International Journal of Innovative Information Systems & Technology Research 13(4):355-374, Oct-Dec, 2025

 www.seahipublications.org ISSN: 2467-8562

doi:10.5281/zenodo.17882226

An AI-Powered Framework For Assessing Cybersecurity Governance Maturity In African Nations: A Hybrid Model Approach

[1]Olugbile Olusegun Hamed,;[2]T.K. Anyachebelu; [3]Steven Bassey; [4]Ojeniyi Joseph & [5]Paul Owoicho Gideon

Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nasarawa State, Nigeria

Email: olugbileolusegun00006@nsuk.edu.ng, ojeniyiji@futminna.edu.ng, anyachebelutk@nsuk.edu.ng, onyelebocho100@gmail.com

ABSTRACT

Africa's rapid digital transformation is fueling unprecedented economic growth but has simultaneously exposed the continent to a surge in sophisticated cyber threats. Ensuring robust cybersecurity governance is critical; however, conventional assessment methods which are rooted in manual and fragmented processes, are increasingly inadequate due to their limited scalability, delayed responsiveness, and objectivity. This paper introduces an innovative, hybrid framework powered by artificial intelligence (AI) to assess the maturity and effectiveness of cybersecurity governance in African nations. The proposed model leverages Natural Language Processing (NLP) to automate the analysis of unstructured policy documents, couples this with continuous, real-time monitoring of technical controls, and incorporates a dynamic, context-sensitive maturity assessment engine. By overcoming the constraints of traditional audits, this approach delivers a more precise, scalable, and actionable methodology for enhancing national cyber resilience. The proposed framework is specifically tailored to address the unique socio-economic, geo-political and technological challenges of the African continent, including data scarcity, infrastructure gaps, and the imperative of digital sovereignty. It provides a transformative path toward proactive and resilient cybersecurity governance across the continent.

Keywords: Cybersecurity Governance; Structural Equation Modeling (SEM); Africa; Natural Language Processing (NLP); Cybersecurity Policy

INTRODUCTION

The proliferation of information and communication technologies (ICTs) has accelerated Africa's socio-economic development, creating new opportunities for businesses and citizens.[1] However, this digital leap is accompanied by a dramatic increase in cyber threats, with a recent report indicating that Africa has become the most targeted region in the world for cyberattacks, enduring 3,374 attacks per week.[3] This context underscores the critical importance of robust cybersecurity governance.

Cybersecurity governance, defined as the formal and strategic management of an organization's cyber presence, risks, and controls [4], is no longer a purely technical concern but a strategic and political one, especially at the national level. Effective governance frameworks are essential for safeguarding critical infrastructure, ensuring citizen trust, and attracting investment into the digital ecosystem.[1]

1.1. Research Problem

A fundamental gap exists between the dynamic nature of cyber threats and the static, manual methods traditionally used to assess cybersecurity governance. Existing assessments, which often rely on periodic audits, questionnaires, and manual reviews, are reactive and fail to provide real-time visibility into an organization's or nation's security posture.[5] This creates a dangerous lag between the emergence of new threats and a board's understanding of its risks. This reactive nature means that defenses are often built on past breaches rather than in anticipation of future ones, leaving organizations playing a constant game of catch-up.[7]

The unique challenges confronting African nations, namely, a fragmented regulatory environment, persistent infrastructural shortfalls, and the critical imperative to establish digital sovereignty, demand the development of a measurement tool that is both adaptive and contextually nuanced. The conceptualisation of a novel model underpinned by artificial intelligence presents a means to surmount these obstacles, thereby facilitating the advancement of more effective and resilient cybersecurity governance across the continent.

The motivation for this research is to provide African states with a mechanism that transitions their cybersecurity stance from a predominantly defensive and reactive orientation to one that is proactive and predictive. Thus, the proposed approach aims to directly enhance digital security autonomy and underpin sustained economic stability within the region.

1.2. Paper Contribution and Structure

The primary contribution of this paper lies in the development of an innovative, multifaceted artificial intelligence framework, meticulously tailored to the assessment of cybersecurity governance maturity within the African contexts. This hybrid model integrates the rigorous analysis of policy documents with the continuous evaluation of empirical, operational data, thereby directly addressing the inherent limitations of prevailing assessment methodologies. The framework aspires to produce a robust, scalable, and objective mechanism for appraising national cyber resilience, specifically attuned to the distinct challenges and requirements of African nations.

The structure of this paper is as follows: Section 2 delivers an exhaustive review of extant literature concerning cybersecurity governance, digital sovereignty, and the distinctive policy environment within Africa.

Section 3 critically examines the shortcomings inherent in conventional assessment methodologies. Section 4 presents the architecture and principal components of the proposed artificial intelligence-driven framework. Section 5 explores the practical implications of the model, with particular emphasis on its capacity to address Africa-specific socioeconomic, regulatory, and technological challenges. Section 6 concludes by summarising the paper's findings, outlining the study’s limitations, and suggesting directions for future research.

II. THE IMPERATIVE OF CYBERSECURITY GOVERNANCE IN AFRICA: A DIGITAL SOVEREIGNTY PERSPECTIVE

2.1. Defining Cybersecurity Governance and its Frameworks

Cybersecurity governance is a strategic function that dictates the policies, procedures, and standards for protecting an organization against cyber threats.[4] It goes beyond technical controls to encompass a formal management structure that includes directive, automated, and manual controls to protect against cyber risks.[4] Widely recognized frameworks such as the NIST Cybersecurity Framework (NIST CSF), ISO 27001, and COBIT provide a structured approach to defining and implementing these controls.[8] While these frameworks offer a robust foundation, their one-size-fits-all nature may not fully align with the unique context of African nations, particularly concerning localized threats, cultural values, and the state of digital infrastructure. The

Cyber Assessment Framework (CAF) developed by the UK's National Cyber Security Centre (NCSC) is another structured tool that provides detailed guidelines for evaluating and enhancing an organization's cybersecurity posture.[9]

2.2. Digital Sovereignty and the Challenge of Digital Colonialism

Digital sovereignty is the ability of a nation to build, govern and protect its digital infrastructure and AI systems in alignment with its social values, economic needs and constitutional rights.[10] It is not about isolation but about autonomy, and it has become a central theme in Africa's digital discourse.[10] This drive is motivated by growing concerns over the dominance of foreign technology firms, a situation often referred to as "digital colonialism".[12]

Digital colonialism describes a modern-day scramble for Africa's data, where large-scale tech companies extract, analyse, and own user data for profit and market influence with nominal benefit to the data source.[13] This process is facilitated by scant data protection laws and the foreign ownership of critical digital infrastructure.[13] As foreign tech companies control digital services and infrastructure, they gain access to vast amounts of user data, which is often exported and monetized through predictive analytics and targeted advertising.[13] The continent's limited voice in global tech policy forums and the fragmentation of national regulations exacerbate this problem, leaving individual countries vulnerable to geopolitical pressure.[10] The pursuit of digital sovereignty, therefore, is not merely a political or security objective; it is an economic and cultural imperative. It is a necessary step for nations to move from "digital consumption to digital capability" [10] and to counter a form of technological dependency that could undermine their ability to shape their own digital future.

III. CONTINENTAL AND NATIONAL POLICY FRAMEWORKS

African nations are actively developing and implementing policies to address these challenges. The African Union (AU) has taken a leading role in creating foundational frameworks.

2.3.1 The Malabo Convention: The African Union Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, is Africa's first continent-wide legal instrument for cybersecurity and data protection.[16] Adopted in 2014, it provides a framework similar to the European Union's GDPR and is a critical tool for protecting personal data and preventing cybercrime.[16] The Convention criminalizes a broad range of cyber activities, establishes personal data protection rights, and mandates international cooperation.[17] A key provision of the treaty, Article 36, states that it would only come into effect upon ratification by 15 member states. This milestone was achieved on June 8, 2023, after Mauritania became the 15th country to ratify it.[17] The Convention requires member states to establish data protection authorities and ensure secure data collection, processing, and storage.[18]

2.3.1 The African Union's AI Strategy: The AU's Continental AI Strategy (2024) is a critical anchor document that positions AI as an enabler of socio-economic growth and emphasizes the importance of robust AI governance based on ethical principles and democratic values. [19] It calls for the development of national AI strategies and considers data protection frameworks as a prerequisite for responsible AI.[20]

2.3.2 National Case Studies: African countries are also developing their own national policies to address the growing cyber threat landscape. In Nigeria, the Nigerian Communications Commission (NCC) is preparing a new regulatory framework to strengthen cybersecurity in the telecommunications sector, building on the Cybercrime Prevention Act of 2015 and the Data Protection Act of 2023.3 South Africa's National Cybersecurity Policy Framework (2012) and the Cybersecurity Hub (2015) emphasize public-private partnerships and participation in regional and international fora to advance the global cybersecurity agenda.21 In Uganda, the National Cybersecurity Strategy aims to create a "cybersafe and protected Uganda" through a "whole-of-nation principle" that calls for collaboration between citizens, the private sector, and government agencies.1

2.3.3 IV. CRITICAL CHALLENGES FOR AFRICAN AI DEVELOPMENT AND GOVERNANCE

significant challenges remain. Many African countries face infrastructure gaps, including limited access to electricity, high-speed internet, and advanced computational infrastructure like GPUs.2 Data centers, crucial for AI, require immense power and water, resources that are scarce in many regions. The lack of locally generated and representative datasets is a major impediment to AI development, contributing to global health inequities and cultural erasure.11 AI models trained on external data may embed biases that do not reflect the lived realities, languages, and cultural diversity of African societies, thereby failing to

address unique needs. Furthermore, there is a significant shortage of professionals with the technical skills needed to develop, maintain, and govern complex AI systems, which contributes to talent migration to the Global North.These interconnected challenges highlight the need for a measurement framework that is not only technologically advanced but also adaptable to these on-the ground realities.

TABLE 1. Key Provisions of the Malabo Convention and AU Policy Frameworks

Framework	Core Focus Areas	Key Provisions and
Malabo Convention [17]	Cybercrime, Data Protection,	Criminalizes cyber activities, establishes data protection authorities, and mandates international cooperation (information sharing, mutual legal assistance, extradition). In effect since June 2023.
AU Continental AI Strategy [19]	Harnessing Benefits, Building Capabilities, Minimizing Risks, Stimulating Investment, Fostering Cooperation	Positions AI as an enabler of socio-economic growth. Considers governance and data protection laws as essential building blocks for responsible AI development. Calls for national AI strategies aligned with development priorities.
AU Data Policy Framework [24]	Data Flow, Human Rights, Security, Equitable Sharing	Provides a shared continental vision to enable data to flow cooperatively across Africa. Promotes data as a strategic asset for innovation and digital transformation.

TABLE 2. Comparison of Traditional vs. AI-Enhanced Cybersecurity Governance Assessments

S/N	Criterion	Traditional Assessment	AI-Enhanced Assessment
I	Speed	Reactive, slower response times due to manual processes [29]	Real-time, automated detection and response [29]
Ii	Scalability	Labor-intensive, struggles with large data volumes [5]	High scalability, processes vast datasets efficiently [30]
Iii	Visibility	Periodic, point-in-time snapshots [5]	Continuous monitoring, provides real-time view of risk [30]
Iv	Accuracy	Prone to human error and subjectivity [6]	Dynamic, continuously learns and improves accuracy [29]
V	Adaptability	Static, built on past threats [7]	Predictive, learns from new data to anticipate threats [29]
vi	Cost	Lower initial cost, but higher long-term maintenance costs [29]	Potentially higher upfront investment, but lower longterm operational costs [29]

3. Limitations of Conventional Cybersecurity Governance Assessment Methodologies

Conventional approaches to assessing cybersecurity governance frameworks are inherently limited and fail to meet the demands of a modern, agile digital environment. These methods, which are often based on manual, periodic audits and compliance checklists, are fundamentally flawed in several keyways.

i. A primary limitation is that traditional audits are reactive and provide a "point-in-time snapshot".[5] They are typically conducted on an annual or quarterly basis and are built on lessons learned from past breaches, not on the anticipation of new threats. This creates a dangerous lag, as new vulnerabilities, zero-day exploits, and emerging threats can go undetected between assessment cycles, leaving organizations and nations dangerously exposed.[5]

ii. Furthermore, these assessments rely heavily on manual processes.[5] Human auditors must review logs, policies, and questionnaires, a process that is time-consuming, labor-intensive, and prone to human error, bias, or misconceptions.[5]

iii. Manual audits also struggle to analyze the sheer volume of data generated by modern IT infrastructures, particularly at the national level, which creates significant scalability issues.[5] This is compounded by the fact that many reports present long lists of technical issues that are not useful for strategic, business-level decision-making, creating a gap between technical teams and executives. [6]

iv. Traditional frameworks often face challenges due to their subjective and ambiguous nature. While frameworks such as the NIST CSF use maturity tiers (e.g., Partial, Risk Informed, Repeatable, Adaptive), a single, highlevel rating can obscure critical, granular vulnerabilities.[27] A key paradox emerges: a high maturity score does not always equate to low risk.[27] A traditional audit might rate an organization as Tier 3 – Repeatable based on its high-level processes. However, this aggregated score, by design, may not drill down to a specific, misconfigured cloud application that represents a severe, immediate risk.[27] The static, point-intime nature of the assessment means it would likely miss this granular

v. Vulnerability, leading to a complacency trap where a false sense of security leads to bad decisions.[6.] This problem is further compounded by the fact that many audits prioritise adherence to regulatory checklists over a comprehensive evaluation of a system's actual security posture.[5] This compliance-driven approach can result in a "high maturity" rating while the organization remains dangerously exposed to a new exploit that wasn't on last year's checklist

4. An AI-Enhanced Approach to Governance Measurement: Theoretical Model and Components

4.1. The Case for AI in Cybersecurity

AI is reshaping cybersecurity strategies by enabling adaptive, proactive defenses that go beyond the static rules and known threat signatures of traditional tools.[29] The capabilities of AI and Machine Learning (ML) empower cybersecurity systems to analyze vast amounts of data, identify patterns, and make informed decisions at speeds and scales far beyond human capabilities.[29] AI-powered systems can detect threats in real-time, enabling rapid response and mitigation.[33] They are effective for realtime threat detection, anomaly detection, and vulnerability management.[32] AI-powered solutions offer predictive capabilities, continuous adaptation, and increased accuracy over time, learning from new data to stay ahead of the evolving threat landscape and reducing false positives and negatives.[29]

AI is not a replacement for human security teams; it is a force multiplier that automates labor-intensive tasks and elevates human roles to strategic oversight.[34] Traditional security analysis involves manually reviewing massive volumes of logs and security data, a time-consuming and errorprone task.[5] AI can automate this log analysis and vulnerability scanning, processing data in real time.[5] This automation reduces "SOC fatigue" and frees human analysts from "labor-intensive task execution".[34] This shift allows security analysts to move towards higher-value activities, focusing on "critical, high business impact activities" and "highvalue decision-making".[34] Thus, the real value of AI is not in replacing human security professionals but in creating a more effective and efficient "human-AI team collaboration".[35]

4.2. Overview of the Conceptual Model

The proposed model is a continuous, feedback-driven system designed to overcome the limitations of traditional assessments. It operates on three interconnected pillars: automated policy analysis, continuous technical assessment, and dynamic risk quantification. The model begins by ingesting a nation's formal cybersecurity governance frameworks, such as laws, policies, and national strategies. A Natural Language Processing (NLP) engine then processes this unstructured text, extracting key requirements and controls. These extracted "rules" are then used to drive a continuous, automated technical assessment of the nation's digital infrastructure. Finally, the collected data is used to generate a dynamic, quantified maturity and risk score, providing a realtime, actionable view of governance effectiveness. This integrated

approach ensures that the assessment is always aligned with both the stated policies and the operational reality of the country's cyber posture.

V THE AUTHOR'S PROPOSED CYBERSECURITY GOVERNANCE MODEL

4.3.1 Conceptual Framework The proposed framework is built upon a conceptual model that identifies seven key independent variables influencing cybersecurity governance, as shown in the author's construct in Figure 2.1. These variables are considered crucial to a holistic assessment of a nation's cyber posture.

- Risk Assessment: This variable captures the nation's capacity to identify, analyze, and prioritize cyber risks and vulnerabilities.
- Cultural Aspects: This dimension includes factors such as public awareness, digital literacy, and the human element in cybersecurity.
- Technology: This variable encompasses the nation's technological infrastructure, adoption of emerging technologies, and the availability of cybersecurity tools.
- Geopolitical Dimension: This accounts for the influence of international relations, conflicts, and digital sovereignty on a nation's cyber defense strategy.
- Economic Matters: This variable considers the financial aspects, including investment in cybersecurity, the economic cost of cyberattacks, and the readiness of economic infrastructure.
- Global Blocs Open Issues: This dimension addresses the challenges and opportunities presented by global digital cooperation and potential fragmentation.
- Legal Aspects: This includes the presence of robust policies, regulations, and legal frameworks for combating cybercrime and ensuring data protection.

The model also explores the roles of mediating and moderating variables. A mediating variable, such as Technology, explains the relationship between an independent variable and a dependent variable. A moderating variable, like the Geo-Political Dimension, alters the strength or direction of a relationship between two other variables. The Structural Equation Model (SEM) will be used to test the relationships between these variables.

Based on the conceptual framework, the author's construct presents a detailed model for measuring cybersecurity governance.[44] The model identifies

Cybersecurity Governance as the dependent variable, influenced by seven key

independent variables.[44]

i. Risk Assessment: This includes several significant independent variables: Threat, Vulnerability,

Board (Strategic level), Management (Tactical level), Operation, Asset, Incident

Response, and Resource capacity (Budget, Training, 3rd Party Supply Chain).[44]

ii. Cultural Factors: Metrics for this variable include Awareness, Culture, Skills/Education, Human Error, Social engineering, and Social trends.[44]

iii. Technology Factors: This variable is measured by factors such as Emerging Technology,

Infrastructure, Dependency, Convergence, Tools, and Remote Operation.[44]

iv. Geopolitical Factors: The model considers Attribution, Human rights, Digital Sovereignty, Digital Diplomacy, Fragmentation, Trade & Commerce, and Geopolitical tension as key metrics. [44]

v. Economic Factors: This includes the Economic Cost of Cyberattack, Investment, Resource mobilisation, Economic Infrastructure, and Intellectual Property.[44]

vi. Global Blocs Open Issues: This variable's metrics are Policy, Regulation, State Adversaries,

Conflicts, and International

Cooperation.[44] vii. Legal Factors: Similar to Risk Assessment, this is considered a significant independent variable with metrics covering Standards/Best Practice, Compliance, and Regulation.[44]

The construct also identifies three variables as insignificant: Social Stratification, Demographical Factor (Age, Gender, Occupation), and Environmental Factor.[44]

The model further incorporates mediating and moderating variables to provide a more nuanced understanding of the relationships between the independent variables and cybersecurity governance.[44] A mediating variable explains the how or why an effect takes place, essentially acting as a link in the causal chain between an independent and a dependent variable.[45] In contrast, a moderating variable affects the

strength and direction of the relationship between two variables, indicating the conditions under which a relationship is stronger or weaker.[45] By including these variables, the model moves beyond a simple correlation to provide a fuller picture of the complex dynamics in the real world.[46]

4.3. 2. Conceptual Hybrid Framework

The conceptual AI model is named the Integrated African Cybersecurity Governance Assessment Model (IACG-AM) is an AI-powered adaptive framework for assessing cybersecurity governance maturity in African nations. It utilises a hybrid model approach using a continuous, feedbackdriven system designed to overcome the limitations of traditional assessments cybersecurity governance. It operates on three interconnected pillars: automated policy analysis, continuous technical assessment, and dynamic risk quantification. The model begins by ingesting a nation's formal cybersecurity governance frameworks, such as laws, policies, and national strategies. A Natural Language Processing (NLP) engine is utilised to process this unstructured text, extracting key requirements and controls.

These extracted rules are then used to drive a continuous, automated technical assessment of the nation's digital infrastructure. The collected data is used to generate a dynamic, quantified maturity and risk score, providing a real-time, actionable view of governance effectiveness. This integrated approach ensures that the assessment is always aligned with both the stated policies and the operational reality of the country's cyber posture.

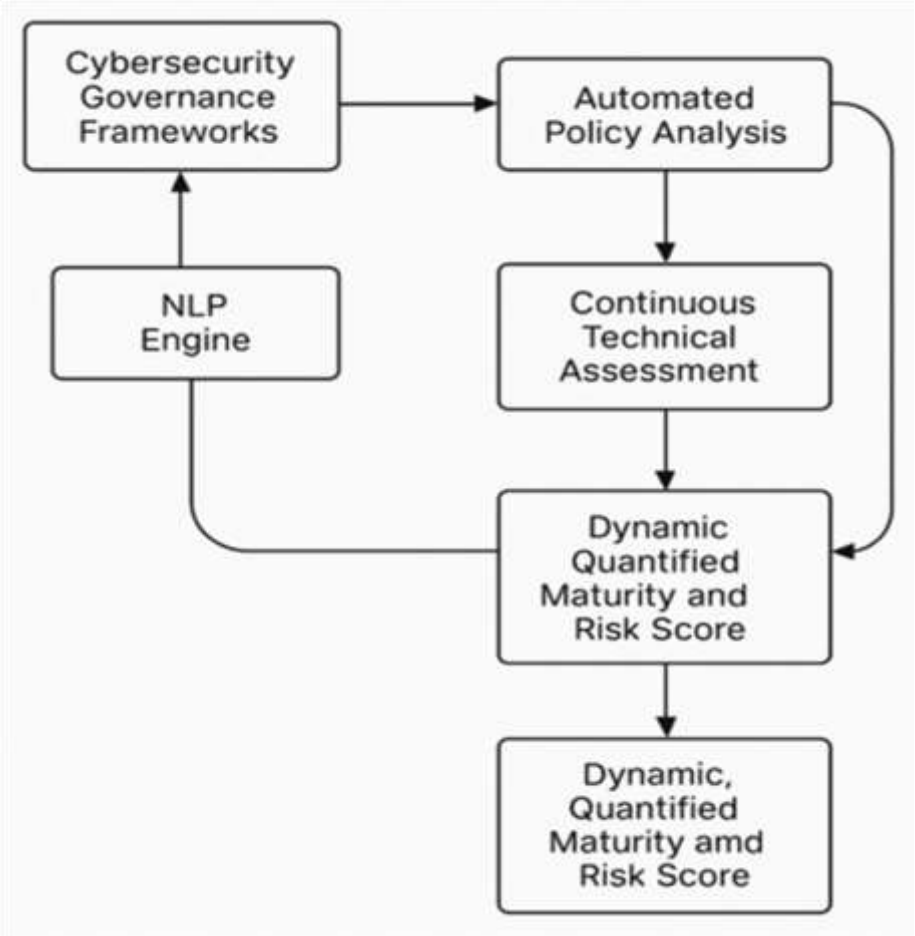

Fig .1 Integrated African Cybersecurity Governance Assessment Model (IACG-AM).

The IACG-AM is a continuous, feedbackdriven AI system designed to move beyond static, checklist-based cybersecurity audits. It provides a living, quantified assessment of an African nation's cybersecurity posture by dynamically aligning its formal governance policies with its technical reality.

4.3.3. Conceptual Model Description of the Integrated African Cybersecurity Governance Assessment Model (IACG-AM)

The diagram conceptually presents an Integrated African Cybersecurity Governance Assessment Model (IACG-AM). The conceptual model illustrates the author's construct and methodology for the IACGAM, presenting the model's core pillars, data flow, and feedback-driven nature. The model is a continuous, feedback-driven system, structured around a central, interconnected flow that begins with policy analysis and culminates in dynamic, actionable insights. It emphasises a continuous cycle, ensuring the assessment remains relevant, updated and effective.

4.4. Theoretical Framework strong validation for the study's conclusions.

The theoretical foundation of this study is the This research establishes a framework for Integrated African Cybersecurity assessing Cybersecurity Governance in Governance Assessment Model (IACG-Africa by integrating a theoretical model with AM). This framework posits that national advanced empirical methodology, providing cyber resilience is a function of seven Ouazzane, 2021). interconnected latent variables, adopting a multi-dimensional perspective of cybersecurity governance that moves beyond purely technical audits (Onwubiko &

TABLE 3. Theoretical Framework

Framework Component	Theoretical Rationale
Multi-Dimensionality	Effective governance requires addressing not only technology but also political, economic, and cultural spheres (Onwubiko & Ouazzane, 2021). This approach addresses limitations found in many static, single-focus maturity models (Lallie, 2025).
Foundational Factors	Legal Aspects provide the necessary policy and compliance environment, acting as the primary deterrent and regulatory mechanism for all governance activities (Rosenzweig, 2012).
Resource Factors	Economic Matters directly relate to resource mobilization and financial investment, which must be adequate to support technical defenses and training (Adekoya et al., 2025).
External Context	The Geo-Political Dimension and Global Blocs Open Issues acknowledge that national cybersecurity is inseparable from international relations, state adversaries, and digital sovereignty debates (Rosenzweig, 2012; Onwubiko & Ouazzane, 2021).
Mechanisms	Mediation and Moderation are included to clarify complex causal pathways. For instance, testing the mediation of Technology helps explain how security culture influences governance, enhancing the model's explanatory power (Byrne, 2010).

4.5 Empirical Framework a mixed-method, hybrid AI approach to rigorously validate the theoretical model and The empirical framework justifies the use of create the functional IACG-AM

.

Methodology	Purpose and Justification
Component	Automated Policy Analysis (NLP) is crucial for analyzing large volumes of unstructured legal and policy text. It translates qualitative "policy intent" into
Validation	quantifiable rules and metrics, overcoming the limitations of manual content analysis (Adhikari et al., 2025; Jin & Mihalcea, 2025).
Causal Testing	Structural Equation Modeling (SEM) is selected as the primary validation tool. It is uniquely suited for testing complex theoretical models involving latent constructs (unobserved variables like 'Cybersecurity Governance')

	and for simultaneously estimating direct and indirect effects (Hoyle, 1995).
Rigorous Testing	SEM enables the testing of the entire theoretical structure as a single system, providing robust Goodness-of-Fit Indices that empirically validate the model, addressing a key criticism of many maturity models (Lallie, 2025).

The model provides a real-time measure of cybersecurity governance in African nations. It operates on three main, interconnected pillars:

i. Automated Policy Analysis: This initial stage focuses on converting a nation's official cybersecurity governance frameworks, such as laws, national strategies, and regulations, from unstructured text into machine-readable rules. An NLP Engine extracts and classifies key controls and requirements, which form the benchmark for all subsequent assessments.

ii. Continuous Technical Assessment: Driven by the rules from the first pillar, this stage involves a continuous, automated scan of the nation's digital infrastructure. It collects real-time data from various sources to validate whether the policies are being effectively implemented in practice. This pillar provides the crucial link between stated policy and operational reality.

iii. Dynamic Risk Quantification: In this final stage, the data from the technical assessment is aggregated and analyzed by an AI/ML Core. The model generates a Dynamic,

Quantifiable Maturity and Risk Score (DAMRS) that provides a clear, actionable view of the nation's cyber posture. This output is not a static report; it is a live metric that can be used to identify governance gaps, prioritize resources, and inform strategic decisions. The results of this analysis then feed back into the system, creating a continuous loop of improvement.

This integrated approach ensures that the assessment is always aligned with both the stated policies and the operational reality of the country's cyber posture

6.1 Core Architecture & Data Flow The model operates on a continuous loop, driven by three interconnected pillars. The following chart illustrates the core data flow and feedback mechanism:

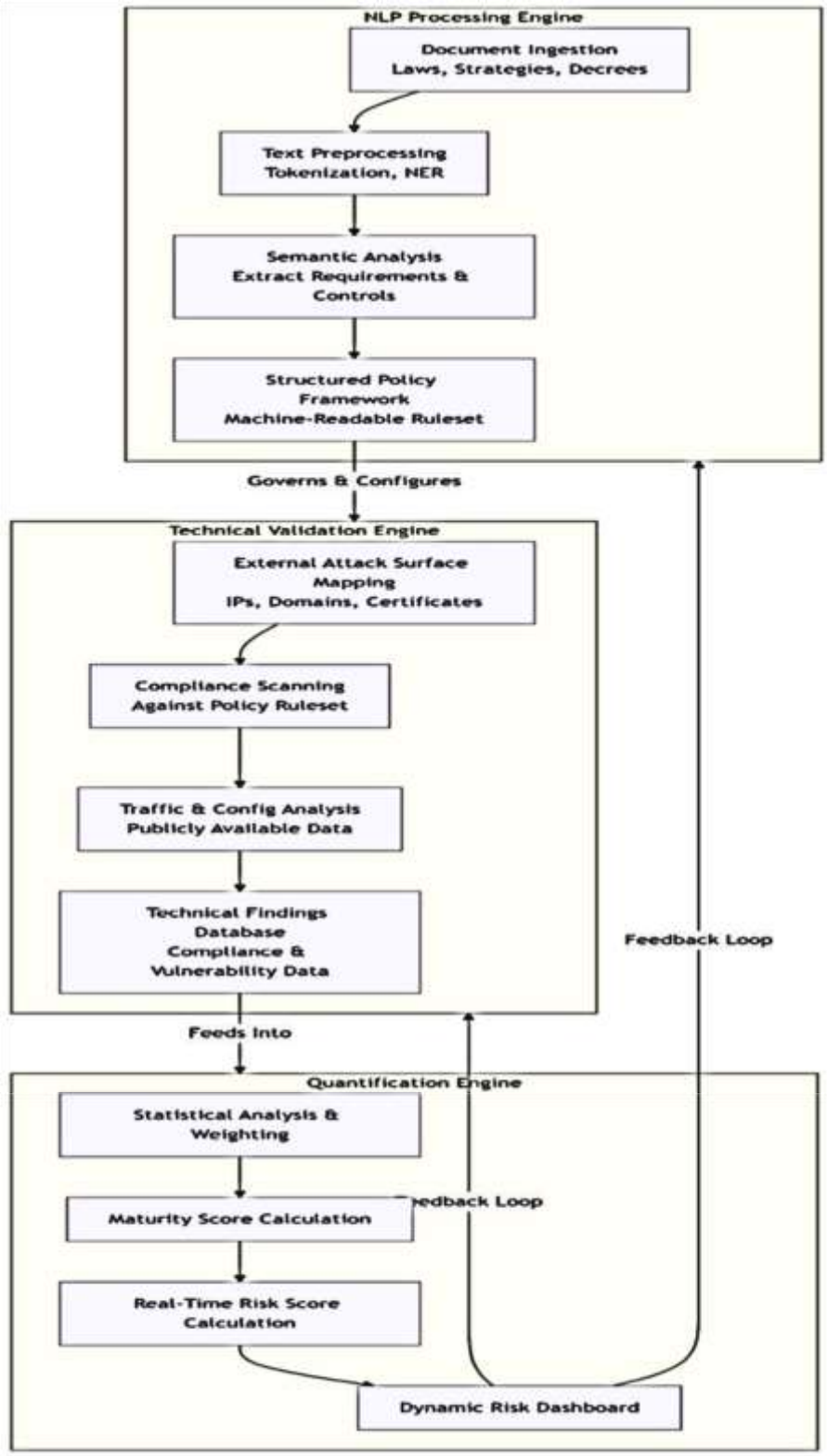

Fig 2 Model Diagram

Pillar 1: Automated Policy Analysis (The "Governance Brain")

This pillar translates unstructured legal and policy documents into a structured, machine-readable ruleset.

- Inputs:

Formal Documents: National cybersecurity strategies, critical infrastructure protection laws, data privacy acts, sector-specific regulations (e.g., for finance, energy), and official implementation decrees.

- International Standards: (For crossreference) NIST CSF, ISO 27001, CIS Controls, etc.
- Core Component: Advanced NLP Engine

Functionality:

Document Ingestion & Preprocessing: Handles PDFs, Word documents, and webscraped text. Performs OCR if needed.

Text Normalization: Tokenization, lemmatization, and removal of boilerplate language.

Named Entity Recognition (NER): Identifies and classifies key entities: ORGANIZATION (e.g., "CERT-NZ", "energy sector"), THREAT (e.g., "ransomware", "statesponsored"), ASSET (e.g., "critical infrastructure", "personal data").

Relation Extraction: Identifies relationships between entities.

For example, it maps a REQUIREMENT to an ORGANIZATION:

a. Sentence: "All banks (ORGANIZATION) must implement (REQUIREM ENT) multi-factor authentication (CONTROL)."

v. Rule Codification: Converts extracted requirements and controls into a structured JSON or SQL format.

Example Output: {entity: "Financial Sector", requirement: "must implement", control: "MFA", standard_ref: "NIST CSF PR.AC.7"}

- Output: A Structured Policy Framework (SPF) - A dynamic knowledge graph of the nation's cybersecurity governance mandates.

Pillar 2: Continuous Technical Assessment (The "Reality Check") This pillar uses the SPF from Pillar 1 to drive automated, large-scale technical assessments of the nation's digital infrastructure.

Inputs:

The Structured Policy Framework (SPF) from Pillar 1.

Target Lists: Nationally scoped IP ranges (ASNs), domain name lists (e.g., .gov.tld, .mil.tld, critical sector domains), and public company registries.

Core Component: Automated Assessment Engine

Methodology:

Discovery & Enumeration: Uses tools like Shodan, Censys, and Amass to discover assets belonging to target IPs and domains.

Policy-Driven Scanning: Configures scanning tools (e.g., Nexpose, Nuclei, O penVAS) based on the controls listed in the SPF. SPF Rule: "All government websites must use HTTPS and support HSTS."

Scanning Logic: Check for port 443, validity of TLS certificates, presence of Strict-Transport-Security header.

iii. Passive Data Analysis: Integrates with public data sources:

a. Certificate Transparency Logs: To discover new/rogue domains.

b. BGP Streams: To detect hijacking events or route leaks.

c. Threat Intelligence Feeds: To correlate discovered assets with known malicious activity.

a) Output: Technical Findings Database - A continuous stream of evidence showing compliance or non-compliance with each rule in the SPF, along with raw vulnerability data.

Pillar 3: Dynamic Risk Quantification
(The "Insight Engine")
This pillar synthesises data from the first two pillars to generate actionable, quantified scores.

- Inputs:
  - The Structured Policy Framework (SPF) from Pillar 1.
  - The Technical Findings Database from Pillar 2.
- Core Component: Quantification

Engine o Methodology:
1. Weight Assignment: Each rule in the SPF is automatically assigned a risk weight based on:
Language
Criticality: " Must" vs.
"Should" vs. "May".
Asset
Criticality: A rule protecting a power grid is weighted higher than one protecting a public blog.
Threat
Severity: Alig ns controls with common threat
frameworks (MITRE
ATT&CK).

2. Maturity Score Calculation: Calculat es a score (0-100) for governance areas (e.g., "Cryptographic Standards", "Incident Response").

 Maturity_Scor e = (∑(Compliant
Findings *
Weight) /
∑(Total
Possible
Findings *
Weight)) *
100

3. Real-Time Risk Score: A composite score reflecting the overall cyber risk posture. It dynamically decreases based on:
The severity and prevalence of discovered technical vulnerabilities.
The criticality of policies that are not being complied with.

4. Trend
Analysis: Tracks scores over time to measure progress or regression.
Output: Dynamic Risk Dashboard

o Visualizations: Interactive charts showing maturity per sector, over time, and against international benchmarks. o Drill-Down Capability: Allows policymakers to click on a low score to see why – e.g., "40% of healthcare websites do not have email security records (DMARC/SPF) configured, as required by Section 4.2 of the National Strategy."

o Actionable Recommendations: AI-generated suggestions for remediation, policy clarification, or investment priorities.

6.2 Implementation Considerations & Challenges

i. Data Sensitivity: The model is designed to operate primarily on publicly available information: laws, policies, and non-intrusively gathered technical data (public scan data, certificate logs, etc.). This avoids legal and ethical issues around classified information.
ii. Bias and Interpretation: The NLP model must be meticulously trained and validated on legal and technical texts to avoid misinterpreting nuanced policy language. Human-inthe-loop review is crucial initially.
iii. Adaptability: The model must be adaptable to different national contexts, legal systems, and writing styles. Modular design allows for country-specific NLP models and policy templates.

- Performance: Scanning an entire nation's IP space is computationally expensive. Requires a cloud-native, scalable architecture with efficient scanning schedulers to avoid causing network disruptions.

The IACG-AM provides a transformative approach to cybersecurity governance. By creating a closed-loop system between policy intent and technical reality, it enables nations to:

i. Move from periodic, subjective audits to continuous, objective measurement.
ii. Prioritize investments and actions based on quantified risk and actual compliance gaps.
iii. Demonstrate accountability and progress to citizens and international partners.
iv. Proactively strengthen their national cyber defense by understanding the gaps between their policies and their digital reality.

6.3. Component 2: Real-time Technical Control Assessment

This component is the link between policy and practice. The extracted rules from the NLP engine are translated into automated checks for a continuous monitoring system. The model continuously collects and analyzes data from a nation's digital estate, including network traffic, system configurations, and user logs.[30] It uses AI and ML to detect anomalies and identify deviations from the baselines and security controls mandated by the governance policies.[5]

Key functions of this component include:

- Anomaly Detection: The model identifies unusual behavior that could indicate a zero-day attack or unauthorized access, something a static audit would miss.[5]
- Automated Policy Enforcement: It can automatically scan for compliance with technical mandates, such as the implementation of encryption, access controls, or multi-factor authentication, as specified in the policy texts.[17] For example, if the Malabo Convention requires data to be stored securely, the model can automatically verify that encryption and access controls are in place on relevant systems.[17]

This continuous data collection and analysis enable a transition from periodic risk assessments to a dynamic, continuous process, empowering security teams with the tools to stay ahead in a volatile threat landscape.[30]

6.4 Component 3: Dynamic Maturity and Risk Quantification

The final component translates the data from the first two pillars into an actionable, quantitative score. This process moves beyond the subjective, high-level tiers of traditional models to provide a more objective, data-driven assessment. The model generates a dynamic maturity score based on real-time data, providing clear indicators of progress toward a set of objectives.[28] It quantifies risk by correlating identified vulnerabilities with the policies and assets they affect.[30] This allows decision-makers to see "where exactly we are most exposed right now," rather than just receiving a generic maturity rating.[27]

This model can help close the security reporting gap between technical teams and executives. Traditional reports often provide executives with "long lists of technical issues and low-level findings" that are not useful for strategic decision-making.[6] These reports also often lack consistency and a uniform quantification method.[40] The proposed AI model, by integrating a "centralized knowledge base" of policies and a "risk and controls analysis" engine, can generate reports tailored for different audiences.[30] It quantifies risk based on correlated data and ML algorithms, providing a more objective and consistent method for reporting.[30] This allows executives to receive actionable insights that "relate to changing business risks," enabling them to justify investments and make informed decisions

Table 4: Cybersecurity Governance Maturity Tiers for AI Assessment

Tier Name	Key Characteristics	AI Model Indicators
Foundational	Ad hoc responses; security practices are reactive and manual.	Policies are not analyzed or linked to controls; technical assessment is ad hoc, with no consistent data collection or reporting.
Emerging	Some security policies are in place, but enforcement is inconsistent.	Policies are analyzed and controls are extracted, but the link to real-time technical monitoring is limited or inconsistent.
Optimized	Security is policy-driven; continuous monitoring and some automation are in use.	Policies and controls are linked and monitored in near real-time; deviations from policy are flagged and reported
Adaptive	Fully integrated governance; the system is predictive and self-improving.	Policies and controls are fully integrated with real-time monitoring; the AI model uses predictive analytics to anticipate threats and automatically adjust controls

VII EMPIRICAL FRAMEWORK

7.1 Structural Equation Modeling (SEM)

Analysis for the Cybersecurity Governance Mode Structural Equation Modeling (SEM) is a highly suitable statistical method for empirically validating the proposed Cybersecurity Governance Model. Given the model's complexity, which involves multiple independent, dependent, and unobserved variables, SEM provides a robust framework for simultaneous hypothesis testing (Byrne, 2016).[1] This method is superior to traditional statistical techniques like regression because it accounts for measurement error in both independent and dependent variables and can analyze a system of complex relationships, including mediation and moderation, in a single, comprehensive model (Hair et al., 2017).[2]The model is represented by a series of equations, which are divided into two main components: the measurement model and the structural model.

7.2 The Measurement Model

The measurement model links the latent (unobserved) variables to their observed indicators (the measurable metrics).[3] Each observed variable ([4]xi for independent, [5]yi for dependent) is a function of its corresponding latent variable and a unique measurement error.[6]

- Independent Latent Variables:

$x_i = \lambda_i \xi_j + \delta_i$

○ xi: Observed indicator (e.g., Threat, Investment).

○ ξ_j: Latent independent variable (e.g., Risk Assessment, Economic Matters).

○ λ_i: Factor loading, representing the strength of the relationship between the observed and latent variable.[7]

○ δ_i: Measurement error for the observed indicator.

- Dependent Latent Variable: $y_i = \lambda_i \eta_1 + \epsilon_i$

○ yi: Observed indicator of governance (e.g., Maturity Score, Policy Compliance).
○ η1: The latent dependent variable, Cybersecurity Governance.
○ λi: Factor loading.[8]
○ ϵi: Measurement error.

7.3 The Structural Model

The structural model tests the hypothesised causal relationships between the latent variables.[9] The primary equation for the dependent variable is:

$\eta 1=\gamma 11\xi 1+\gamma 12\xi 2+\gamma 13\xi 3+\gamma 14\xi 4+\gamma 15\xi 5+\gamma 16\ \xi 6+\gamma 17\xi 7+\zeta 1$

- η1: Latent dependent variable, Cybersecurity Governance.
- ξ1 through ξ7: The seven latent independent variables (Risk Assessment, Legal, Economic, GeoPolitical, Technology, Cultural, Global Blocs).
- γ1j: Path coefficients, quantifying the direct effect of each independent variable on Cybersecurity Governance. A statistically significant γ value confirms the existence and strength of the relationship.
- ζ1: The residual error in the structural equation.

7.4. Mediating and Moderating Effects

SEM allows for the precise quantification of indirect effects, which provides a more nuanced understanding of the model's dynamics.[10]

 Mediation: The proposed model explores the mediation of the relationship between Cultural Aspects (ξ6) and Cybersecurity
Governance (η1) by Technology (ξ5). This is represented by a two-step process:
Step 1: Technology is treated as a dependent variable of Cultural Aspects. $\xi 5=\gamma 56\xi 6+\zeta 5$
○ γ56: The path coefficient representing the effect of Cultural Aspects on Technology.
Step 2: The total effect of Cultural Aspects on Cybersecurity
Governance is decomposed into a direct effect and an indirect effect.
○ Direct Effect: γ16 (as shown in the main structural equation).
○ Indirect Effect: The product of the paths from Cultural Aspects to Technology and from Technology to Cybersecurity Governance. The indirect effect is calculated as (γ56)×(γ15). A significant indirect effect would provide strong empirical evidence that improved cultural aspects lead to better technology adoption, which in turn enhances governance.

 Moderation: The model proposes that the relationship between Economic Matters (ξ3) and Cybersecurity Governance (η1) is moderated by the Geo-Political Dimension (ξ4). This is tested by including an interaction term in the structural equation: $\eta 1=\ldots+\gamma 13\xi 3+\gamma 14\xi 4+\gamma 1(3\times 4)(\xi 3\times \xi 4)+\ldots$
○ γ1(3×4): The coefficient for the interaction term. A statistically significant value for this coefficient indicates a moderating effect. A positive value would mean that the positive effect of Economic Matters on governance is strengthened in a more volatile geo-political environment, while a negative value would indicate a weakening effect.

7.5. Correlations Among Independent Variables

The SEM will also estimate the correlations between the seven independent latent variables, denoted by the covariance term ψij . For example, the covariance between Legal Aspects (ξ2) and Economic Matters (ξ3) (ψ23) will be a key part of the analysis. A significant positive correlation here would confirm that nations with more developed legal frameworks for cybersecurity also tend to have greater economic investment in the sector, as is hypothesised in the model.

7.6 Empirical Justification

This SEM analysis provides a rigorous statistical foundation for the proposed research findings. By simultaneously testing the measurement and structural models, it will not only confirm the existence of the hypothesized relationships between the independent variables and Cybersecurity Governance but also quantify their strength through the path coefficients (γ). Furthermore, the analysis will clarify the intricate mechanisms of mediation and moderation, providing a deeper understanding of the factors that truly drive effective

cybersecurity governance in Africa. This empirical validation will provide a robust basis for the policy recommendations and theoretical contributions of the research paper.

8. **Discussion: Addressing African** Realities and Implications

The proposed framework is not merely a technical solution; it is a tool for addressing Africa's unique challenges and advancing its digital sovereignty agenda. By moving beyond a one-size-fits-all approach, the model can be configured to address the continent's specific realities.

8.1. Addressing African-Specific Challenges with the Proposed Model

The model directly addresses several of the continent's most pressing challenges. In response to data scarcity and bias, the model

can be designed to use local, representative to mitigate the impact of the talent gap by datasets and focus on federated learning and enabling a small number of experts to have a data-visiting models.[41] This ensures that data much larger impact.

remains localized and avoids the risks associated with external sharing and third- Most importantly, the framework directly party attacks.38 The model's ability to be supports the digital sovereignty agenda by trained on local data is critical for ensuring enabling nations to assess and enforce their that AI systems are ethically aligned and do own governance frameworks, rather than not perpetuate the biases of models relying on external, potentially biased, developed outside the continent.11 Western-centric models.[13] It empowers Furthermore, the framework's reliance on AI African nations to take ownership of their and automation reduces the need for constant digital future by providing them with a tool human intervention, which is critical in to measure their progress from "digital regions with a skills gap and under-resourced consumption to digital capability".10 research ecosystems.[25] This approach serves

Table 5: Challenges in African Cybersecurity and Solutions from the Proposed AI Model

African Challenge	Problem Description	Proposed Model's Solution
Digital Colonialism [13]	Data extraction by foreign tech companies; reliance on external, Western-centric frameworks.	Promotes local data retention and processing; allows nations to measure and enforce their own governance standards based on their unique policies.
Data Scarcity and Bias 11	Lack of local datasets leads to AI models with representational biases and limited utility.	Can be trained on local, representative datasets; utilizes federated learning to allow training without exporting sensitive data.[41]
Regulatory Fragmentation [15]	Inconsistent national laws leave individual countries vulnerable and unable to coordinate a unified response.	The NLP component can help harmonize laws by identifying and flagging inconsistencies between national and regional frameworks.[37]
Skills Gap [11]	Shortage of AI experts and cybersecurity professionals to develop and maintain systems.	Automates manual assessment tasks, reducing the need for extensive human resources and allowing a small team to have a broad impact.

8.2. Ethical Considerations and the African Context

The development and deployment of this AI model must be guided by principles that reflect African moral traditions and values, such as Ubuntu, which emphasizes community, interdependence, and collective benefit.[41] This involves ensuring the model is fair, transparent, accountable, and respects human rights and dignity.[41] The AI must be built "with Africa, by Africa, and for Africa" to avoid embedding biases and to ensure it serves local needs and priorities.[19] This ethical alignment is paramount to prevent the framework from inadvertently reinforcing existing societal inequalities or facilitating pervasive surveillance, which are significant risks of AI.[10] The model must also be transparent enough to be understandable and auditable, as the "black box" nature of many AI systems can create ambiguity around accountability.[43] By integrating these ethical safeguards from the design phase, the framework can become a trustworthy tool for advancing a truly African-centric digital future.

9. **Conclusion and Future Work**

9.1. Summary of Findings and Contributions

This paper has detailed the limitations of traditional cybersecurity governance assessments, highlighting their inadequacy in a dynamic threat environment. These manual, periodic, and subjective methods are unable to provide the real-time, objective, and scalable insights needed to manage modern cyber risks. A fundamental paradox was revealed: a high-level maturity rating does not guarantee low risk, as granular vulnerabilities can be obscured by an aggregated score.

To overcome these shortcomings, a novel, AI-powered framework was proposed. The hybrid model uses NLP for the automated analysis of a nation's policy documents, translates these policies into a continuous technical monitoring system, and quantifies the results into a dynamic maturity and risk score. This framework offers a superior, more scalable, and more accurate approach to measuring governance maturity. By specifically addressing the unique challenges of the African continent—from infrastructure gaps and data scarcity to the strategic imperative of digital sovereignty—the framework provides a practical tool for building long-term cyber resilience.

9.2. Limitations and Future Research

While the proposed framework offers a powerful conceptual solution, it is important to acknowledge that it remains a theoretical model. Future work will involve building a prototype and testing it with a pilot case study in a specific African country, such as Nigeria or South Africa. The effectiveness of the model is contingent on access to reliable and representative data, and addressing data scarcity remains a significant challenge that requires further research into effective datasharing and data-visiting models. Furthermore, future research is needed to refine the AI's ability to handle the nuances of human-centric legal and policy language and to ensure the ethical alignment of the algorithms with the diverse cultural values of the continent.

REFERENCES

[1] Byrne, B. M. (2010). Structural equation modeling with AMOS: Basic concepts, applications, and programming. Routledge[1].

[2] Rosenzweig, P. (2012). The International Governance Framework for Cybersecurity.
Canada-United States Law Journal, 37(2), 405–420[2].

[3] Hair, J. F., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). Multivariate Data Analysis (7th ed.). Pearson Education[3].

[4] Fielder, A., & Brogi, L. (2020). Cybersecurity as a holistic approach encompassing people, processes, and technology. In Proceedings of the 2020
International Conference on Computer Science and Information Technology (pp. 45–51)[4].

[5] Onwubiko, C., & Ouazzane, K. (2021). Multidimensional Cybersecurity Framework for Strategic Foresight. Intl. Journal on Cyber Situational Awareness , 6(1), 47–64[5]. e-Governance Academy. (2022).

[6] NATIONAL CYBERSECURITY STRATEGY. https://ega.ee/wpcontent/uploads/2022/08/Ugandan-nationalcybersecurity-strategy.pdf[6].

[7] Adekoya, O. A., Atlam, H. F., & Lallie, H. S. (2025). Quantifying the Multidimensional Impact of Cyber Attacks in Digital Financial Services: A Systematic Literature Review. International Journal of Computer Science and Network Security, 25(1), 101–115[7].

[8] Adhikari, A., Das, S., & Dewri, R. (2025).
Natural Language Processing of Privacy Policies: A Survey. arXiv preprint arXiv:2501.10319[8].

[9] AI4D Africa. (2025). AI Sovereignty in Africa. Retrieved September 16, 2025, from https://www.ai4d.ai/blog/ai-sovereignty-inafrica[9].

[10] Baobab Consulting. (2025). The Current State of Cybersecurity in Africa: Potential Threats and Mitigation Recommendations. Retrieved September 16, 2025, from https://baobab-consulting.net/en/he-currentstate-of-cybersecurity-in-africa-potentialthreats-and-mitigation-recommendations/[10].

[11] BDO. (2025). Cybersecurity governance and information governance (incl. Data privacy). Retrieved September 16, 2025, from https://www.bdo.co.za/enza/services/advisory/cyber-securityen/cybersecurity-governance-andinformation-governance-(incl-data-privacy[11].

[12] Carnegie Endowment for International
Peace. (2025). Understanding Africa's AI
Governance Landscape: Insights From
Policy Practice and Dialogue. Retrieved September 16, 2025, from https://carnegieendowment.org/posts/2025/09/understanding-africas-ai-governancelandscape-insights-from-policy-practiceand-dialogue?lang=en[12].

[13] Center for Global Development. (2025). Data Localization: A "Tax" on the Poor. Retrieved September 16, 2025, from https://www.cgdev.org/sites/default/files/dat a-localization-tax-poor.pdf[13].

[14] Centre for Intellectual Property and Information Technology Law. (2025).
ETHICAL AI DEVELOPMENT IN AFRICA: INTEGRATING CULTURAL VALUES AND ADDRESSING GLOBAL DISPARITIES.
Retrieved September 16, 2025, from https://cipit.org/ethical-ai-development-inafrica-integrating-cultural-values-andaddressing-global-disparities/[14].

[15] CMU-Africa. (2025). Water consumption of African data centers in the age of AI. Retrieved September 16, 2025, from https://www.africa.engineering.cmu.edu/new s/2025/08/13-water-efficiency.html[15].

[16][CyberSaint. (2025). Benefits Of An Automated Security Risk Assessment. Retrieved September 16, 2025, from https://www.cybersaint.io/blog/benefits-ofan-automated-security-risk-assessment[16].

[17]Cybersecurity Hub. (2025).
CyberSecurity Hub: HOME. Retrieved September 16, 2025, from https://www.cybersecurityhub.gov.za/[17].

[18] CIO VIEWS. (2025). Top 3 Challenges with Measuring Cybersecurity. Retrieved September 16, 2025, from https://cioviews.com/top-3-challenges-withmeasuring-cybersecurity/[18].

[19]Darktrace. (2025). AI Maturity Model: A
Roadmap for Security. Retrieved September 16, 2025, from https://www.darktrace.com/blog/introducingthe-ai-maturity-model-for-cybersecurity[19]. [21] Diplomacy.edu. (2025). Cybersecurity, cybercrime & COP in Africa: National approaches. Retrieved September 16,
2025, from http s://www.diplomacy.edu/resource/reportstronger-digital-voices-fromafrica/cybersecurity-cybercrime-cop-inafrica-nationalapproaches/#:~:text=South%20Africa's%20 National%20Cybersecurity%20Policy,the%20secure%20use%20of%20ICTs. [20].

[22]Empowered Systems. (2025).
Automating Security Risk Assessments: A
Comprehensive Guide. Retrieved September 16, 2025, from
https://empoweredsystems.com/blog/autom ating-security-risk-assessments-acomprehensive-guide/[21].

[23]Extensia Ltd. (2025). Nigeria prepares cybersecurity regulatory framework for telecoms sector. Retrieved September 16,
2025, from
https://extensia.tech/nigeria-preparescybersecurity-regulatory-framework-fortelecoms-sector/ [22].

[24] Fortinet. (2025). Artificial Intelligence (AI) in Cybersecurity: The Future of Threat Defense. Retrieved September 16, 2025, from https://www.fortinet.com/resources/cyberglo ssary/artificial-intelligence-incybersecurity[23].

[25] The Future of Privacy Forum. (2025). The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation. Retrieved September 16, 2025, from https://fpf.org/blog/global/the-african-unionscontinental-ai-strategy-data-protection-andgovernance-laws-set-to-play-a-key-role-inai-regulation/[24].

[26] Huntsman. (2025). Challenges in Cyber Security Auditing. Retrieved September 16, 2025, from https://huntsmansecurity.com/blog/challeng es-in-cyber-security-auditing/[25].

iAfrica.com. (2025). Africa Pushes For Ethical AI Governance To Build Digital Sovereignty And Inclusive Development. Retrieved September 16, 2025, from https://iafrica.com/africa-pushes-for-ethicalai-governance-to-build-digital-sovereigntyand-inclusive-development/[26].

[27]IFE. (2025). 2nd International Conference on Digital Sovereignty (ICDS) 2025. Retrieved September 16, 2025, from https://ife.no/en/event/internationalconference-on-digital-sovereignty-icds2025/[27].

[28]ijrpr. (2025). AI-Enhanced Cybersecurity Audits in IT Governance: Strengthening Risk Management, Compliance, and Threat Intelligence. Retrieved September 16, 2025, from https://ijrpr.com/uploads/V6ISSUE2/IJRPR3 8545.pdf[28].

[29]Jin, Z., & Mihalcea, R. (2025). Natural Language Processing for Policymaking. In Artificial Intelligence in Policy and Governance. Springer[29].

[30] Ksolves. (2025). Enhancing Legal Document Analysis with NLP. Retrieved September 16, 2025, from https://www.ksolves.com/blog/artificialintelligence/nlp-legal-document-analysis[30]. [31]Lallie, H. S. (2025). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. Applied Sciences, 13(1), 52[31].

[32] Michalsons. (2025). AU Convention on Cyber Security and Personal Data Protection .... Retrieved September 16, 2025, from https://www.michalsons.com/blog/auconvention-on-cyber-security-and-personaldata-protection-malabo-convention/65281[32].

[33] Netguru. (2025). Lower Data Breaches and Security Risks with Local Language Models. Retrieved September 16, 2025, from https://www.netguru.com/blog/lower-databreaches-and-security-risks-with-locallanguage-models[33].

[34] New America. (2025). Africa's Digital Sovereignty Trap: Breaking the Data Center Development Deadlock. Retrieved September 16, 2025, from https://www.newamerica.org/planetarypolitics/briefs/africas-digital-sovereigntytrap/[34].

[35]Palo Alto Networks. (2025). AI Risk Management Framework. Retrieved September 16, 2025, from https://www.paloaltonetworks.com/cyberped ia/ai-risk-management-framework[35].

[36] Peltola, M. (2025). Motolani Peltola: "The pursuit of digital sovereignty and local data ownership has implications for local capacity development". GEG. Retrieved September 16, 2025, from https://www.geg.ox.ac.uk/content/motolanipeltola-pursuit-digital-sovereignty-and-localdata-ownership-has-implications [36]. [37] Prey Project. (2025). Implementing a Cybersecurity Assessment Framework. Retrieved September 16, 2025, from https://preyproject.com/blog/cybersecurityassessment-framework[37].

[38]Prey Project. (2025). Cybersecurity frameworks 101. Retrieved September 16, 2025, from

https://preyproject.com/blog/cybersecurityframeworks-101#:~:text=The%20best%20cybersecurity %20frameworks%20to,tailored%20to%20specific%20organizational%20needs.[38].
[39]ResearchGate. (2025). (PDF) Natural Language Processing (NLP) for Document Analysis. Retrieved September 16, 2025, from https://www.researchgate.net/publication/39 0941525 _Natural_Language_Processing_NLP_for_Document_Analysis[39].
[40]SailPoint. (2025). Machine learning (ML) in cybersecurity. Retrieved September 16, 2025, from https://www.sailpoint.com/identitylibrary/how-ai-and-machine-learning-areimproving-cybersecurity[40].
[41] Scirp.org. (2025). Challenges of Technology in African Countries: A Case Study of Zambia. Retrieved September 16, 2025, from https://www.scirp.org/journal/paperinformati on?paperid=129992[41].
[42]Scribbr. (2025). Mediator vs. Moderator Variables | Differences & Examples. Retrieved September 16, 2025, from https://www.scribbr.com/methodology/media tor-vs-moderator/[42].
Scribbr. (2025). www.scribbr.com. Retrieved September 16, 2025, from https://www.scribbr.com/methodology/media tor-vs-moderator/#:~:text=Revised%20on%20June %2022%2C%202023,and%20direction%20 of%20that%20relationship.[43].
[43]Sprinto. (2025). When Cyber Threats Outrun the Playbook: The Limits of NIST CSF. Retrieved September 16, 2025, from https://sprinto.com/blog/limitations-of-nistcsf/[44].
[44]The CPA Journal. (2025). Metrics or Maturities. Retrieved September 16, 2025, from https://www.cpajournal.com/2025/06/24/met rics-or-maturities/ [45].
arXiv. (2025). Themed Challenges to Solve Data Scarcity in Africa: A Proposition for Increasing Local Data Collection and Integration. Retrieved September 16, 2025, from https://arxiv.org/html/2508.00925v1 [46].
[45] T20 South Africa. (2025). From digital dependence to digital sovereignty: South Africa's G20 opportunity in the age of AI. Retrieved September 16, 2025, from https://t20southafrica.org/commentaries/fro m-digital-dependence-to-digital-sovereigntysouth-africas-g20-opportunity-in-the-age-ofai/[47].
[46] University of Cambridge. (2025). Artificial intelligence, digital colonialism, and the implications for Africa's future development. Data & Policy. Retrieved September 16, 2025, from https://www.cambridge.org/core/journals/dat a-and-policy/article/artificial-intelligencedigital-colonialism-and-the-implications-forafricas-future-development/4BD73E9129A9CD9E9301C6 1CB2401450[48].
[47] University of Michigan. (2025). Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. Retrieved September 16, 2025, from https://repository.law.umich.edu/mjrl/vol24/is s2/6/[49].
[48] Wikipedia. (2025). Malabo Convention. Retrieved September 16, 2025, from https://en.wikipedia.org/wiki/Malabo_Conve ntion[50].
[49] Zscaler. (2025). AI vs. Traditional Cybersecurity: Which Is More Effective?. Retrieved September 16, 2025, from https://www.zscaler.com/zpedia/ai-vstraditional-cybersecurity[51].
[50] Zscaler. (2025). www.zscaler.com. Retrieved September 16, 2025, from https://www.zscaler.com/zpedia/ai-vstraditionalcybersecurity#:~:text=While%20traditional% 20 approaches%20rely%20on,mitigate%20threats%20in%20real%20time.[52].