Current Research in Interdisciplinary Studies, 5(4):1–12, 2026. DOI: 10.58614/cris541

Current Research in Interdisciplinary Studies

Journal homepage: https://jpub.org/journal-details.php?journal-id=40

Review Article

Assessing the Effectiveness of Cybercrime Laws in Africa: A Systematic Review of Enforcement Barriers and Policy Reform Options

Sandra Frimpong [1*], Charles C. Udechukwu [2], Mariam Iyabo Adeoba [3], Thomas Kofi Mensah [4] and Doreen Mensah [5]

[1] *School of Media and Communications, Bowling Green State University, USA.*
[2] *Department of Administration of Justice, Texas Southern University, Houston Texas, USA.*
[3] *Department of Mechanical, Bioresources and Biomedical Engineering, University of South Africa, Florida, Johannesburg, South Africa.*
[4] *Cyber/Computer Forensics and Counterterrorism, Department of Computing and Information Technology, College of Southern Nevada, USA.*
[5] *Department of Computing and Information Technology, College of Southern Nevada Las Vegas, Nevada, USA.*
[*] *Corresponding author: sfrimpo@bgsu.edu*

Article Info

Keywords: *Cybercrime, Cybercrime law, Cybersecurity governance, Law enforcement, Institutional capacity, Africa, Systematic review.*

Received: *20.03.2026;*
Accepted: *08.04.2026;*
Published: *13.04.2026*

Abstract

Cybercrime has emerged as a significant threat to economic stability, governance, and security worldwide, with particularly profound implications for developing regions such as Africa. In response, many African countries have adopted cybercrime laws and policy frameworks aimed at preventing, detecting, and prosecuting cyber offences. However, the effectiveness of these legal frameworks remains unclear. This study addresses this gap by conducting a systematic literature review to assess the effectiveness of cybercrime laws in Africa, with a particular focus on enforcement challenges, institutional capacity, and policy reform. Using a systematic review approach guided by the SPIDER framework and PRISMA 2020 guidelines, relevant studies were identified from African Journals Online (AJOL) and Google Scholar. A total of 850 records were retrieved, of which 19 studies met the inclusion criteria following rigorous screening and quality appraisal. The review integrates empirical studies, legal analyses, and policy documents to provide a comprehensive synthesis of cybercrime governance across the African context. The findings reveal a persistent gap between the formal existence of cybercrime laws and their practical enforcement. Across multiple contexts, enforcement effectiveness is constrained by institutional, technological, legal, and socio-cultural barriers, including limited technical expertise, inadequate digital forensic capacity, weak inter-agency coordination, and low levels of digital literacy. The results further indicate that the proliferation of cybercrime legislation has not translated into proportional improvements in enforcement outcomes. This study contributes to the literature by advancing a capacity-centric perspective on cybercrime governance, demonstrating that the effectiveness of legal frameworks is contingent upon institutional and technological capabilities rather than legislative presence alone. The findings highlight the need for integrated policy approaches that prioritise capacity-building, technological investment, and regional cooperation, while also ensuring the protection of fundamental rights. Overall, the study provides a comprehensive and policy-relevant assessment of cybercrime law effectiveness in Africa, offering insights for researchers, policymakers, and practitioners seeking to strengthen cybercrime governance in the region.

How To Cite: S. Frimpong, C.C. Udechukwu, M.I. Adeoba, T.K. Mensah, D. Mensah. Assessing the Effectiveness of Cybercrime Laws in Africa: A Systematic Review of Enforcement Barriers and Policy Reform Options. *Current Research in Interdisciplinary Studies*, 5(4):1–12, 2026. https://doi.org/10.58614/cris541

1. Introduction

The rapid expansion of digital technologies has fundamentally transformed economic, social, and governance systems across the globe. While this transformation has generated significant opportunities for development, it has also created new avenues for criminal activity, particularly in the form of cybercrime. Cybercrime has emerged as a critical global security concern, with increasing sophistication, transnational reach, and economic impact [1]. In response, governments worldwide have adopted legal and policy frameworks aimed at preventing, detecting, and prosecuting cyber offences. However, the effectiveness of such frameworks remains uneven, particularly in developing regions.

In Africa, the growth of internet penetration, mobile technologies, and digital economies has been accompanied by a corresponding rise in cybercrime activities, including fraud, identity theft, hacking, and cyber-enabled financial crimes [2, 3]. The continent has witnessed significant efforts to develop legal and institutional responses, including the adoption of national cybercrime laws and regional frameworks such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). These developments reflect an increasing recognition of cybercrime as a major threat to economic stability, governance, and public trust.

Despite these advancements, concerns persist regarding the effectiveness of cybercrime laws in Africa. Existing literature suggests that while many countries have established formal legal frameworks, enforcement remains inconsistent and often ineffective [4, 5]. Challenges such as limited institutional capacity, inadequate technical expertise, weak inter-agency coordination, and insufficient digital forensic infrastructure continue to undermine enforcement efforts [6]. Furthermore, the transnational nature of cybercrime presents additional difficulties, as jurisdictional boundaries complicate investigation and prosecution.

Beyond institutional and technical constraints, cybercrime governance in Africa is also shaped by broader socio-political and economic factors. Low levels of digital literacy, underreporting of cybercrime incidents, and concerns about corruption and accountability further complicate enforcement [7]. In addition, tensions between cybercrime legislation and the protection of fundamental rights, such as privacy and freedom of expression, raise important questions about the balance between security and civil liberties [8, 9].

While previous studies have examined aspects of cybercrime in Africa, much of the literature has focused either on technical cybersecurity measures or on descriptive analyses of cybercrime trends. There remains a lack of comprehensive synthesis that critically evaluates the effectiveness of cybercrime laws within the broader context of enforcement capacity, institutional dynamics, and policy frameworks. In particular, limited attention has been given to the interplay between legal provisions and the practical realities of enforcement, which is essential for understanding why cybercrime persists despite the existence of legislation.

This study addresses this gap by conducting a systematic literature review of cybercrime laws and enforcement in Africa. Drawing on empirical studies, legal analyses, and policy documents, the study examines the extent to which existing legal frameworks are effective in practice, identifies key barriers to enforcement, and explores the role of institutional capacity and policy interventions. By integrating diverse sources of evidence, the study provides a comprehensive and critical assessment of cybercrime governance in the African context.

The contribution of this study is twofold. First, it advances the literature by moving beyond descriptive accounts of cybercrime legislation to a more analytical understanding of effectiveness, with particular emphasis on enforcement and institutional capacity. Second, it provides policy-relevant insights by identifying structural and systemic factors that shape cybercrime governance, thereby informing future reforms and capacity-building initiatives.

The remainder of the paper is structured as follows. Section 2 outlines the methodology employed in the systematic review. Section 3 presents the results of the analysis. Section 4 discusses the findings in relation to existing literature and theoretical perspectives. Section 5 concludes with implications for policy and future research.

Theoretical Framework

This study is grounded in institutional capacity theory and broader perspectives on governance effectiveness, which emphasize that the success of legal and regulatory frameworks depends not only on their formal design but also on the institutional environments within which they are implemented. Institutional theory posits that formal rules and policies may exist without producing substantive outcomes if implementing institutions lack the capacity, resources, or coordination required for enforcement [10, 11].

In the context of cybercrime governance, this perspective is particularly relevant due to the complex and technologically intensive nature of cybercrime. Effective enforcement requires not only legal provisions but also specialized technical expertise, digital forensic capabilities, and coordinated institutional responses. As such, cybercrime regulation can be conceptualized as a capacity-dependent governance domain, where the effectiveness of legal frameworks is contingent upon the alignment between regulatory design and institutional capability.

This study adopts this theoretical lens to examine the extent to which cybercrime laws in Africa are supported by the necessary institutional and technological conditions for effective enforcement. By doing so, it moves beyond law-centric analyses and contributes to a more nuanced understanding of cybercrime governance as an interaction between legal frameworks and capacity constraints.

2. Methodology

2.1. Research Design

This study adopts a systematic literature review (SLR) approach to examine the effectiveness of cybercrime laws, enforcement challenges, and policy responses in Africa. A systematic review provides a transparent, rigorous, and replicable method for synthesising existing evidence, which is particularly valuable in an interdisciplinary field such as cybercrime governance that spans law, criminology, information systems, and public policy [12].

To guide the review, the study is structured around five key research questions. First, it examines the nature and scope of cybercrime legal frameworks across African countries. Second, it assesses the extent to which these laws are effective in practice. Third, it investigates the major barriers to the enforcement of cybercrime laws in Africa. Fourth, it explores the role of law enforcement and judicial institutions in shaping the effectiveness of these laws. Finally, it identifies the policy and regulatory reforms required to strengthen cybercrime governance across the continent. Together, these questions provide a coherent analytical framework for examining both the formal existence of cybercrime legislation and the practical realities of its implementation.

To ensure methodological rigour, the review process is guided by the SPIDER framework (Sample, Phenomenon of Interest, Design, Evaluation, Research type), which is particularly suited to qualitative and mixed-method evidence synthesis (Cooke et al., 2012). Within this framework, the sample comprises African countries and institutions affected by cybercrime. The phenomenon of interest focuses on cybercrime laws, enforcement practices, and policy frameworks. The design includes empirical studies, such as surveys and interviews, as well as doctrinal and policy analyses. The evaluation centres on effectiveness, enforcement challenges, institutional capacity, and policy outcomes. The research type encompasses both qualitative and quantitative studies, alongside relevant grey literature.

By integrating clearly defined research questions with a structured and systematic review design, this study ensures a comprehensive and methodologically robust examination of the effectiveness of cybercrime laws in Africa.

2.2. Search Strategy

A structured and replicable search strategy was implemented using two primary databases: African Journals Online (AJOL) and Google Scholar. These databases were selected to ensure coverage of region-specific academic literature as well as broader scholarly and policy-related sources. AJOL provides access to African-focused peer-reviewed studies that are often underrepresented in global indexing databases, while Google Scholar enables retrieval of interdisciplinary and grey literature relevant to cybercrime governance.

For AJOL, a detailed Boolean search string was used to capture studies addressing legal frameworks, enforcement processes, and institutional challenges within the African context. The search string applied was:

(cybercrime law OR cybercrime legislation OR computer crime law OR cybersecurity law) AND (enforcement OR implementation OR prosecution OR investigation) AND (barriers OR challenges OR institutional capacity OR law enforcement capacity OR digital forensics) AND (Africa OR Sub-Saharan Africa)

This search strategy was designed to maximize both sensitivity and specificity by combining legal, operational, and contextual terms while restricting results to the African context. The initial AJOL search yielded 350 records. Following relevance screening based on titles, abstracts, and keywords, this number was reduced to 100 records. Full-text assessment was conducted on 41 studies, resulting in the inclusion of 9 studies that met the predefined criteria.

For Google Scholar, a broader and more flexible search strategy was employed due to differences in indexing and retrieval mechanisms. The core search string was:

“cybercrime law” OR “cybercrime legislation” OR “cybersecurity law” AND “Africa” AND (enforcement OR implementation OR prosecution OR investigation) AND (challenges OR barriers OR capacity OR digital forensics)

In addition, iterative searches were conducted using related terms such as “cybercrime policy Africa”, “cybersecurity governance Africa”, and “law enforcement cybercrime Africa” to ensure comprehensive coverage. The first 10 pages of results were systematically screened in order of relevance, in line with established practice for managing large search outputs. The initial Google Scholar search returned approximately 500 records, which were reduced to 50 following relevance screening. Full-text assessment resulted in the inclusion of 10 studies.

All database searches were conducted between January and March 2025.

2.3. Inclusion and Exclusion Criteria

Studies were included in the review if they focused on cybercrime laws, enforcement mechanisms, or policy frameworks within the African context, and addressed issues related to effectiveness, institutional capacity, or enforcement challenges. Eligible studies comprised empirical research, legal analyses, and policy-oriented publications in order to capture the multidisciplinary nature of cybercrime governance.

Studies were excluded if they focused solely on technical cybersecurity solutions without relevance to legal or policy dimensions, were not situated within the African context, or lacked sufficient relevance to the research questions guiding this review. No restriction was placed on publication year in order to capture both foundational and contemporary developments in cybercrime law.

2.4. Study Selection Process

The study selection process followed the PRISMA 2020 guidelines for systematic reviews. A total of 850 records were identified across the two databases (AJOL = 350; Google Scholar = 500). After the removal of duplicates and irrelevant records, 150 studies were retained for screening.

Following title and abstract screening, 91 studies were selected for full-text assessment (AJOL = 41; Google Scholar = 50). After applying the inclusion and exclusion criteria, 19 studies met the eligibility requirements and were included in the final review. The remaining studies were excluded due to lack of relevance to cybercrime law, enforcement, or policy outcomes.

Screening and selection were conducted by the authors, with careful cross-checking applied to ensure consistency and minimise selection bias.

The study selection process is summarised in Figure 1

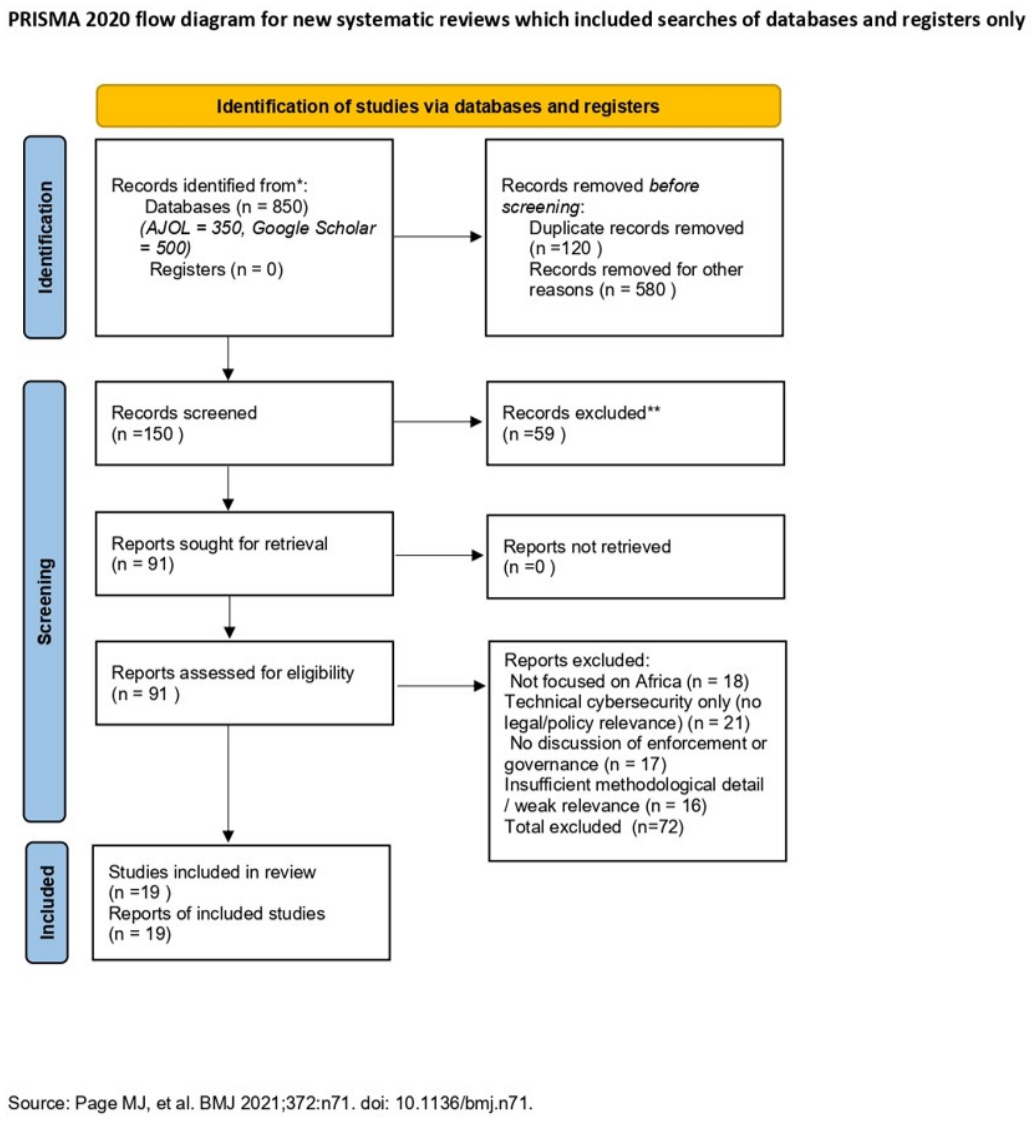

Figure 1: Identification of studies via databases and registers

2.5. Data Extraction

Data extraction was conducted using a structured approach to ensure consistency across studies. Information extracted included author(s), year of publication, geographical focus, study type, methodological approach, and key findings related to cybercrime laws and enforcement.

The characteristics of the included studies are presented in Table 1.

2.6. Quality Appraisal of Included Studies

A quality appraisal of the included studies was undertaken to assess the strength, credibility, and relevance of the evidence synthesised in this review. This step was included to enhance methodological rigour and minimise the risk of bias.

Given the diversity of the included sources, which comprised empirical studies, legal analyses, policy documents, and institutional reports, a pragmatic appraisal approach was adopted. Studies were evaluated using common criteria, including methodological clarity, data reliability, analytical depth, and relevance to the research objectives.

Empirical studies were assessed based on research design transparency, data collection methods, and analytical rigor. Legal and policy documents were evaluated based on source authority, analytical relevance, and contribution to understanding cybercrime governance. Each study was categorised as high, moderate, or low quality.

Overall, the included evidence was predominantly of moderate to high quality. Legal frameworks and policy documents were generally strong in authority and relevance, while empirical studies varied in methodological depth. The quality appraisal results are summarised in Table 2.

Table 1: Characteristics of Included Studies (n = 19)

Author(s) & Year	Country/ Region	Study Type	Methodological Approach	Thematic Focus	Contribution to Review	Quality
Empirical Studies						
Ayub & Akor (2022)	Nigeria	Empirical	Secondary data analysis	Cybercrime trends and enforcement	Demonstrates persistence of cybercrime despite existence of legal frame works	Moderate
Matsaung & Masiloane (2025)	South Africa	Empirical	Semi-structured interviews (law enforcement)	Cybercrime policing and intelligence	Identifies institutional and technical constraints affecting enforcement capacity	High
Ifenyiwa & Eneh (2024)	Nigeria	Empirical	Survey	Youth involvement in cybercrime	Links socio-economic factors to cybercrime participation and vulnerability	Moderate
Garba (2023)	Nigeria	Empirical	Questionnaire survey	Community-level cybercrime	Highlights prevalence and awareness gaps at the local level	Moderate
Ushie & Ndoma (2024)	Nigeria	Empirical	Survey	Digital literacy and cybercrime	Demonstrates role of social media literacy in cybercrime exposure and prevention	Moderate
Legal and Policy Analyses						
Jemberie & Guinchard (2024)	Ethiopia	Legal analysis	Doctrinal legislative review	Cybercrime legislation	Identifies legal gaps and limitations in national cybercrime frameworks	High
Chitimira &Ncube (2021)	South Africa	Legal/policy analysis	Doctrinal analysis	AI, 5G and cybercrime regulation	Evaluates adequacy of legal frameworks in addressing emerging technologies	High
Yilma (2021)	Ethiopia	Legal analysis	Policy and legal review	Cybercrime and human rights	Highlights tensions between enforcement measures and fundamental rights protections	High
Tachie-Menson (2023)	West Africa	Qualitative	Conceptual analysis	Maritime and cybercrime nexus	Explores emerging dimensions of cybercrime in maritime contexts	Moderate

Table 1 Continuous

Institutional and Policy Reports						
Global Cybersecurity Index (2024)	Africa (multi-country)	Report	Comparative index analysis	Cybersecurity capacity	Assesses national preparedness and institutional capacity across countries	High
AU Digital Transformation Strategy (2020)	Africa	Policy document	Strategic framework analysis	Digital governance and cybersecurity	Emphasises need for harmonised policy and institutional development	High
ECOWAS Cybersecurity Strategy	West Africa	Policy document	Strategic analysis	Regional cybersecurity governance	Highlights coordination and enforcement challenges at regional level	High
Legal Frameworks and Statutory Instruments						
Malabo Convention (2014)	Africa	Legal framework	Continental treaty	Cybersecurity and data protection	Establishes continental legal standards for cybercrime governance	High
ECOWAS Directive (2011)	West Africa	Legal framework	Regional directive	Cybercrime legislation	Promotes harmonisation of cybercrime laws across member states	High
SADC Model Law (2013)	Southern Africa	Legal framework	Model law	Cybercrime legislation	Provides template for national cybercrime legislation	High
Nigeria Cybercrime Act (2015)	Nigeria	Legal framework	Statutory law	Cybercrime enforcement	Defines offences, investigative powers, and enforcement mechanisms	High
Ghana Cybersecurity Act (2020)	Ghana	Legal framework	Statutory law	Institutional capacity	Establishes national cybersecurity authority and governance structure	High
South Africa Cybercrimes Act (2020)	South Africa	Legal framework	Statutory law	Investigation and prosecution	Strengthens legal basis for cybercrime investigation and prosecution	High
Kenya Computer Misuse & Cybercrimes Act (2018)	Kenya	Legal framework	Statutory law	Cybercrime offences	Provides comprehensive legal framework for prosecution of cyber offences	High

Table 2: Quality appraisal of included studies

Study	Type	Appraisal criteria considered	Quality rating
Ayub & Akor (2022)	Empirical	Clear focus, relevant evidence, moderate analytical depth	Moderate
Jemberie & Guinchard (2024)	Legal analysis	Strong legal analysis, high relevance, clear argumentation	High
Matsaung & Masiloane (2025)	Empirical	Clear design, direct law enforcement evidence, strong relevance	High
Chitimira & Ncube (2021)	Legal/policy analysis	Strong doctrinal depth, high relevance	High
Tachie-Menson (2023)	Qualitative/conceptual	Relevant but less directly focused on legal enforcement	Moderate
Ifenyiwa & Eneh (2024)	Empirical	Relevant findings, but narrower policy/legal depth	Moderate
Garba (2023)	Empirical	Local relevance, limited scope and methodological depth	Moderate
Ushie & Ndoma (2024)	Empirical	Relevant to awareness barriers, moderate methodological strength	Moderate
Yilma (2021)	Legal analysis	Strong conceptual and legal critique, highly relevant	High
Global Cybersecurity Index (2024)	Institutional report	Authoritative source, strong comparative relevance	High
AU Digital Transformation Strategy	Policy document	Authoritative policy relevance, limited empirical depth	High
Malabo Convention	Legal framework	Foundational continental legal instrument	High
ECOWAS Directive	Legal framework	Strong regional relevance and authority	High
ECOWAS Cybersecurity Strategy	Policy document	Strong policy relevance and regional authority	High
SADC Model Law	Legal framework	Strong legislative relevance and authority	High
Nigeria Cybercrime Act (2015)	Statutory law	Core national legal source	High
Ghana Cybersecurity Act (2020) (Republic of Ghana, 2020)	Statutory law	Core national legal source	High
South Africa Cybercrimes Act (2020)	Statutory law	Core national legal source	High
Kenya Computer Misuse & Cybercrimes Act (2018)	Statutory law	Core national legal source	High

2.7. Data Synthesis and Analysis

A thematic synthesis approach was used to analyse the data. This involved coding the findings of each study, identifying recurring patterns, and grouping these into themes aligned with the research questions. Key themes that emerged include cybercrime legal frameworks, enforcement effectiveness, institutional barriers, and policy reform.

This approach enabled the integration of diverse sources, including empirical studies and policy documents, into a coherent analytical framework.

2.8. Methodological Limitations

Despite efforts to ensure methodological rigour, this study has certain limitations. The review relied on two primary databases, which may not capture all relevant literature. In addition, the inclusion of grey literature introduces variability in evidence quality. However, these limitations were mitigated through a structured search strategy, predefined inclusion criteria, and systematic quality appraisal procedures.

3. Results

3.1. Overview of Included Studies

Following a rigorous screening and selection process, 19 studies were included in the final review. The characteristics of these studies are presented in Table 1, which summarizes their geographical scope, methodological approaches, and thematic focus.

The included studies comprise a combination of empirical research (n = 10) and legal and policy-oriented sources (n = 9), reflecting the interdisciplinary nature of cybercrime governance in Africa. Empirical studies primarily employed survey methods, interviews, and secondary data analysis, while legal and policy studies utilized doctrinal, conceptual, and comparative approaches to examine cybercrime legislation and governance frameworks.

Geographically, the evidence base is concentrated in a limited number of countries, particularly Nigeria, South Africa, and Ethiopia, with

additional insights drawn from regional and continental frameworks such as ECOWAS, SADC, and the African Union. This distribution reflects both the availability of research and the uneven development of cybercrime governance across the continent.

Overall, the included studies collectively address key dimensions of cybercrime governance, including legal frameworks, enforcement effectiveness, institutional capacity, and policy reform. Together, they provide a comprehensive foundation for analyzing the effectiveness of cybercrime laws in Africa.

3.2. Thematic Synthesis of Findings

Cybercrime Legal Frameworks in Africa (RQ1)

Across multiple contexts, the findings indicate that African countries have made significant progress in establishing formal cybercrime legal frameworks, supported by both national legislation and regional instruments. A consistent pattern emerging from the reviewed studies is the widespread adoption of legal provisions that criminalize cyber offences and define investigative and prosecutorial powers. National laws such as those in Nigeria [13], South Africa [14], and Kenya [15] illustrate this trend, reflecting increasing alignment with international and regional standards [16, 17].

At the regional and continental levels, frameworks such as the African Union Malabo Convention (African Union 2024) and the ECOWAS Directive [18] promote harmonization of cybercrime laws and encourage cooperation among member states. Similarly, the SADC Model Law provides a template for aligning national legislation with international standards [19]. As illustrated in Table 1, these policy and legal instruments form a multi-layered governance structure for cybercrime regulation in Africa.

However, despite the existence of these frameworks, several studies highlight inconsistencies in legislative scope and implementation. For instance, Jemberie and Guinchard (2024) [20] identify gaps in Ethiopia's cybercrime legislation, while Yilma (2021) [21] argues that rapid lawmaking processes often neglect stakeholder participation and human rights considerations. These findings suggest that the mere existence of legal frameworks does not guarantee their effectiveness or coherence across jurisdictions.

Effectiveness of Cybercrime Laws (RQ2)

Across the included studies, a consistent pattern emerges indicating that the effectiveness of cybercrime laws in Africa remains limited despite their formal adoption. While legal frameworks have contributed to the recognition and formalization of cybercrime offences, their practical impact on reducing cybercrime incidence appears constrained. Evidence from multiple national contexts suggests that cybercrime continues to persist, with offenders adapting to enforcement mechanisms and exploiting institutional weaknesses.

Empirical studies conducted in Nigeria indicate that cybercrime persists despite the presence of legislative measures, with offenders continuously adapting to enforcement strategies [16, 22]. Similarly, findings from South Africa reveal that although cybercrime laws provide a legal basis for prosecution, practical enforcement challenges undermine their effectiveness [23].

At a broader level, the Global Cybersecurity Index (2024) [24] demonstrates significant disparities in cybersecurity capacity across African countries, highlighting that legislative adoption does not necessarily translate into effective enforcement. As shown in Table 1, studies consistently report a gap between legal provisions and their operational outcomes, indicating that cybercrime laws alone are insufficient to achieve meaningful deterrence.

Enforcement Barriers (RQ3)

A dominant and recurring theme across the reviewed studies is the presence of significant and multi-layered barriers to the enforcement of cybercrime laws. Across diverse national and regional contexts, these barriers consistently manifest in legal, institutional, technological, and socio-cultural forms. The convergence of findings from both empirical and legal studies suggests that enforcement challenges are systemic rather than context-specific.

Legal barriers include ambiguities in legislative provisions and conflicts between cybercrime enforcement and human rights protections. Yilma (2021) [21] highlights that certain cybercrime laws in Ethiopia risk infringing on fundamental rights such as privacy and freedom of expression, thereby complicating enforcement efforts.

Institutional barriers are particularly prominent, with multiple studies reporting limited capacity within law enforcement agencies. For example, Matsaung and Masiloane [23] identify challenges related to insufficient training, lack of specialized personnel, and weak inter-agency coordination. Similarly, Jemberie and Guinchard (2024) [20] emphasize structural weaknesses in legislative and institutional frameworks.

Technological barriers further exacerbate enforcement challenges. Law enforcement agencies often lack access to advanced digital forensic tools and expertise required for investigating cybercrime. This limitation is compounded by difficulties in collecting and preserving digital evidence, as well as the rapid evolution of cybercriminal techniques [17].

In addition, socio-cultural factors such as low levels of digital literacy and underreporting of cybercrime significantly hinder enforcement. Ushie and Ndoma (2024) [25] demonstrate that social media illiteracy increases vulnerability to cybercrime, while also limiting the effectiveness of prevention strategies. These findings, summarized in Table 1, underscore the multidimensional nature of enforcement barriers in the African context.

Role of Law Enforcement and Judicial Institutions (RQ4)

Across multiple studies, the role of law enforcement and judicial institutions emerges as a central determinant of cybercrime law effectiveness. A consistent pattern identified in the literature is that, while these institutions are formally tasked with enforcing cybercrime laws, their operational capacity remains constrained. This limitation is observed across different country contexts, indicating a broader structural challenge rather than isolated institutional weaknesses.

Law enforcement agencies face significant challenges in investigating cybercrime cases, particularly in relation to digital evidence collection and analysis. Matsaung and Masiloane (2025) [23] report that investigators often encounter difficulties in accessing reliable

forensic tools and maintaining the integrity of digital evidence. Furthermore, victim reluctance to report cybercrime or participate in legal proceedings poses additional challenges.

Judicial institutions also face capacity constraints, including limited expertise in handling cybercrime cases and delays in adjudication. These issues contribute to low conviction rates and undermine the deterrent effect of cybercrime laws. As indicated in Table 1, empirical studies consistently highlight the need for specialized training and institutional reforms to enhance the effectiveness of both law enforcement and judicial systems.

Despite these challenges, some progress has been observed, including the establishment of specialized cybercrime units and increased collaboration among agencies. However, these efforts remain uneven across countries and are often insufficient to address the scale and complexity of cybercrime.

Policy and Regulatory Reform (RQ5)

Across the reviewed literature, there is strong convergence on the need for comprehensive policy and regulatory reforms to enhance cybercrime law enforcement in Africa. A consistent pattern emerging from both empirical and policy-oriented studies is that existing frameworks require not only legal refinement but also institutional strengthening and technological investment. This reflects a shared recognition that legislative development alone is insufficient to address the evolving nature of cybercrime.

Regional cooperation emerges as a critical component of effective cybercrime governance. Policy frameworks such as the African Union Digital Transformation Strategy [26] and the ECOWAS Cybersecurity Strategy (ECOWAS. , n.d.) highlight the importance of coordinated approaches to cybersecurity and cross-border collaboration.

Furthermore, several studies stress the need to balance cybercrime enforcement with the protection of human rights. Yilma (2021) [21] argues that legal frameworks must be designed to safeguard fundamental freedoms while addressing cybercrime threats. Similarly, Jemberie and Guinchard [20] advocate for evidence-based legislative reforms that reflect both technological developments and international best practices.

Public awareness and digital literacy are also identified as essential elements of effective cybercrime prevention. Ushie and Ndoma (2024) [25] emphasise that improving digital literacy can reduce vulnerability to cybercrime and enhance the overall effectiveness of enforcement strategies.

Overall, the synthesis of findings across the included studies reveals a consistent pattern in which the existence of cybercrime laws is not matched by their effective implementation, highlighting a systemic gap between legal frameworks and enforcement capacity in the African context.

4. Discussion

This study examined the effectiveness of cybercrime laws in Africa through a systematic synthesis of empirical studies, legal analyses, and policy frameworks. The findings reveal a persistent gap between the formal adoption of cybercrime legislation and its practical enforcement, highlighting a broader challenge in translating regulatory frameworks into effective governance outcomes.

A central insight emerging from this study is the existence of a structural disconnect between legal development and enforcement capacity. While many African countries have established cybercrime laws aligned with regional and international standards, these legal frameworks have not consistently resulted in effective deterrence or prosecution. This pattern is not unique to the African context but reflects a broader phenomenon observed in global cybercrime governance, where the rapid evolution of digital threats often outpaces institutional and regulatory responses [5, 27]. However, the findings of this study suggest that this gap is particularly pronounced in contexts where institutional and technological capacities remain limited.

This disconnect can be understood through the lens of institutional capacity theory, which emphasizes that the effectiveness of legal systems is contingent upon the capabilities of the institutions responsible for their implementation [28, 29]. In the context of cybercrime, enforcement requires specialized expertise, digital forensic infrastructure, and coordinated inter-agency responses. The findings indicate that, across multiple African contexts, these enabling conditions are often insufficiently developed, resulting in what can be conceptualized as a capacity-constrained regulatory environment. In such settings, legal frameworks may exist in formal terms but remain underutilized or inconsistently applied in practice.

The study further demonstrates that enforcement challenges are not merely technical but are embedded within broader structural and systemic constraints. Consistent with regulatory effectiveness literature, enforcement outcomes are shaped by the interaction between legal rules, institutional arrangements, and socio-economic conditions [30]. In the African context, these challenges manifest in limited technical expertise, inadequate access to digital forensic tools, weak institutional coordination, and resource constraints within law enforcement and judicial systems. These factors collectively undermine the ability of institutions to investigate, prosecute, and deter cybercrime effectively.

In addition to institutional limitations, the findings highlight important tensions within cybercrime legal frameworks themselves. While these laws are designed to enhance security and address emerging threats, they may also create risks for fundamental rights if not carefully calibrated. This reflects a broader tension identified in global cyber governance literature between the need for effective security measures and the protection of civil liberties [31, 32]. In some contexts, concerns regarding privacy, freedom of expression, and due process may affect both the legitimacy and the practical enforcement of cybercrime laws.

Another significant dimension of the findings is the role of socio-cultural factors in shaping cybercrime governance outcomes. The effectiveness of legal frameworks is influenced not only by institutional capacity but also by levels of public awareness, digital literacy, and reporting behaviour. Low levels of digital literacy and underreporting of cybercrime incidents limit the ability of authorities to respond effectively and reduce the overall impact of legal interventions [33, 34]. This suggests that cybercrime governance should be understood as a socio-technical system in which legal, institutional, and societal factors interact to influence enforcement outcomes.

The study also highlights the fragmented nature of cybercrime governance across the African continent. Although regional frameworks such as those developed by the African Union and ECOWAS aim to promote harmonization, their implementation remains uneven. This fragmentation poses significant challenges in addressing transnational cybercrime, which inherently operates across borders [35]. The absence of strong and coordinated cross-border enforcement mechanisms limits the effectiveness of national legal frameworks and underscores the

need for deeper regional integration.

From a policy perspective, the findings challenge the prevailing emphasis on legislative reform as the primary response to cybercrime. While the development of legal frameworks is an important step, it is insufficient in the absence of corresponding investments in institutional capacity and technological infrastructure. The findings suggest that effective cybercrime governance requires a more integrated approach that prioritizes capacity-building, including specialized training for law enforcement and judicial actors, investment in digital forensic capabilities, and improved inter-agency coordination.

Importantly, this study contributes to the literature by advancing a shift from a law-centric to a capacity-centric understanding of cybercrime governance in Africa. While previous research has highlighted the growth of cybercrime and the development of legal responses [36]. This study provides a systematic synthesis demonstrating that enforcement effectiveness is primarily shaped by institutional and technological constraints rather than the absence of legal frameworks. This contribution offers a more nuanced analytical lens for understanding cybercrime governance in developing contexts.

At the same time, the findings underscore the importance of balancing enforcement objectives with the protection of fundamental rights. Effective cybercrime governance must ensure that legal frameworks are not only enforceable but also legitimate and consistent with principles of accountability, proportionality, and transparency. This balance is critical for maintaining public trust and ensuring compliance with legal and regulatory measures.

Overall, the findings of this study suggest that the effectiveness of cybercrime laws in Africa is determined by a complex interplay of legal, institutional, technological, and societal factors. Addressing the challenges identified requires a shift towards integrated governance approaches that align legal frameworks with the institutional and technological realities of the African context. Such an approach is essential for developing resilient and effective cybercrime governance systems capable of responding to the evolving nature of digital threats.

5. Conclusion

This study set out to critically examine the effectiveness of cybercrime laws in Africa by synthesising empirical, legal, and policy evidence through a systematic literature review. The findings demonstrate that while significant progress has been made in the development of cybercrime legislation across the continent, the effectiveness of these laws remains constrained by a persistent gap between legal frameworks and their practical enforcement.

The study makes an important contribution by reframing cybercrime governance in Africa as a capacity-driven challenge rather than a purely legal one. It shows that the proliferation of cybercrime laws, often aligned with international and regional standards, has not translated into commensurate improvements in enforcement outcomes. Instead, the effectiveness of these laws is shaped by deeper structural factors, including limited institutional capacity, inadequate technological infrastructure, weak inter-agency coordination, and socio-cultural dynamics such as low digital literacy and underreporting.

By integrating diverse sources of evidence, this study advances a more nuanced understanding of cybercrime governance as a multi-dimensional system in which legal, institutional, technological, and societal elements interact. This perspective moves beyond traditional law-centric analyses and highlights the need for a more holistic approach that prioritizes capacity-building, institutional strengthening, and technological investment alongside legislative reform.

The findings also underscore the importance of regional cooperation in addressing the transnational nature of cybercrime. While frameworks developed by organizations such as the African Union and ECOWAS provide a foundation for harmonization, their effectiveness depends on consistent implementation and stronger mechanisms for cross-border collaboration. At the same time, the study highlights the need to ensure that cybercrime laws are designed and implemented in a manner that respects fundamental rights, thereby maintaining public trust and legitimacy.

From a policy perspective, the study suggests that future efforts should focus on enhancing the operational capabilities of law enforcement and judicial institutions, investing in digital forensic infrastructure, and promoting public awareness and digital literacy. These measures are essential for bridging the gap between legal provisions and enforcement outcomes.

Despite its contributions, this study is not without limitations. The review is based on a finite number of studies and databases, which may not capture all relevant literature. In addition, variations in methodological approaches across the included studies may influence the comparability of findings. Future research should explore comparative analyses across regions, as well as empirical assessments of specific capacity-building interventions and their impact on cybercrime enforcement.

In conclusion, the effectiveness of cybercrime laws in Africa cannot be understood solely in terms of legislative development. Rather, it depends on the broader governance ecosystem within which these laws operate. Addressing the challenges identified in this study requires a shift towards integrated, capacity-oriented approaches that align legal frameworks with the institutional and technological realities of the African context. Such an approach is essential for developing resilient and effective cybercrime governance systems capable of responding to the evolving nature of digital threats.

Article Information

Acknowledgments: The authors would like to acknowledge the contributions of colleagues and researchers whose work informed this study. We also appreciate the support of our respective institutions in facilitating this research.

Author Contributions: Sandra Frimpong - Conceptualization, Methodology, Writing – original draft, Supervision, Writing – review & editing; Charles C. Udechukwu - Conceptualization, Writing – original draft, Writing – review & editing; Mariam Iyabo Adeoba - Methodology, Formal analysis, Writing – review & editing; Thomas Kofi Mensah - Data curation, Formal analysis, Writing – review & editing; Doreen Mensah - Data curation, Writing – review & editing.

Funding / Financial Support: The authors received no external funding.

Conflict of Interest: The authors declare no competing interests.

Disclaimer (Artificial Intelligence): The author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.), and text-to-image generators have been used during writing or editing of manuscripts.

References

[1] Y. Shan. Digital platforms and the transformation of crime governance. *Journal of Chinese Sociology*, 13(1), 2026. URL https://doi.org/10.1186/s40711-025-00252-0.

[2] V. A. Adewopo, S. W. Azumah, M. A. Yakubu, et al. Comprehensive analytical review of cybercrime and cyber policy in West Africa. *Journal of Electrical Systems and Information Technology*, 12(20), 2025. URL https://doi.org/10.1186/s43067-025-00216-x.

[3] R. Boateng, L. Olumide, R. S. Isabalija, and J. Budu. Sakawa cybercrime in Ghana: A criminological perspective. *Journal of Financial Crime*, 27(1):39–52, 2020.

[4] S. A. Asongu, J. C. Nwachukwu, and S. M. Orim. Mobile phones, institutional quality and cybercrime in Sub-Saharan Africa. *Information Technology for Development*, 25(2):350–370, 2019.

[5] A. A. Khan. Reconceptualizing policing for cybercrime: Perspectives from Singapore. *Laws*, 13(4):44, 2024. URL https://doi.org/10.3390/laws13040044.

[6] N. Kshetri. Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2):77–81, 2019.

[7] T. J. Holt, A. M. Bossler, and K. C. Seigfried-Spellar. *Cybercrime and digital forensics: An introduction*. Routledge, 2018.

[8] D. Clark, T. Berson, and H. S. National Research Council Lin. *At the nexus of cybersecurity and public policy: Some basic concepts and issues*. National Academies Press, 2014. URL https://www.ncbi.nlm.nih.gov/books/NBK223213/.

[9] N. Kshetri. *Cybercrime and cybersecurity in the global South*. Palgrave Macmillan, 2013.

[10] O. A. C. Pirrolas and P. M. A. R. Correia. From isomorphism to institutional work: The advancement of institutional theory in public administration. *Encyclopedia*, 5(4):184, 2025. URL https://doi.org/10.3390/encyclopedia5040184.

[11] F. Palazzi, A. Sentuti, and F. Sgrò. The institutionalisation of a new management control system: A focus on situated rationality. *Journal of Management and Governance*, 29:1045–1082, 2025. URL https://doi.org/10.1007/s10997-025-09753-z.

[12] H. Snyder. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104:333–339, 2019.

[13] Federal Republic of Nigeria. Cybercrime (prohibition, prevention, etc.) act. 2015.

[14] Republic of South Africa. Cybercrimes act. 2020.

[15] Republic of Kenya. Computer misuse and cybercrimes act. 2018.

[16] A. O. Ayub and L. Akor. Trends, patterns and consequences of cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences*, 2022.

[17] H. Chitimira and P. Ncube. The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African banks. *PER/PELJ*, 24, 2021.

[18] ECOWAS. Directive on fighting cybercrime. 2011.

[19] SADC. Model law on computer crime and cybercrime. 2013.

[20] M. A. Jemberie and A. Guinchard. Assessing Ethiopia's readiness to combat computer-focused crimes: A legislative analysis. *Bahir Dar University Journal of Law*, 2024.

[21] K. M. Yilma. *Cybercrime lawmaking and human rights in Ethiopia*. Mizan Law Review, 2021.

[22] J. Garba. An approach to cybercrime issues in Dandume Local Government Area of Katsina State, Nigeria. 2023.

[23] P. Matsaung and D. T. Masiloane. *The role of cyber intelligence in policing cybercrime in South Africa*. African Security Review, 2025.

[24] International Telecommunication Union. Global cybersecurity index 2024. 2024.

[25] C. U. Ushie and R. N. Ndoma. Social media literacy and cybercrime: A study of Calabar metropolis, Nigeria. *LWATI Journal of Contemporary Research*, 2024.

[26] African Union. Digital transformation strategy for Africa (2020–2030). 2020.

[27] M. Chawki. Legal foundations and future directions of AI-enabled cybersecurity: A cross-jurisdictional analysis. *Cogent Social Sciences*, 12(1), 2026. URL https://doi.org/10.1080/23311886.2026.2614015.

[28] Y. Tan. Historical institutionalism, political settlement and land ownership system in Nigeria. *International Journal of Urban Sustainable Development*, 17(1):136–153, 2025. URL https://doi.org/10.1080/19463138.2025.2495580.

[29] O. H. Okunola. Beyond institutional silos: Rethinking multilevel disaster risk governance in Africa a decade into the Sendai framework implementation. *International Journal of Disaster Risk Science*, 16:321–332, 2025. URL https://doi.org/10.1007/s13753-025-00646-1.

[30] A. Paranata. A systematic literature review of anti-corruption policy: A future research agenda in Indonesia. *Public Organization Review*, 25:1181–1214, 2025. URL https://doi.org/10.1007/s11115-025-00847-8.

[31] J. He and Z. Zhang. Algorithm power and legal boundaries: Rights conflicts and governance responses in the era of artificial intelligence. *Laws*, 14(4):54, 2025. URL https://doi.org/10.3390/laws14040054.

[32] S. Savaş and S. Karataş. Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, 3(1):7–34, 2022. URL https://doi.org/10.1365/s43439-021-00045-4.

[33] H. H. Alnaqbi and E. A. M. Ali. Social media impact on societal security. *Frontiers in Sociology*, 10:1508542, 2025. URL https://doi.org/10.3389/fsoc.2025.1508542.

[34] S. Mushtaq and M. Shah. Critical factors and practices in mitigating cybercrimes within e-government services: A rapid review on optimising public service management. *Information*, 15(10):619, 2024. URL https://doi.org/10.3390/info15100619.

[35] African Union. Convention on cyber security and personal data protection (Malabo Convention). 2014.

[36] S. Khan, T. Saleh, M. Dorasamy, N. Khan, S. L. O. Tan, and R. Gale Vergara. A systematic literature review on cybercrime legislation. *F1000Research*, 11:971, 2022. URL https://doi.org/10.12688/f1000research.123098.1.