RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
August 7-8, 2025
DOI:10.5281/zenodo.16894954

A Case Study on Ghana's Cybersecurity Posture: Strengthening Cybercrime Enforcement and Regional Cooperation in West Africa

Cedric Nartey[1], Samson Quaye[2], Maurice Dawson[3]

[1]*Illinois Institute of Technology, Chicago, Illinois, United States, cnartey1@hawk.illinoistech.edu*
[2]*Illinois Institute of Technology, Chicago, Illinois, United States, squaye@hawk.illinoistech.edu*
[3]*Illinois Institute of Technology, Chicago, Illinois, United States, mdawson2@illinoistech.edu*

Abstract: Given the borderless nature of cyber threats, this study examines the collaboration to combat cybercrime through legal frameworks and law enforcement in Ghana and its neighboring countries. Many West African countries still have underdeveloped cybersecurity laws or strategies. For instance, as of 2021, only 29 out of 54 African states had enacted cybersecurity legislation, and just 10 had a national cybersecurity strategy. This fluctuating landscape allows criminals to exploit jurisdictions with weaker laws. Ghana stands out as a regional leader—ranked among the top in Africa for cybersecurity maturity— taking steps in ratifying the Budapest Convention on Cybercrime and the African Union's Malabo Convention. However, Ghanaian officials have cautioned that this progress "will be meaningless if other African countries do not develop along the same line, as cyber insecurity in one country has a real impact on another." This study explores mechanisms to bolster regional enforcement: harmonizing laws through Economic Community of West African States (ECOWAS) initiatives, improving cross-border information sharing, and building capacity among police and judicial authorities to handle digital evidence. The topic directly engages law enforcement and democratic institutions, since a secure cyberspace is essential for stable governance. It aligns with current policy needs by offering practical recommendations—such as cooperative frameworks and mutual legal aid improvements—and theoretical grounding in how international law can be localized to enhance West Africa's cybersecurity posture.

Keywords: cybersecurity, law enforcement, ECOWAS, cybercrime

1. Introduction

Cybercrime has become one of the most pervasive and rapidly evolving threats in West Africa, destabilizing economic systems, eroding public trust in digital services, and compromising national security (INTERPOL 2024a, Pakshad 2025). The region has witnessed a surge in online fraud, identity theft, ransomware attacks, and financial scams, often orchestrated by transnational criminal organizations that operate with impunity across borders lacking effective enforcement (GIABA, 2022). Despite increasing connectivity and digital adoption, many West African countries struggle to implement effective countermeasures due to weak cybersecurity laws, inadequate forensic capabilities, and the absence of robust regional cooperation frameworks (Adewopo, 2024).

Ghana has made significant strides in establishing a comprehensive legal framework for cybersecurity over the past decade. The Electronic Transactions Act (2008) introduced penalties for criminal computer misuse and cyber offenses (National Information Technology Agency, 2008), while the Data Protection Act (2012) created a commission to oversee responsible data management (National Information Technology Agency, 2012). More recently, the Cybersecurity Act (2020) established the Cyber Security Authority (CSA) and mandated international cooperation in combating cybercrime (Parliament of Ghana, 2020). These laws are reinforced by Ghana's National Cybersecurity Policy and Strategy, which prioritizes resilience, public-private partnerships, critical infrastructure protection, and public education. Legislative amendments to the Electronic Communications Act have also targeted SIM box fraud and the use of preregistered SIM cards, measures aimed at curbing anonymous communications exploited by cybercriminals. Ghana's participation in global programs such

as the GLACY+ program of the Council of Europe has further strengthened its capacity, training hundreds of police officers, prosecutors, and judges on the handling of electronic evidence (Council of Europe, 2023).

While global frameworks such as the Budapest Convention have shaped transnational cybercrime strategies, their adoption in West Africa remains limited. Regional instruments like the ECOWAS Directive on Cybercrime (2011) and the African Union's Malabo Convention 2014 seek to harmonize legal responses, but implementation has lagged—by 2024, only four of twelve ECOWAS member states had ratified the Malabo Convention (African Union, 2024). Ghana stands out as an exception, having passed both the Data Protection Act and the Cybersecurity Act, while also ratifying the Budapest and Malabo conventions (Cyber Security Authority, 2023a). Nonetheless, the absence of parallel enforcement in neighboring states creates regional asymmetries that undermine collective security (Orji, 2019).

Ultimately, Ghana's cybersecurity resilience is constrained by the region's weakest link. Given the borderless nature of cybercrime, effective defense requires seamless legal, technical, and operational collaboration across states—an objective hindered by inconsistent legislation, resource disparities, and limited technical infrastructure (UNODC, n.d.). As West African nations grapple with the dual challenge of building national resilience while fostering coordinated regional action, this study examines the steps necessary to bridge these gaps.

2. Problem Statement

Cybercrime in West Africa continues to escalate in both scale and sophistication, yet many nation-states in the region lack the legislative, institutional, and operational capacity to address transnational threats effectively (GIABA 2022; Orji 2019). National cybercrime laws remain fragmented, and the limited ratification of regional legal instruments has produced jurisdictional inconsistencies that obstruct timely cross-border investigations and prosecutions (Cyber Security Authority, 2023b). These legal gaps are compounded by systemic weaknesses in enforcement, including under-resourced cybercrime units, insufficient digital forensic capabilities, and the absence of specialized judicial training (Adewopo, Mensah & Okafor, 2024). Ghana has made notable progress in strengthening its cybersecurity framework—most prominently through the establishment of the Cyber Security Authority (CSA) and active engagement with international treaties. However, without corresponding advancements in neighboring countries, Ghana remains exposed to transnational cyber threats originating from jurisdictions with weaker legal protections or inadequate enforcement (Cyber Security Authority, 2023b). This asymmetry in regional preparedness undermines collective cyber resilience and poses a shared security challenge. The absence of a dedicated regional enforcement body or follow-up mechanism in West Africa further limits the harmonization of cyber laws. Cybercrime responses are largely siloed within individual nations, which impedes the pursuit of perpetrators operating across multiple jurisdictions (UNODC, n.d.). Even within Ghana, prior to the creation of the CSA, cyber initiatives were often fragmented across agencies, weakening enforcement outcomes (Cyber Security Authority, 2023a). Across the region, the shortage of trained investigators, certified digital forensic specialists, and judicial officers with cybercrime expertise persists, with only a few states maintaining specialized cybercrime units (UNODC, n.d.). Consequently, many cybercrime cases remain unresolved, and cross-border evidence sharing is inconsistent due to the lack of clearly defined mutual legal assistance protocols tailored to the digital domain.

3. Significance

Cybercrime poses a growing threat to national security, economic stability, and democratic governance in West Africa. While Ghana has made commendable progress in developing its cybersecurity framework, its efforts are undermined by the fragmented legal and institutional landscape across the region. This study is significant because it addresses the urgent need for

stronger regional collaboration, legal harmonization, and enforcement mechanisms to confront cyber threats that easily exceed national borders. Failure to address the issues outlined in this study will continue to allow cybercriminals to exploit legal loopholes and jurisdictional weaknesses, thereby increasing financial losses, weakening public trust in digital systems, and hindering regional integration. The lack of uniform enforcement standards, mutual legal assistance, and digital forensic capacity in neighboring countries compromises Ghana's national security and regional stability. By proposing practical solutions and highlighting Ghana's role as a potential leader in regional cybersecurity reform, this study contributes to ongoing policy debates and supports the development of a safer digital environment in West Africa.

4. Methodology

This study is conceptual, focusing on the importance of strengthening cybersecurity governance within the West African region. It employs a qualitative research design grounded in doctrinal legal analysis and comparative policy evaluation. The doctrinal approach involves a systematic examination of legislative texts, judicial interpretations, and statutory frameworks related to cybersecurity and cybercrime enforcement across selected West African countries, with Ghana serving as a case study. To enhance contextual understanding, the research includes a comparative policy analysis of cybersecurity strategies and enforcement mechanisms among ECOWAS member states by reviewing official government publications, regional directives, and reports from international organizations such as INTERPOL and ECOWAS. Case studies detailing significant cybercrime incidents in the region are also used to complement the analysis and illustrate the severity of the issue.

5. Literature Review

5.1. Legal Theories & Frameworks

In order to promote effective cybersecurity governance, enforcement in the West African region must be grounded in foundational legal doctrines that emphasize the need of balancing collective responsibility with state sovereignty. In one case with the rule of law, the theory states the importance of consistent, transparent, and predictable legal responses to cyber threats. This principle is supported by the United Nations Office on Drugs & Crimes (UNODC)'s emphasis on ensuring a synergy between cybercrime laws with international human rights standards, ensuring that the measures placed for enforcement are respectful of basic rights while upholding the rule of law (UNODC, n.d.).

A theory applied in global governance debates pertaining to internet use also plays a key role in shaping cybersecurity and is referred to as Multistakeholder governance. It advocates that governments, private sector actors, civil society, and academia all share a joint responsibility in shaping cybersecurity norms, frameworks, and mechanisms of enforcement (Kurbalija, 2016). This is evident in Ghana's collaborative approach through the Cyber Security Authority, which includes stakeholder engagement from law enforcement, telecommunication companies, and financial institutions in shaping the respective laws of each related sector (Cyber Security Authority, 2023b).

Another relevant theory that acknowledges that cyber norms in Africa often operate within a vacuum influenced by formal legislation, customary norms, and various governance structures that can pose both a challenge and opportunity for designing cyber laws is known as Legal pluralism (Bouke et al., 2023). With the ability to resonate with empirical expectations, countries in the region can work to construct frameworks that remain true to local contexts that still allow for exchange of information that is compliant with international standards, in spite of differences in various customs.

Overall, these theoretical foundations help illustrate why regional differences in legal frameworks persist and highlight the importance of legal cooperation strategies across

ECOWAS states. By contextualizing the region's development in cybersecurity through these lenses, the friction between sovereignties, legal consistencies, and global cooperation that underpins current enforcement gaps is better understood.

5.2. Regional & National Cybersecurity Frameworks

West African states have gradually developed a series of cybersecurity strategies and legal frameworks, both at regional and national levels, to combat cybercrime. At the regional level, the Economic Community of West African States (ECOWAS) adopted Directive C/DIR.1/08/11 in 2011, with the aim of harmonizing member states' substantive criminal laws and procedures for addressing cyber offenses (ECOWAS, 2021). This directive categorized cybercrimes into offenses related to Information and Communication Technologies (ICTs) and traditional crimes committed via ICTs, while also recommending sanctions and procedures to guide national legislation. On the continental level, the African Union's Malabo Convention—officially known as the AU Convention on Cyber Security and Personal Data Protection—was adopted in 2014 as a framework for unifying cyber laws across Africa (African Union, 2014). The Malabo Convention aims to create a compatible legal regime addressing cybercrime, data protection, and electronic transactions to close regulatory gaps and foster cross-border cooperation (CIPIT, 2024). It entered into force in June 2023, after reaching the required 15 ratifications, with Ghana among the countries that have both ratified and aligned its national laws accordingly. However, progress has been uneven, as several states in the region have yet to adopt or implement the convention's provisions, highlighting disparities in regional legal harmonization. At the national level, Ghana stands out for its comprehensive cybersecurity framework in recent years. Since 2020, Ghana has updated its National Cybersecurity Policy and Strategy and enacted the Cybersecurity Act (Act 1038), which established the Cyber Security Authority and strengthened the legal foundation for combating cybercrime. These measures ranked Ghana 3rd in cybersecurity across the continent in the ITU's Global Cybersecurity Index for 2020 (Cyber Security Authority, 2023b). Earlier legislation, such as the Electronic Transactions Act (2008) and the Data Protection Act (2012), further reinforced Ghana's position as a regional leader. Ghana's commitment is also evident in its ratification of the Malabo Convention, the Budapest Convention on Cybercrime, and its support for ECOWAS initiatives such as the ECOWAS Regional Cybersecurity and Cybercrime Strategy (2021). Other West African nations have enacted national cyber laws with varying scopes. For example, Nigeria passed the Cybercrime Act in 2015 to criminalize hacking, fraud, and related offenses, and revised its National Cybersecurity Policy in 2021 to align with the Act. Similarly, Côte d'Ivoire, Senegal, and Benin have introduced cybercrime laws or updated their penal codes in line with ECOWAS directives. Despite this progress, some smaller states in the region still lack dedicated cybercrime legislation or face delays in implementation (CIPIT, 2024). The unevenness in the region means cybercriminals may exploit jurisdictions with weaker laws or enforcement, which further highlights the importance of regional frameworks. Building on this, studies from high-risk urban centers show that adaptive security frameworks combining real-time threat intelligence with infrastructure-specific safeguards can reduce cyber threat. Applying similar context-aware approaches to West Africa could also help address the operational asymmetries currently constraining regional cybersecurity threat (Pakshad, 2025 LLM).

5.2.1. Legal Implications & Enforcement Gaps

The emergence of multiple frameworks highlights a stride towards legal harmonization, but also reveals gaps between policy and practice. The ECOWAS Cybercrime Directive of 2011 is now over a decade old and has not been uniformly implemented by all member states. It is also in the process of being updated to address new challenges such as privacy and human rights concerns in cyber policing. The AU's Malabo Convention, likewise, has energized countries to pass new laws, such as Ghana's data protection authority and cyber laws post-2014 (Kaaniru, 2023). A significant gap still lies in cross-jurisdictional enforcement. Many national laws in West Africa

still lack clear provisions on handling extraterritorial affairs or streamlining extradition for cyber offenses, which creates obstacles when cybercriminals operate across borders. For instance, a fraud perpetrator in one West African country targeting victims in another may fall into the legal gray area if the two jurisdictions lack mutual assistance agreements due to misalignments in their laws. These gaps limit the efficacy of enforcement, as criminals exploit these lenient environments. Harmonization is a key to closing these gaps, through the adoption of common definitions of cybercrime and compatible procedures to address them. West African states would be able to deter "safe havens" for cybercriminals and enable closer cooperation in investigations, thereby strengthening collective security of the digital domain in the region.

5.3. Case Studies & Cultural Phenomena

5.3.1. 419 Scam

The term "419 scam" comes from Section 419 of the Nigerian Criminal Code, which deals with advance-fee fraud. In this type scam, victims are tricked into sending money upfront with the hope of receiving a larger sum later. Over the years, this form of cybercrime has become a well-known method of online fraud in West Africa and beyond. It often includes fake job offers, investment schemes, romantic relationships, or claims of large inheritances. Victims are contacted through email, social media, or messaging apps, and are persuaded to send money for supposed legal fees, taxes, or travel expenses. This type of scam has grown into an organized activity, especially in countries like Nigeria and Ghana. In some urban communities, young people—mainly unemployed or underemployed—are drawn into what is called the "Yahoo Yahoo" lifestyle. This term refers to internet fraud networks where individuals learn how to scam through online forums or peers. Some view it as a way to escape poverty or gain quick wealth, while others justify it as a response to global inequality or even see it as a game of who can outsmart whom (Tade & Aliyu, 2011).

Research shows that some youth involved in these scams do not see themselves as criminals. Instead, they often frame their actions as survival tactics in a system where opportunities are limited (Udupa & Pohjonen, 2019). Social media has also played a role in glorifying this behavior. The flashy lifestyle of scammers—cars, clothes, and parties—is celebrated online, further encouraging the practice among young people who feel excluded from formal job markets. However, 419 scams are not just a youth issue—they are a serious cybercrime problem with real victims around the world. According to INTERPOL (2024), many of these scams are now part of larger criminal networks that move across countries. These groups use tools like fake websites, untraceable phone numbers, and cryptocurrency to avoid being caught. Most West African countries lack the laws, resources, and trained officers to investigate these crimes effectively. Many police units do not have digital forensic labs or staff who understand cyber laws, making it difficult to trace suspects or collect electronic evidence (Adewopo, Mensah & Okafor, 2024). In addition, the fact that laws differ from one country to another in the region creates loopholes that scammers exploit. For example, a scammer operating in one country with weak enforcement can target victims in another country with strong laws, knowing there is little chance of arrest. Even when suspects are identified, poor cooperation between countries delays or prevents legal action.

This case highlights the importance of having consistent cybercrime laws across ECOWAS member states. Regional enforcement efforts must go beyond passing laws—they should include setting up shared investigation teams, fast channels for sharing digital evidence, and training programs for judges and police in handling cybercrime cases. Public education is also important. Awareness campaigns can help people understand how to recognize scams and report them early, reducing the number of victims. Ultimately, the fight against 419 scams must address both the crime and the conditions that allow it to thrive. That means giving young people better economic options, strengthening law enforcement, and

improving cooperation between countries. If West African nations can take these steps together, it would not only reduce cyber fraud but also build greater trust in digital spaces across the region.

5.3.2. Sakawa & Yahoo Boys

The terms Sakawa boys in Ghana and Yahoo boys in Nigeria refer to youth involved in internet fraud, especially advance-fee scams and online impersonation schemes. While both terms describe similar activities, Sakawa in Ghana has a unique cultural and spiritual dimension that combines cyber fraud with traditional rituals or occult practices, believed to "bless" or ensure the success of the scam (Osumanu, 2021). Yahoo boys, on the other hand, are more closely associated with urban Nigerian internet fraud culture, often carried out through email scams and social media deception (Tade & Aliyu, 2011). These groups target individuals globally by creating fake online identities and relationships—often pretending to be wealthy business people, government officials, or love interests. Once trust is built, victims are tricked into sending money for false reasons like travel, fees, or business deals.

An example that gained public attention was the arrest of Nigerian Instagram celebrity Ramon Abbas, popularly known as "Hushpuppi", in 2020. He was involved in a global fraud network that stole millions of dollars from individuals and companies across different countries. His case showed how online scammers can operate international networks while flaunting their wealth on social media (FBI, 2020). Hushpuppi became a role model for many young fraudsters, highlighting the growing connection between internet fraud, fame, and digital lifestyle.

In Ghana, Sakawa is often portrayed in films and music, sometimes glamorizing the fast money lifestyle. This has led to a cultural shift, where some youth begin to see internet fraud as a normal or even respectable way of making a living. The rituals associated with Sakawa involve spiritual consultations, sacrifices, and charms that scammers believe can make victims easily manipulated. Though not all fraudsters follow this path, the belief in spiritual aid adds a unique cultural twist that blends technology with traditional beliefs (Osumanu, 2021; Quarshie, 2019).

These practices thrive in environments where poverty, joblessness, and lack of digital literacy are common. Many young people are drawn into this lifestyle because they feel left out of the formal economy. Social media platforms amplify this by displaying the flashy lifestyles of successful fraudsters, making it seem like an attractive alternative to conventional work (Udupa & Pohjonen, 2019). From a legal perspective, both Sakawa and Yahoo-related cybercrime are difficult to prosecute because of limited cross-border cooperation, outdated laws, and the use of anonymizing tools online. Ghana and Nigeria have introduced cybercrime laws and digital forensic units, but enforcement is still weak in many areas due to lack of training and resources. Moreover, the blending of culture and crime makes enforcement more complicated, since some communities may tolerate or even support these practices as survival strategies.

Tackling this issue requires a multi-layered approach: updating cybercrime laws, increasing regional cooperation, and running public education campaigns that target the root causes of fraud culture. Ghana's Cybersecurity Authority, for example, has taken steps to regulate digital space and collaborate with religious and traditional leaders to demystify Sakawa practices (Cyber Security Authority, 2023a). ECOWAS can also play a stronger role in promoting coordinated investigations and youth-focused interventions across borders.

5.3.3. Abuja Airport Scam

The Abuja Airport Scam is one of the biggest fraud cases in Nigeria's history, and it shows how scammers can trick people using fake documents, official names, and international banks. Even

though this scam happened in the 1990s, it still matters today because many modern online scams use the same tricks.

The scam was led by Emmanuel Nwude, a former Nigerian banker. He pretended to be the Governor of the Central Bank of Nigeria and convinced a Brazilian bank official, Nelson Sakaguchi, to invest in a fake project to build a new airport in Abuja. Nwude promised that Sakaguchi would get a big profit and a $10 million commission. Over three years, Sakaguchi sent over $242 million to Nwude's fake accounts, believing the deal was real (U.S. Department of Justice, 2005). Nwude used fake letters, company names, and bank accounts in places like the Cayman Islands and Switzerland. He moved the stolen money through different countries to hide it. These steps are similar to how cybercriminals today use fake online identities and anonymous accounts to hide their crimes. This case shows that even without the internet, people were already using smart tricks to commit fraud across borders (Adewopo, Mensah & Okafor, 2024).

The fraud was discovered in 1997 when Banco Santander tried to buy Banco Noroeste, the Brazilian bank that lost the money. The suspicious transactions were reported, and the case was investigated in Brazil, the U.S., the UK, and Nigeria. Sakaguchi was arrested in the U.S., and Nwude was later tried and sentenced in Nigeria. He was given 25 years in prison and ordered to return a large amount of the stolen money (EFCC, 2006).

This scam is important because it showed the need for strong anti-money laundering laws, better banking checks, and international cooperation. Even though the internet wasn't used, the case helped shape how countries now fight online fraud. Today's 419 email scams follow a similar idea: offer something fake, gain trust, and take people's money.

5.3.4. Romance Scams

Romance scams are a growing form of cyber-enabled fraud in Ghana, where individuals create fake online identities to deceive victims—often foreign nationals—into sending money under the guise of a romantic relationship. These scams usually target emotionally vulnerable people, such as the elderly or those seeking companionship online, using platforms like Facebook, Instagram, and WhatsApp to build false trust and manipulate victims emotionally and financially (Tade & Aliyu, 2011). Scammers often fabricate compelling backstories, including military deployment, inheritance disputes, or medical emergencies, to extract funds in small or large amounts over time. Victims may send thousands of dollars believing they are helping a romantic partner in distress. These scams are difficult to detect early because they do not start as financial solicitations but develop gradually through emotional manipulation.

A recent high-profile case that illustrates the scale and sophistication of such scams is that of Mona Faiz Montrage, popularly known as Hajia4Reall, a Ghanaian social media influencer. According to the U.S. Department of Justice (2024), between 2013 and 2019, Montrage was involved in a transnational criminal scheme that targeted elderly Americans through online romance scams (MyJoyOnline, 2024). Posing as various fictitious identities, she and her co-conspirators deceived victims into sending money under false pretenses—such as assistance for shipping gold or resolving fabricated legal problems. Montrage personally received over $2 million from multiple victims and even sent one victim a fake tribal marriage certificate to secure continued payments (U.S. Department of Justice, 2024). She was arrested in the UK in 2022, extradited to the United States in 2023, and pleaded guilty in early 2024 to conspiracy to receive stolen money. In mid-2024, she was sentenced to 12 months in prison, three years of supervised release, and ordered to forfeit over $2 million (New York Post, 2024). This case highlights how romance fraud can involve public figures, operate across borders, and rely on emotional and cultural manipulation to succeed.

The Hajia4Reall case underscores the urgent need for updated cybercrime laws in Ghana that specifically address romance scams and similar online offenses. While the Ghanaian Cybersecurity Act (2020) has made progress, enforcement challenges remain due to

resource constraints and the difficulty of tracking digital communications. The case also illustrates the importance of international cooperation in investigating and prosecuting cybercrime, as well as the need for public education campaigns to prevent individuals—especially vulnerable groups—from falling prey to these schemes.

5.4. Current Initiatives

In October 2024, INTERPOL announced the arrest of eight suspected cybercriminals behind an elaborate phishing operation based out of Abidjan, Côte d'Ivoire, with logistical support coming in from Nigeria (INTERPOL, 2024a). They were found to have been responsible for more than 260 victim reports submitted in Switzerland between August 2023 and April 2024, with confirmed losses of more than USD 1.4 million (The Record, 2024). Digital forensics on-site prompted the officers to confiscate storage devices, laptops and phones, and the alleged ringleader admitted making over USD 1.9 million personally through the conspiracy (INTERPOL, 2024a).

Operation Contender 2.0 is among the African Joint Operations against Cybercrime (AFJOC) a multi-year programme sponsored by the UK Foreign, Commonwealth & Development Office on a GBP 2.68 million budget for 2024-25 (INTERPOL, 2024b). Swiss federal police supplied initial indicators of compromise; INTERPOL's cyber-intelligence unit merged those leads with commercial data from Group-IB and Trend Micro, and forwarded them on to Ivorian and Nigerian counterparts via AFJOC's secure Cyber Fusion Platform (INTERPOL, 2024b).

In addition to the arrests, Contender 2.0 also created broader strategic value. First, standardized evidence standards—both nations had recently revised their criminal-procedure codes to accept digital evidence—brought mutual-legal-assistance timelines under ten days, compared to a 90-day regional average in previous phishing cases. Second, logs seized at the Abidjan command node connected the syndicate to a minimum of three business-email-compromise clusters based in Lagos, demonstrating how one jurisdictional vulnerability can multiply regional exposure (INTERPOL, 2024a).

Building on these findings, advanced analytical methods such as machine learning and large language models provide the capability to process telemetry at scale, correlate cross-border digital evidence, and identify cyber-attack patterns that may otherwise remain undetected (Pakshad2025LLM). Large Language Models can strengthen regional cyber defense efforts and accelerate the timeliness of coordinated response operations by leveraging automated vulnerability detection and predictive risk assessment (Pakshad2023Predictor, Azizi2025CVSS).

The removal emphasizes how Ghana's call for legal harmonization in the region is urgent. Although Ghana has criminalized QR code-enhanced phishing for years under its 2020 Cybersecurity Act, Côte d'Ivoire had to prosecute under a 2013 decree calling such frauds generic "fraud," complicating extradition\citep{orji2019ecowas}. By contrast, Nigeria's 2024 Cybercrime (Amendment) Bill follows a Budapest-Convention-type approach so that cross-border warrants seamlessly pass. Contender 2.0 thus offers ECOWAS a model: shared typologies, border-interoperable evidence-handling rules, and an ongoing operating desk can turn isolated national laws into a cohesive regional shield.

6. Results

The findings of this study demonstrate a vast divide in Ghana’s cybersecurity advancement and the broader regional context. Standing out with its proactive legislative frameworks, demonstrated by the Cybersecurity Act or its ratification of both the Malabo and Budapest Conventions, Ghana has institutionalized cyber governance through the development of the Cyber Security Authority and participating in cross-border initiatives such as the GLACY+ program. The broader West African region presents a fragmented cybersecurity landscape. Many countries lack dedicated cybercrime laws or have yet to ratify key international conventions in the continental or regional

aspect, creating enforcement gaps and jurisdictional blind spots that cybercriminals actively exploit. The prevalence of scams such as the 419 fraud, the evolution of subcultures such as the Sakawa and Yahoo Boys, and other high-profile incidents all point to how transnational actors leverage weak regulations and enforcement zones to conduct coordinated operations. In addition, most countries in the region lack specialized resources capable of addressing these cybercrimes, as discussed in Adewopo et al.'s (2024) study. Even in Ghana, where its capacity is stronger, systemic challenges such as inconsistent coordination amongst various agencies and public awareness deficits persist.

Countries in the region operate under hybrid legal systems combining various avenues of the law, ranging from statutory to religious aspects. While this diversity, defined through legal pluralism, can enrich approaches to governance, it leads to inconsistent interpretations of cyber-related offenses and complicates efforts to implement regionally consistent legal norms (Bouke et al., 2023). A study conducted by Dawson and Walker (2022) documented that 62% of the 48 councils surveyed across five ECOWAS states had no budget allocated for cybersecurity, and fewer than 5% had an incident-response plan. Unpatched Windows 7 systems and default passwords in local tax offices became easy targets for regional crime syndicates (Dawson & Walker, 2022). This gap was further illustrated by Kaspersky's (2024) findings that over 30% of ICS systems tied to subnational utilities in Nigeria and Ghana had been compromised by malware during H2 2023. Yet as of May 2025, only four ECOWAS member states Ghana, Nigeria, Cabo Verde, and Benin, report that their Computer Security Incident Response Teams (CSIRTs) offer continuous municipal-level support.

Nevertheless, there are promising signs of progress. Ghana mandates that each district assembly appoint a Digital Service Security Focal Point, enroll in CSIRT training, and report cyber hygiene metrics quarterly (Cyber Security Authority, 2023b). WARDIP Component 3 supports similar reforms by funding baseline security audits across six ECOWAS countries through the World Bank (2024). The ECOWAS 2021 Cybersecurity Strategy acknowledges that regional resiliency is dependent on subnational compliance with baseline safeguards, yet policy enforcement remains uneven. In short, these findings suggest that West Africa's cybersecurity challenges stem from legal fragmentation, limited institutional readiness, and inconsistent support at the municipal level. Ghana's example shows what is possible when legal and operational reforms are coordinated across the various levels of government.

7. Recommendations & Solutions

To address immediate concerns of jurisdictional inconsistencies, ECOWAS member states should prioritize fully ratifying and implementing the directives designated within the Malabo Convention and ECOWAS Directive C/DIR 1/08/11. These legal instruments should reflect mandatory national plans of action, standardized cybercrime classifications, and explicit timelines for compliance. Overall, a dedicated regional task force under ECOWAS should be initialized to oversee progress, resolve challenges in conflicting legal statutes, and offer technical guidance to unify cybercrime legislation amongst member states.

National cybersecurity agencies must mandate subnational authorities to require minimum control measures for public service systems. Ghana's Cyber Security Authority has already championed this with quarterly reporting by district assemblies, a model that can be scaled across ECOWAS (CSA, 2023). Measures such as mandatory TLS encryption, quarterly software patch cycles, and enforceable password policies should be incorporated additionally to strengthen regional directives (Dawson & Walker, 2022). Doing this creates a standard across the region to ensure necessary controls for public service systems are implemented. Various development institutions are increasingly tying aid disbursements to cybersecurity benchmarks to incentivize improving cyber resilience. One such initiative stems from the African Development Bank (AfDB), through its African Digital Financial Inclusion Facility (ADFI), which created a cybersecurity capacity building grant that is contingent on an

acceptable audit conducted on a project's cybersecurity measures (African Development Bank, 2021). Through this practice, funds would only be released after a recipient underwent the audit and addressed findings, tying cyber hygiene compliance into a project's milestones. By linking financial support to these audits and cyber maturity assessments, institutions ensure that recipient countries build sustainable cyber defenses as a part of development initiatives undertaken across the country, and ensure concrete progress in strategies are followed through. West African policymakers can further this through the implementation of a legal harmonization task force to drive implementation of continental conventions. As stated earlier, a legal framework such as Multistakeholder governance is vital in achieving governance through incorporating various voices within the federal and private sector arenas, as well as academia, to create resilient cyber frameworks (Kurbalija, 2016). According to the Directive on Fighting Cyber Crime in ECOWAS, the idea of Legal harmonization is needed to ensure all ECOWAS states adopt robust and aligned cybercrime, data protection, and cybersecurity laws (ECOWAS, 2011). Strides to achieve this in other areas, such as the African Union's Malabo Convention, only entered into force in 2023, and still lack broad ratification as of 2024 (African Union, 2024). A dedicated ECOWAS task force would accelerate the implementation of these directives by coordinating member states' legislative updates, sharing best practices to achieve these in the face of competing interests, and tracking progress to achieve compliance with international and regional norms. These cybercrime units would then be able to form collaborative efforts through joint task forces such as those illustrated in INTERPOL's Operation Contender 2.0, which proved that intergovernmental coordination amongst different states yields measurable impacts (INTERPOL, 2024a). Other international collaborations, such as the Council of Europe's GLACY+ program and its results, also show the benefits of expanding such initiatives to offer sustained technical assistance and forensic training within the region to achieve these standards (COE, 2023).

8. Conclusions

Cybercrime remains an urgent and complex security threat within West Africa. Despite the leadership in cybersecurity governance seen in states such as Ghana, the broader region continues to struggle with the lack of standardization in legal doctrines, limited enforcement capacities, and inconsistency with cross-border cooperation. This study has illustrated how Ghana's robust legal and institutional architectures led by initiatives such as the Cybersecurity Act of 2020, other Cyber Security Authority led initiatives, and its participation in programs such as GLACY+, can serve as a model for broader regional replication. However, this effectiveness does expose a foundational reality that cybersecurity should be pursued not only nationally but regionally. The persistent threat and proliferation of cyber powered frauds highlight the need for region-wide cyber resilience led by uniformity in cyber laws, capable institutions, and continuous collaboration.

Findings also show that empowering governments at a subnational level, incorporating cybersecurity into development aid conditionality, and expanding coordinated operations on a regional and international level offer viable paths forward. The introduction of legal harmonization frameworks and binding cyber hygiene benchmarks represent immediate steps that regional stakeholders can look into. A secure digital future for West Africa depends on more than just legislative reforms. It requires political enforcement, international partnerships, and a shared vision of cyber stability. As ECOWAS revisits its regional cybersecurity strategy in the coming years, the lessons from Ghana and other regional leaders should guide its roadmap towards equitable and enforceable cybersecurity governance across the region.

9. Recommendations for Future Research

To further the discussion and implementation of effective cybersecurity governance across West Africa, there is a need for continued academic and policy research to strengthen the dialogue at hand. Future studies should track and assess the rate of implementation and enforcement of ECOWAS and African Union directives aimed at cyber governance, evaluating their measurable impact on reducing cybercrime incidence and enabling timely cross-border prosecutions. Researchers should also explore the fiscal and policy outcomes of making cybersecurity compliance a prerequisite for development assistance. By examining how cybersecurity benchmarks influence aid disbursement in infrastructure and digital transformation projects, studies can highlight the broader implications of embedding cyber resilience into the core of international development frameworks. Another critical research avenue is investigating the sociocultural dynamics of cybercrime proliferation. Understanding the motivations, perceptions, and local attitudes surrounding phenomena such as SIM card fraud, internet romance scams, and hybrid digital rituals can enable the design of targeted public awareness and education campaigns tailored to regional contexts. Furthermore, future works should examine how the private sector and non-state stakeholders can cooperate with governments to enhance data sharing, intelligence coordination, and cybercrime mitigation efforts. Finally, a more in-depth analysis is needed into the cyber readiness of municipal and subnational governments. Evaluating their access to technical expertise, incident response trainings, and digital hygiene protocols can help build an inclusive, decentralized regional security framework that aligns with the integration goals of both ECOWAS and the African Union.

Acknowledgements

We gratefully acknowledge the Center for Cyber Security and Forensics Education (C²SAFE) for providing access to its core facilities, including the Ed Kaplan Family Institute for Innovation and Tech Entrepreneurship, during the course of this research.

References

Adewopo, A., Mensah, K., & Okafor, T. (2024). Regional cybersecurity cooperation in West Africa: Legal gaps and enforcement challenges. *ECOWAS Legal Studies Review*, *11*(1), 23–45.

African Development Bank. (2021). *Multinational Africa Cybersecurity Resource Center (ACRC) for Financial Inclusion: Appraisal report*. https://www.afdb.org/sites/default/files/documents/projects-and-operations/multinational_-_africa_cybersecurity_resource_center_acrc_for_financial_inclusion_-_appraisal_report.pdf

African Union. (2024, July 8). *List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf

Azizi, S., Pakshad, P., Shameli-Sendi, A., & Faraji Daneshgar, F. (2025). Vulnerability scoring metric of CVSS needs to be adjusted per each product: Our analysis on Linux and Apache. *Information Security Journal: A Global Perspective*, 1–26.

Bci. (n.d.). *Digital transformation, development and resilience in West Africa*. Business Continuity Institute. https://www.thebci.org/news/digital-transformation-development-and-resilience-in-west-africa.html

Bouke, M. A., Abdullah, A., Alshatebi, S. H., El Atigh, H., & Cengiz, K. (2023). *African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions*. https://arxiv.org/abs/2307.01966

Kaaniru, J. (2023) . *The African Union Convention on Cyber Security and Personal Data Protection: Key insights*. Centre for Intellectual Property and Information Technology Law (CIPIT).https://cipit.strathmore.edu/the-african-union-convention-on-cyber-security-and-personal-data-protection-key-insights/

Kaspersky. (2024, December 13). *Threat landscape for industrial automation systems – Regions, Q2 2024*. Kaspersky ICS CERT. https://ics-cert.kaspersky.com/publications/reports/2024/11/21/threat-landscape-for-industrial-automation-systems-regions-q2-2024/

Kurbalija, J. (2016). An Introduction to Internet Governance (7th ed.)**.** *DiploFoundation.* https://www.diplomacy.edu/resource/an-introduction-to-internet-governance/

Council of Europe. (2023). *GLACY+ activities in Ghana*. https://www.coe.int/en/web/cybercrime/ghana

Cyber Security Authority. (2023a). *Ghana signs Council of Europe Second Additional Protocol to the Convention on Cybercrime*. https://www.csa.gov.gh/ghana-signs-council-of-europe-second-additional-protocol-to-the%20-convention-on-cybercrime

Cyber Security Authority. (2023b). *Annual Cybercrime and Cybersecurity Report*. Government of Ghana. https://www.csa.gov.gh

Dawson, M., & Walker, D. (2022). Argument for improved security in local governments within the Economic Community of West African States. In *Cybersecurity Measures for E-Government Frameworks* (pp. 96–106). IGI Global Scientific Publishing.

ECOWAS. (2021). *ECOWAS Regional Cybersecurity and Cybercrime Strategy*. https://ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf

EFCC. (2006). *High-profile convictions*. Economic and Financial Crimes Commission, Nigeria.

FBI. (2020). *Nigerian national arrested for fraud and money laundering*. United States Department of Justice.

GIABA. (2022). *Threat assessment on cyber-enabled financial crimes in West Africa*. Inter-Governmental Action Group Against Money Laundering.

INTERPOL. (2024a). *Cybercrime threat assessment for West Africa*. INTERPOL Cybercrime Directorate.

INTERPOL. (2024b). *Arrests in international operation targeting cybercriminals in West Africa*. https://www.interpol.int/en/News-and-Events/News/2024/Arrests-in-international-operation-targeting-cybercriminals-in-West-Africa

MyJoyOnline. (2024). *Hajia 4Reall sentenced to over a year in U.S. prison for romance scam*. MyJoyOnline. https://www.myjoyonline.com/hajia-4reall-sentenced-to-over-a-year-in-u-s-prison-for-romance-scam/

National Communications Authority. (2020). *Amendments to the Electronic Communications Act on SIM box fraud and pre-registered SIMs*. Ghana Government.

New York Post. (2024, March 9). Influencer Mona Montrage pleads guilty to conspiracy charge in multimillion-dollar catfishing scam. https://nypost.com/2024/03/09/social-media-influencer-fesses-up-to-lonely-hearts-scam/

Orji, U. J. (2019). *ECOWAS legal framework for cybersecurity and cybercrime: A review of regional responses and obligations for member states*. African Journal of International and Comparative Law, 27(1), 101–121. https://doi.org/10.3366/ajicl.2019.0260

Osumanu, I. K. (2021). Rituals and cybercrime in Ghana: Understanding the practice of Sakawa. *Journal of African Cultural Studies*, *33*(1), 56–72.

Pakshad, P. (2025). *An in-depth analysis of a cyber attack: Case study and security insights.* In *Integrating artificial intelligence in cybersecurity and forensic practices* (pp. 379–400). IGI Global Scientific Publishing. https://www.igi-global.com/book/integrating-artificial-intelligence-cybersecurity-forensic/360022

Pakshad, P., & Aqanasiri, S. (2025). Are textual prompts in large language models sufficient for vulnerability detection? In *Navigating law and policy in STM enterprises: Ethical governance, regulation, and innovation strategy* (pp. 121–138). IGI Global Scientific Publishing.

Pakshad, P., Shameli-Sendi, A., & Khalaji Emamzadeh Abbasi, B. (2023). A security vulnerability predictor based on source code metrics. *Journal of Computer Virology and Hacking Techniques, 19*(4), 615–633.

Quarshie, M. (2019). Sakawa: Hybrid spiritualities and the politics of occult economies in Ghana. *African Studies Review*, *62*(2), 154–176.

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860–875.

U.S. Department of Justice. (2005). *Report on international advance-fee fraud and bank fraud cases*. DOJ Archives.

U.S. Department of Justice. (2024). *Social media influencer pleads guilty in romance scam targeting elderly Americans*. https://www.justice.gov

Udupa, S., & Pohjonen, M. (2019). Digital cultures of political participation: Internet memes and misinformation in Africa. In S. Udupa & M. Pohjonen (Eds.), *Media as politics in postcolonial Africa* (pp. 121–142). Zed Books.

UNODC. (n.d.). *Using technology to combat crime and promote the rule of law*. United Nations Office on Drugs and Crime. https://www.unodc.org/conig/en/stories/using-technology-to-combat-crime-and-promote-the-rule-of-law.html

World Bank. (2024). *Development Projects: Digital Transformation for Africa/ Western Africa Regional Digital Integration Program SOP1 - P176932*. https://projects.worldbank.org/en/projects-operations/project-detail/P176932