the functioning of transnational policing frameworks in a regional dimension. Primary data collection was done through semi-structured interviews with officials from critical institutions in cybercrime response and coordination, who have been interviewed for the first time. A total of nine officials were interviewed.

These interviews were conducted with five officials of the Economic and Financial Crimes Commission (EFCC), an official from the INTERPOL National Central Bureau in Abuja, two officials of the National Information Technology Development Agency (NITDA), and another one from the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA). These interviews provided first-hand experience in cooperation, information sharing, capacity and limitations and the realities of transnational investigations.

Secondary data were also collected to complement these findings in the shape of an INTERPOL report on African Cyberthreat Assessments (2021-2024), GIABA Typology Reports on Money Laundering with Cybercrime Proceeds, and domestic cybercrime laws in Africa, alongside studies of peer-reviewed research on global policing and cybergovernance.

Such a combination of sources guaranteed methodological triangulation and added reliability and depth of the analysis. The data was analysed using thematic content analysis, which revealed institutional coordination, legal harmonization, resource asymmetry and politics of regional enforcement as central tendencies. Ethical considerations were addressed in line with standard qualitative research practices. Interviews were conducted with the informed verbal consent of participants and were voluntary.

Results and discussions

The idea of cyber diplomacy has come out as a remarkable tool of global reaction to the issue of cybercrime, offering a measure of connectedness between the national law enforcement operations and the shifting, transnational character of digital threats. Cyber diplomacy is no longer merely an extension of law enforcement in West Africa, as the environment is full of cyber-enabled fraud and financial crimes that often cross jurisdictional borders and are a primary tool of keeping the region stable and economically intact (Attatfa et al., 2020). The concept of cyber diplomacy includes diplomatic, legal and institutional avenues to negotiate cooperation structures, exchange intelligence, coordinate laws and enhance common abilities of the states to avert, investigate and convict cybercrimes. For Nigeria and Ghana, two region's key digital economies, active engagement in cyber-diplomatic affairs has become essential to their national cybersecurity posture. This is evident in their involvement within INTERPOL and in the Economic

Community of West African States (ECOWAS), as well as their global cooperation with the European Union and the United States.

From a criminology perspective, the governance of cybercrime in West Africa can be understood as a networked system of multiple interdependent actors. This paper is grounded in the criminological frame of nodal governance, which theorises crime regulation as a practice enforced by more than one sovereign entity. The results indicate that the system of cybercrime governance in Nigeria and Ghana is based on decentralized nodes, such as INTERPOL, national law enforcement services, financial intelligence, regulatory institutions and the players of the private sector. This networked structure highlights increased dependence of informal collaboration and intelligence-sharing processes in transnational control of cybercrime. The study however also uncovers governance tensions due to unequal state capacity, legal fragmentation and gaps in accountabilities in these networks. Through a West African case study, the paper contributes to criminological literature on networked governance by illustrating how institutional asymmetries influence the nature and performance of transnational policing in the Global South.

The rationale behind cyber diplomacy in the West African scenario is based on the need. Enterprises that are carried out by cybercriminals usually do so by taking advantage of jurisdictional gaps between states and the ineffective cross-border enforcement systems to avoid detention and charges. Due to this, the unilateral actions of national authorities like the EFCC or the Ghana Cybercrime Unit only have a small effect. The emergence of organized cyber syndicates, which are usually executed using the digital infrastructures in several states, has highlighted the boundaries of conventional policing and the need to develop a comprehensive international system of governing cyber.

Law enforcement agencies also use cyber diplomacy as a channel of sharing intelligence as well as negotiating mutual legal assistance treaties (MLATs), capacity-building alliances, and joint task forces. As an example, the partnership between Nigeria and the FBI, and that between the National Crime Agency (NCA) and the UK can illustrate how partnership in law enforcement can occur through diplomatic means even in the event that no treaties exist. These collaborations have already received tangible outcomes in both transnational fraud and asset recovery cases.

In addition to official bilateral and multilateral systems, cyber diplomacy can also serve as a trust-building tool improving the legitimacy and confidence needed to continue cooperating. Through the leadership of GIABA and ECOWAS, the states in West Africa have progressively employed diplomatic contacts and strategies to harmonize national laws against cybercrime with the international laws, especially the stipulations of the Budapest Convention on Cybercrime. Though the West African countries are not signatories to all, the impact of this convention has been used to shape the use of national cybersecurity strategies and formation of Computer Emergency Response Teams (CERTs) throughout the sub region.

Nevertheless, implementing cyber diplomacy can be effective in deterring cyber frauds based on the level of consistency and the political desire of states to transform diplomatic engagements into operational coordination. The experience of Nigeria proves that the alignment at the diplomatic level should be supported by domestic institutional reforms, legal harmonization, and inter-agency

co-ordination. Equally, the proactive involvement of Ghana in the diplomacy has been most successful when augmented with national funding of digital forensics and training of prosecutors. The continuing process of dialogue between ECOWAS member countries facilitated by GIABA with the assistance of INTERPOL points that cyber diplomacy in West Africa is shifting its informal interaction to a more formal structure.

Nevertheless, there are still critical issues, such as the necessity to standardize the procedures of digital evidence, ensure that the intelligence-sharing systems are safe, and preserve the sovereignty of data even in the context of the enhanced international collaboration. However, according to this paper, cyber diplomacy is still the most plausible route toward establishing a coordinated and resolute regional process of fighting transnational cyber fraud.

The interviews of the key officials in the EFCC, GIABA (in Nigeria), and INTERPOL indicate a multi-layered and dynamic strategy of addressing cybercrime in West Africa. This is because the results indicate that there is a continued development of cyber-facilitated criminality that is influenced by technological advancement, young people, and global financial weaknesses. Simultaneously, the reactions of national and regional institutions reveal both the advances achieved in the area of cross-border policing and the institutional constraints that do not allow achieving sustainable deterrence.

One theme that has surfaced repeatedly because of the Nigerian context is the paradox of the technological innovation and deviance. According to one of the respondents of the EFCC, due to the ingenuity of the youth, instead of applying the different technological devices to their benefit, they now apply this technology to commit bad acts merely to earn money. Cybercrime in West Africa has taken the form of commodification of technological-based lying. A large number of juvenile offenders use digital instruments, artificial intelligence, and social engineering strategies to impersonate identities and swindle foreign women and men. The fact that technological creativity has been turned into a source of criminal enterprise stresses a criminological paradox, namely that it is the same infrastructure that facilitates digital entrepreneurship that enables transnational fraud networks.

The operational policy of the EFCC demonstrates a multi-layered and pragmatic type of transnational cooperation. International cooperation between the government and foreign governments like the Federal Bureau of Investigation (FBI) and the United Kingdom National Crime Agency (NCA) has become a foundation of cybercrime enforcement. The interviews underscore a dual-track system of cooperation: one that is formal and regulated by mutual legal assistance treaties (MLATs), and another that is informal, based on intelligence give and take. According to the officials, the latter is faster and more dependable, and day-to-day information sharing occurs with the help of secure email and encrypted communication. Using these unofficial channels, data on intercountry transactions, movements of offenders, and online tracks is rapidly passed and responded to (EFCC official, personal communication, August 2025). On the contrary, such formal cooperation as the Central Authority Unit under the Ministry of Justice in Nigeria is characterized as procedurally complex and shows the rigidity of the international transfer of evidence in its procedures (GIABA representative, personal communication, August 2025).

This lack of correspondence between official and unofficial cooperation exemplifies a bigger criminological conflict between legal sovereignty and performance effectiveness. Though informal dealings are faster in enforcement, they are in the legal grey area: the information obtained in such a case is usually inadmissible in court. As a result, this presents a paradox to investigators; they have actionable intelligence but are bound by evidentiary standards which favour due process over speed (GIABA representative, personal communication, August 2025). The dilemma is reflective of results in more generalized transnational policing literature in which a fast intelligence can be followed by a slow justice.

The involvement of the EFCC in transnational policing groups, including the Egmont Group of Financial Intelligence Units (FIUs) and forums of international asset-recovery, shows that Nigeria is deeply integrated into the international anti-money-laundering (AML) regime (EFCC official, personal communication, July 2025). Under the Nigeria Financial Intelligence Unit (NFIU), domestic investigators can have access to the financial data and suspicious transactions reports that are exchanged among jurisdictions. However, as one of the authorities stressed, what is obtained at the NFIU cannot be admitted in the courtroom, it is just information or intelligence (EFCC official, personal communication, July 2025). This limitation portrays an epistemological disconnect between intelligence and evidence, and it is why there is a need to have tougher legal measures that would help convert financial intelligence into prosecutable material.

On a regional level, the results of the interviews with the representatives of GIABA emphasize the institutionalization of the standards of anti-money-laundering as a method of controlling cybercrime. GIABA is the West African Financial Action Task Force (FATF)-like regional organization that ensures the adherence of member states to the international standards of anti-money laundering and counter-terrorist financing. Its jurisdiction goes beyond money laundering that involves the traditional financial crimes to cover the cases of money laundering that deal with cybercrime especially when digital fraud gives rise to cross-border financial transactions. The official explained the role of GIABA as making the countries comply with international standards established by the FATF, by the 40 recommendations aimed at rendering the national financial systems less vulnerable to cybercrime and money laundering (GIABA representative, personal communication, August 2025).

Based on the interviews, the new legal changes in Nigeria, the Money Laundering (Prohibition and Prevention) Act, the Terrorism Prevention and Prohibition Act, and the Proceeds of Crime (Recovery and Management) Act, all of which were adopted within 2022-2023, were mostly facilitated by the technical advice and assistance of GIABA. These changes in legislation played a major role in trying to pull Nigeria out of the FATF greylist which has raised massive concerns in the ability of Nigeria to trace and recover illicit funds in the country. The process demonstrates how the supranational evaluation process, like mutual evaluation report, may trigger domestic legal modernization (GIABA representative, personal communication, August 2025). Nevertheless, it also reflects a structural dependence: the West African states tend to reform in reaction to the external evaluation mechanism, but not as a proactive criminological planning.

The regulation of cybercrime in West Africa is increasingly shaped by a hybrid architecture of transnational governance, driven by the interaction between the enforcement activity of the EFCC and the regulatory oversight of GIABA. The agencies of the country impose, the regional associations standardize and the partners in the international relations organize. However, this architecture is still weak, full of imbalance of distribution of resources, lack of interoperability of databases, and informal communication continues to be used as an alternative to institutional trust. In spite of this fragility, the Nigerian experience shows how, despite the lack of effectiveness at present, there is an incremental move towards acknowledging that cybercrime policing can no longer be exercised through the usual territorial logics but, instead, through the less rigid, intelligence-driven, and diplomatically mediated collaboration.

The contribution of INTERPOL in the West African cybercrime enforcing environment proves to be both catalytic and limiting. Investigations with the representatives of INTERPOL in Nigeria have shown that the role of the organization is not limited to sharing intelligence but also includes coordinating multinational activities strategically. INTERPOL also serves as a channel in which local organizations like the EFCC, Nigeria Police force and Cybercrime Unit in Ghana can access international databases, alerts, and notices. Practically, this form of coordination helps to close the intelligence gap between local and international law enforcement systems and allows tracing, detecting, and disrupting transnational cyber networks.

Operations like Cyber Surge (2023) and Jackal (2022-2023) are the most demonstrative examples of the involvement of INTERPOL as both activities were organized enforcement operations involving a number of West African states, including Nigeria, Ghana, Cote d'Ivoire, and Cameroon. These efforts focused on cyber-enabled fraud and business email compromise (BEC), rings of extortion over the internet which drained millions of dollars on the victims in Europe, North America, and Asia. The operations led to dozens of arrests, confiscation of digital devices and retrieval of illegal funds. Nigerian officials underlined that this joint action became possible due to the constant exchange of digital forensic intelligence by the means of the INTERPOL I-24/7 channel and the INTERPOL Global Complex of Innovation (IGCI) in Singapore (Stalcup, 2013). The same case happened to the Ghanaian experience, where the national police cyber unit relied on the digital forensics support of INTERPOL to process data on the servers and mobile devices that have been taken.

Nonetheless, the interviews and the analysis of the documents reveal that these successes are disguised with serious structural obstacles. One EFCC official, a senior one, observed that although the activities of INTERPOL make the operation visible and coordinated, the real depth in the investigation remains a matter of the domestic agencies. By its design, INTERPOL does not have the ability to prosecute anyone and solely depends on the goodwill and ability of member states to conduct follow-up investigations (EFCC official, personal communication, July 2025). The continuity between the operation of INTERPOL and that of the local prosecutions frequently fails within the Nigerian and Ghanaian environments where institutional fragmentation and bureaucratic duplication remain deeply problematic. Apprehensions of offenders through international operations are not necessarily followed by conviction, and this is mostly because of the evidence admissibility issues and lack of inter-agency communication after the operation is complete.

The situation in Ghana shows the problem of coordination and capacity. Ghana Police Service, via its Cybercrime Unit has been successful in capacity building of digital forensic with the assistance of INTERPOL as well as Global Action on Cybercrime (GLACY+), programme by the European Union (Nartey et al., 2025). The officers of the unit are now trained in forensic imagery, malware, and open-source intelligence methods. However, the Ghanaian officials acknowledge the fact that national response is largely donor-supported and capacity-oriented. Cybercrime infrastructure, labs and other specialized prosecutors are often funded by external grants, not by the state sustainable budgets. This reliance solidifies a lopsided concept of collaboration in which local agencies continue to be executing and deploying systems that have been developed externally instead of creating their own localized cyber policing approaches.

The comparison between Nigeria and Ghana shows a more general pattern in the region: the centrality of international cooperation in maintaining cybercrime enforcement. The structure of INTERPOL has made a platform of operational synergy between West African states, but the effectiveness of this is determined by the levels of political will and institutional cohesiveness in the states. The legal systems of both nations have been adapted to cybercrime policing, with the law enforcement of the countries having Cybercrime (Prohibition, Prevention, etc.) Act 2015 and Electronic Transactions Act 2008 as the legal basis of their regulatory framework. The interviews, however, indicate that application is still patchy, which is, in part, because prosecutors vary in expertise and judges vary in their knowledge of digital evidence. This imbalance enables the cybercriminal networks to take advantage of the gaps in jurisdiction and shift their activities in and out of states in order to go undetected.

One of the most frequent common themes among all the respondents was that trust, both interpersonal and institutional, is a very important factor to cross-border cooperation (INTERPOL Nigeria officer, personal communication, October 2025). Non-legal mutual legal assistance systems are frequently replaced by informal trust networks among investigators as previously noted in the transnational policing literature. Even off official missions, the EFCC and INTERPOL officials reported common informal intelligence exchanges with Ghanaian and foreign investigators. This is a pragmatic, and a necessity, in such an atmosphere where bureaucratic inertia is likely to paralyze anything, personal relationship between investigators tend to keep things moving. However, the same informality brings into doubt the accountability and protection of data as well as long-term cooperation even after the individual officers are removed.

Criminologically, the relations between INTERPOL, the EFCC, and GIABA will become a new networked governmental model where the power is distributed among various nodes, including national, regional, and international. This model is not the old Westphalian concept of policing as a sovereign role which was imposed within boundaries. Rather, an example of cybercrime policing in West Africa can be viewed as a type of "transnational assemblage," in which enforcement is implemented based on overlapping institutional logics: the coordination of INTERPOL, the regulatory mandate of GIABA, and the enforcement mandate of domestic agencies. The success of this assemblage relies on the legal frameworks, but also on the interoperability of data systems, mutual trust, and professional culture among actors of enforcement.

Although there are significant success stories, the interviews indicate clearly that the enforcement of cybercrime in West Africa is still structural in response. INTERPOL has enhanced tactical communications and is yet to gain strategic autonomy via regional coordination. Nigeria and Ghana still do things within the paradigms that are dictated by the external stakeholders like FATF, INTERPOL and the donor agencies. Regional policing will pose a threat of recreating dependency instead of creating resilience without localized research-based policies. The West African problem, therefore, is two-pronged, the issue being first to empower national institutions to be able to maintain international cooperation, and second to translate functional collaborations into tangible deterrence and legal outcomes.

The increased transnationalism of cybercrime in West Africa highlights the insufficiency of localized national solutions. Although organisations such as Nigerian EFCC or Ghana Economic and Organised Crime Office (EDCO) have recorded significant steps in ensuring that cyber-crime offenders are brought to book, they are limited in their scope by the nature of cyber-crime, which is borderless. In the interviews conducted with law enforcement officials, fragmentation is still observed even in national jurisdictions between the different bodies dealing with cybercrime control. These flaws become intensified where cases cross borders oftentimes causing jurisdictional issues, challenges in admissibility of evidence and delays in monetary redemption.

A more integrated regional structure is hence needed. The porous borders in West Africa combined with the common language and culture have rendered the region an opportune bedrock to the spread of cyber-enabled fraud groups (Obah-Akpowoghaha et al., 2020). Regional coordination should not be just an act of information sharing but develop into an effective harmonised system of cyber governance. The contribution of GIAA in this mechanism is especially important. As the Financial Action Task Force for West Africa, GIABA is at the intersection point of anti-money laundering (AML), counter-terrorist financing (CFT), and financial integrity framework. GIABA implements the 40 recommendations of FATF, which forces its member states to have good regimes in detecting and tracing of illicit financial flows, most of which are rooted in cyber-fraud related activities. The data gathered in the interview indicate that the periodic mutual evaluations conducted by GIABA have played a significant role in pressuring the member states such as Nigeria and Ghana to upgrade their legal and institutional structures.

In the case of Nigeria, the supervision of GIABA directly affected the passing of Money Laundering (Prevention and Prohibition) Act, the Terrorism (Prevention and Prohibition) Act, and the Proceeds of Crime (Recovery and Management) Act in 2023. Through these reforms, Nigeria was brought a step closer to FATF compliance and it also increased the capacity of the EFCC in tracing digital proceeds of crime. The collaborative processes which are encouraged by GIABA like regional workshops and financial intelligence training have contributed to inter agency synergy. Nevertheless, the region still does not have a standardized system in cross-border exchange of evidence and digital forensic, and it still compromises the speed and admissibility of prosecutions.

One of the most important aspects of this coordination dilemma is harmonisation of Financial Intelligence Units (FIUs). The NFIU of Nigeria and the Financial Intelligence Centre (FIC) of Ghana are both members of the Egmont Group network, where suspicious transactions are shared. However, these FIUs frequently work under other legislative and procedural doctrines and thus intelligence

outputs are hard to be mutually recognized. Standardising operational practices of FIUs in the region, by way of technical leadership of GIABA, would not only make interoperability, but also minimise redundancy of effort in tracking cyber-related financial offences (Chawki, 2009). This type of harmonisation may result in the establishment of a West African Financial Intelligence Exchange Protocol, which is a regional mechanism of the rapid recognition of intelligence and mutual search and seizure actions.

The landscape of cross-border cyber governance has been significantly reshaped by the adoption of the United Nations Convention against Cybercrime in late 2024. As a landmark global framework, the treaty provides standardized mechanisms for the expedited preservation and disclosure of electronic evidence, directly optimizing how law enforcement agencies in developing nations cooperate across jurisdictions. For West African nations like Nigeria and Ghana, aligning domestic law enforcement protocols with this UN framework establishes 24/7 points of contact for rapid digital evidence sharing, thereby mitigating the traditional legal barriers that have historically hindered transnational cyberfraud investigations.

Cybercrime enforcement is slowly ceasing to be an EFCC responsibility within Nigeria and is increasingly becoming more networked and encompassing other agencies and regulators. The Nigerian Communications Commission (NCC) has a proactive role because it ensures there is registration of SIM cards and monitoring digital service providers to reduce identity-based frauds. The Central Bank of Nigeria (CBN) has also put loaned Know-Your-Customer (KYC) and anti-money laundering rules as a binding requirement to all financial institutions, which further narrows the loopholes that cybercriminals use. NITDA has a role to play in terms of enforcing data protection policies to enhance cyber hygiene by service providers and users (NITDA official, personal communication, July 2025). These structures are further filled with specialized units in agencies like the National Agency against Trafficking in Persons (NAPTIP) and the Cybercrime Unit of the Nigeria Police Force. As an example, NAPTIP recently revealed sexually exploitative and trafficking networks that use electronic platforms to recruit and coerce victims. All of these agencies as a whole are part of a developing yet still incomplete cybersecurity ecosystem that needs to be better coordinated and integrated legislatively.

The same situation is observed in Ghana. The passage of the Cybersecurity Act of 2020 by the Ghanaian government formalized the Cyber Security Authority (CSA), a body that will act as the national coordinating organ to respond to the cyber incidents, create cybersecurity awareness, and enforce the regulation of cybersecurity. The EOCO in Ghana works closely with the Financial Intelligence Centre and Bank of Ghana to detect the suspicious transactions related to online fraud and money laundering. Moreover, Ghana was also involved in regional activities, including Operation Jackal II by INTERPOL in 2023, which showed that the agencies of the West African region can collaborate in massive transnational investigations. The raid resulted in the arrest of several suspects in Ghana and Nigeria, the confiscation of digital equipment, and the retrieval of the fraud funds. However, in Ghana, similar to Nigeria, the ecosystem of enforcement is still isolated, and financial regulators, the police, and specialized cyber units have few integrations.

As the cases of both Nigeria and Ghana demonstrate, there are two sides to the issue of cybercrime governance in West Africa: on the one hand, there is improvement at the national

level, and on the other hand, there is disintegration at the regional one. An official West African Cybercrime Coordination Framework under the banner of GIABA and ECOWAS is required to achieve a sustainable response (Ifeakandu & Ardzard, 2022; Olowookere & Adewale, 2020). The framework must incorporate cybercrime policing, financial intelligence and digital forensics into a common platform which is facilitated by the I-24/7 network of INTERPOL. This would codify the sharing of data on a continuous basis, align investigative principles and facilitate multilateral recovery of assets. Other areas that should be incorporated in the policy direction will be the integrating cyber legislation, standard training materials to be used by investigators and regional database of cyber offenders and typologies. Criminologically, the analysis shows how transnational cybercrime control is made effective and constrained in West Africa through the influence of networked governance structures.

Conclusion and Policy Implications

The findings indicate how transnational cybercrime control can be effective and limited by networked systems of governance in West Africa, and that effectiveness is not merely a problem of national institutions. The war on cybercrime in West Africa is on the crossroads between national enforcement efforts and international collaboration. The case study of Nigeria and Ghana shows that although both of the states have developed significant institutional structures, the dynamic nature of cybercrime keeps pointing to the shortcomings of nationalized responses. The wide-ranging cooperation of the EFCC with the agencies, including the FBI, the NCA, and other foreign organizations, has brought significant gains in the area of investigation and assets recovery in Nigeria. The proactive strategy of Ghana, which is institutionalized by its Cyber Security Authority and EOCO, reflects this development. However, regardless of the improvements, the two systems continue to suffer with jurisdictional loopholes, legislative discrepancies and sluggishness in the process of mutual legal assistance. What is obtained is a regional enforcement landscape that is strong in some areas but with no single architecture on how it coordinates and remains sustainable.

The main lesson that comes out of this research is that the key to successful cybercrime management in West Africa is a strategic move to stop a country-specific policy of addressing cybercrime to a harmonized regional regime. The unstructured forms of collaboration that already exist among the agencies such as the emails, joint task forces and ad hoc intelligence exchange should be formalized into an ingrained system that has clear protocols and which has joint responsibility. The current basis of this is provided in the position of GIABA as the regional body of the FATF. Its track record in marketing anti-money laundering and counter-terrorist financing principles provide it with the technical ability, as well as political authority, to take the lead in the coordination of cyber-financial activities at the regional level. GIABA can develop a cross-border culture of compliance by reaching out to cybercrime indicators through its monitoring and evaluation mechanisms.

One of the viable starting points towards integration is the harmonization of Financial Intelligence Units (FIUs). The NFIU in Nigeria and FIC in Ghana are already members of the Egmont Group but their collaboration is still more of a bilateral and unorganized form. Regional FIU coordination procedure under the control of GIABA and in line with the recommendation of

FATF on international cooperation would permit quicker intelligence confirmation, coordinated suspicious transaction reporting, and joint asset restoration. The model would become a regional Financial Intelligence Fusion Centre covering West Africa as a repository of cross-border financial data that is connected with cyber-enabled crime.

On the national level, it is evident that there is a need to enhance inter-agency cooperation. The EFCC cannot solely rely on the battle against cybercrime in Nigeria. The NCC, CBN, and NITDA as well as special cyber units within NAPTIP and Nigeria Police Force are important elements of a holistic cyber governance system. By consolidating these actors into a single cybercrime coordination council, this will reduce overlaps and enhance operational capabilities as well as create cohesiveness in the execution of regulatory, preventive, and enforcement functions. The Cyber Security Authority in Ghana can also expand its coordination mandate by aligning financial regulators, law enforcement as well as players in the private sector by a joint national policy framework on cybersecurity.

The networked aspects of cybercrime enforcement across several nodes require West Africa to treat the problem as a governance challenge and not a policing one. GIABA and INTERPOL should collaborate with regional political institutions like ECOWAS to establish a West African Cybercrime Coordination Framework. The mechanism would entrench the I-24/7 network in the region, enhance the exchange of digital evidence, and standardize training and certification of investigators of cybercrime. This type of structure must also require the annual cyber drills of the region, workshops of peer learning, and a central database of all cyber criminals and typologies that are available to all member states.

Policy implications are thus two-fold. To begin with, cybercrime in West Africa has to be discussed as a transnational governance concern. This therefore demands financial, legal, and technical efforts. Second, long-term political commitment and institutional assimilation is essential so as to avoid fragmentation. Greater emphasis should be put on regional cooperation in enhancing networked governance in cybercrime so that nodes at national and regional levels operate in a well-coordinated manner. With the synergistic value of sharing the national capabilities, GIABA oversight, and the global presence of INTERPOL, West Africa is able to shift away to a patchy form of enforcement to a fitful regional security system.

The complexity of cybercrime will keep changing with the technology in its transnational nature. However, through harmonized frameworks, shared accountability, and inexorable dedication to regional solidarity, West Africa can develop an adaptive, intelligence-driven, and collaborative concept of cyber governance, one that is not only capable of responding to threats, but also determining the digital future of the area.

Acknowledgement

The authors extend sincere appreciation to officials from the Economic and Financial Crimes Commission (EFCC), the National Information Technology Development Agency (NITDA), INTERPOL Nigeria, and the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) for their valuable insights and cooperation during the course of this research.

Their professional perspectives and practical experiences significantly enriched the analysis and contributed to a deeper understanding of the institutional dynamics and regional frameworks shaping cybercrime control efforts in West Africa.

Conflict of Interest

No conflict of interest was identified in the development of this academic research. I declare that I have no financial, professional, or personal relationships that could influence the study design, interpretation, or publication of the results. Furthermore, I affirm my compliance with ethical standards and scientific integrity, in accordance with the guidelines established by the academic community and this journal.

References

Abubakari, Y. (2024). Modelling the modus operandi of online romance fraud: Perspectives of online romance fraudsters. *Journal of Economic Criminology*, *6*, e100112. https://doi.org/10.1016/j.jeconc.2024.100112

Akande, O. N., Akande, H. B., Kayode, A. A., Adeyinka, A. A., Olaiya, F., & Oluwadara, G. (2022). Development of a real time smishing detection mobile application using rule based techniques. *Procedia Computer Science*, *199*, 95-102. https://doi.org/10.1016/j.procs.2022.01.012

Apau, R., & Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, *2*, 299-309. https://doi.org/10.1016/j.fsisyn.2020.10.002

Attatfa, A., Renaud, K., & De Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, *176*, 60-69. https://doi.org/10.1016/j.procs.2020.08.007

Button, M., Hock, B., Suh, J. B., & Koh, C. S. (2025). Policing cross-border fraud 'Above and below the surface': Mapping actions and developing a more effective global response. *Crime, Law and Social Change*, *83*(1), 5. https://doi.org/10.1007/s10611-024-10186-2

Calcara, G. (2021). Balancing international police cooperation: INTERPOL and the undesirable trade-off between rights of individuals and global security. *Liverpool Law Review*, *42*(2), 111-142. https://doi.org/10.1007/s10991-020-09266-9

Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of information, Law and Technology*, *1*(1), 1-20.

Forest, J. J. (2022). Crime-terror interactions in sub-Saharan Africa. *Studies in Conflict & Terrorism*, *45*(5-6), 368-388. https://doi.org/10.1080/1057610X.2019.1678881

Hall, T., & Ziemer, U. (2023). Cybercrime in Commonwealth West Africa and the regional cyber-criminogenic framework. *The Commonwealth Cybercrime Journal*, *1*(1), 5-27.

Ifeakandu, I. O., & Ardzard, H. (2022). The role of institutional framework in entrenching effective anti-money laundering/combating terrorist financing in West Africa: Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) in perspective. *Beijing Law Review*, *13*(3), 575-593. https://doi.org/10.4236/blr.2022.133037

INTERPOL. (2023). Annual Report 2023. https://www.INTERPOL.int/content/download/22267/file/INTERPOL%20Annual%20Report%202023%20EN.pdf

INTERPOL. (2021). Africa Cyberthreat Assessment Report 2021. https://www.INTERPOL.int/en/content/download/21048/file/AJFOCAfrica%20Cyberthreat%20Assessment%20Report2024.pdf

Lazarus, S., Button, M., Garba, K. H., Soares, A. B., & Hughes, M. (2025). Strategic business movements? The migration of online romance fraudsters from Nigeria to Ghana. *Journal of Economic Criminology*, *7*, e100128. https://doi.org/10.1016/j.jeconc.2025.100128

Nartey, C., Quaye, S., & Dawson, M. (2025). A case study on Ghana's cybersecurity posture: Strengthening cybercrime enforcement and regional cooperation in West Africa. *Research Association for Interdisciplinary Studies*, 85-96. https://doi.org/10.5281/zenodo.16894954

Obah-Akpowoghaha, N. G., Ojakorotu, V., & Tarro, M. L. (2020). Porous Borders and the Challenge of National Integration in Africa: A Reflection of Ghana, Republic of Benin and Nigeria. *Journal of African Foreign Affairs*, *7*(3). https://hdl.handle.net/10520/ejc-aa_jafa-v7-n3-a6

Ojewumi, T. O., Ogunleye, G. O., Oguntunde, B. O., Folorunsho, O., Fashoto, S. G., & Ogbu, N. J. (2022). Performance evaluation of machine learning tools for detection of phishing attacks on web pages. *Scientific African*, *16*, e01165. https://doi.org/10.1016/j.sciaf.2022.e01165

Olowookere, T. A., & Adewale, O. S. (2020). A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. *Scientific African*, *8*, e00464. https://doi.org/10.1016/j.sciaf.2020.e00464

Stalcup, M. (2013). Interpol and the emergence of global policing. In W. Garriott (Ed.), *Policing and Contemporary Governance: The Anthropology of Police in Practice* (pp. 231-261). Palgrave Macmillan. https://doi.org/10.1057/9781137309679_10

Stock, J. (2023). Interpol: the past, present and future of international police cooperation. *Belügyi Szemle*, *71*(3), 89-95. https://doi.org/10.38146/BSZ.SPEC.2023.3.8

Vanguard. (2025, March 10). EFCC secures 4,111 convictions, biggest asset recovery in 2024. *Vanguard News*. https://www.vanguardngr.com/2025/03/efcc-secures-4111-convictions-biggest-asset-recovery-in-2024/

Yansaneh, M. L. (2020). The West African Police Information System (WAPIS) A catalyst to regional security integration in West Africa. *International Journal of Novel Research in Humanity and Social Sciences*, *7*(4), 16-28. https://www.noveltyjournals.com/upload/paper/paperpdf-1595067443.pdf