Background Paper for UN IGF 2026 Workshop Proposal

AI-SENTINEL AS A MULTISTAKEHOLDER PATH TO CYBER SOVEREIGNTY

Supporting Background Material on AI-Sentinel Africa, Adaptive Cybersecurity Governance and Cyber Sovereignty for the Global South

Authored by:

Olusegun H. Olugbile

President, Global Network for Cybersolution
Founder/Author, AI-Sentinel Africa
Developer, Adaptive Cybersecurity Governance Model Framework

Submitted by:
Global Network for Cybersolution

With the Support of the Centre for Cyberspace Studies, Nasarawa State University and the United Nations Economic Commission for Africa (UNECA) as UN-IGF Proposed Workshop Co-organisers

Date: July 2026

Authorship and Intellectual Property Notice

This background material was authored by Dr. Segun H. Olugbile in support of the UN IGF 2026 workshop proposal titled “AI-Sentinel as a Multistakeholder Path to Cyber Sovereignty.” The AI-Sentinel concept, Adaptive Cybersecurity Governance Model-derived framework, taxonomy, indicators, governance logic and related architecture are the intellectual property of Olusegun Hamed Olugbile[1]. This document is submitted for policy discussion, peer review, workshop background and multistakeholder engagement purposes only. No part of the proprietary model, framework, indicators or architecture may be reproduced, adapted, commercialised or implemented without prior written permission of the author and copyright owner.

[1] *© 2026 Olusegun Hamed Olugbile. All rights reserved. AI-Sentinel Africa and ACGM-derived framework.*

1.0 Purpose of the Background Material

This background material supports the workshop proposal titled *AI-Sentinel as a Multistakeholder Path to Cyber Sovereignty***.** It provides the policy, empirical, and governance rationale for discussing AI-Sentinel Africa as a federated, rights-preserving, and human-in-the-loop model for cyber sovereignty, digital trust, AI safety, and resilient digital public infrastructure in Africa and the wider Global South.

The material is designed to accompany the UN IGF 2026 workshop submission as a concise supporting document. The IGF 2026 workshop form allows background documentation to be uploaded as a PDF with a maximum file size of 2 MB, and the review process emphasises topic relevance, workshop content, policy questions, engagement strategy, and diversity.

2.0 Context: Why Cyber Sovereignty Now?

Africa's digital future is increasingly shaped by artificial intelligence, mobile connectivity, digital public infrastructure, fintech, cloud services, e-commerce, digital identity, data flows and platform-mediated public services. These systems expand opportunity, but they also create new forms of dependency, exposure and institutional risk. Cyber sovereignty, in this context, does not mean digital isolation. It means the capacity of societies, institutions and states to govern cyber risk, protect citizens, preserve rights, control sensitive data, sustain critical digital services and cooperate across borders on fair and accountable terms.

The scale of the governance challenge is significant. The International Telecommunication Union reported that almost three-quarters of the world's population were online in 2025, while 2.2 billion people remained offline, mostly in low- and middle-income countries. Mobile broadband coverage is nearly universal globally, but quality, affordability, and meaningful use gaps persist (ITU, 2025). This is directly relevant to Africa, where digital inclusion and cyber resilience must be designed together rather than treated as separate policy agendas.

Africa's connectivity model is also heavily dependent on mobile networks. ITU data show 56 mobile broadband subscriptions per 100 inhabitants in Africa, compared with 132 per 100 inhabitants in the Americas. In addition, while 5G accounts for 36% of mobile broadband subscriptions globally, in Africa and the CIS region, there are two or fewer 5G subscriptions per 100 mobile broadband subscriptions (ITU, 2025). This means African cyber governance must address mobile-first risks, legacy infrastructure, uneven broadband quality, low-bandwidth environments, and emerging 5G/AI adoption simultaneously.

Cross-reference: *This context directly supports Policy Question 1, which asks how multistakeholder Internet governance can help African and Global South countries*

achieve cyber sovereignty without weakening openness, rights and cross-border cooperation.

3.0 Africa's Digital Economy and Cyber Risk Exposure

Mobile technology is now central to Africa's digital economy. GSMA reports that mobile technologies and services contributed approximately US$240 billion to Africa's economy in 2025, equivalent to 7.8% of GDP, and that this contribution is forecast to reach US$290 billion by 2030 (GSMA, 2026). At the same time, the GSMA notes that almost 1 billion people in Africa still do not use mobile Internet, representing about 63% of the population. This creates a dual policy challenge: protecting those already participating in the digital economy while ensuring that cybersecurity requirements do not exclude citizens, micro-enterprises, informal markets, women, youth and rural communities.

The World Bank's Digital Economy for Africa initiative similarly warns that Africa can harness the digital economy as a driver of growth and innovation, but failure to bridge the digital divide risks economic isolation and stagnation. It also highlights the need for governments to invest more strategically in digital infrastructure, services, skills and entrepreneurship (World Bank, 2026).

The policy implication is clear: cybersecurity governance cannot be limited to national security agencies, banks and telecoms. It must also become part of economic inclusion, consumer protection, digital public infrastructure governance, data protection and Internet governance.

Cross-reference: *This supports the workshop outcome on creating a checklist of deployable indicators across the seven ACGM pillars, especially the economic, cultural, technology and legal pillars*.

4.0 Cybercrime Trends: From Technical Threats to Governance Failure

Cybercrime is now a major public policy, economic and law-enforcement challenge across Africa. INTERPOL's 2025 Africa Cyberthreat Assessment reported that cybercrime accounts for more than 30% of all reported crime in Western and Eastern Africa. It also identified online scams, ransomware, business email compromise and digital sextortion as the most reported cyberthreats, while 90% of African countries reported needing significant improvement in law enforcement or prosecution capacity (INTERPOL, 2025).

This evidence shows that Africa's cyber challenge is no longer only about technical protection of networks. It is also about institutional coordination, legal capacity, cross-border cooperation, evidence handling, citizen protection, public trust and economic stability. INTERPOL's Cybercrime Director also emphasised that no single agency or

country can address these challenges alone, reinforcing the need for multistakeholder governance, regional cooperation and public-private coordination (INTERPOL, 2025).

AI-enabled fraud further complicates the problem. Generative AI can lower the cost of phishing, impersonation, automated scams, synthetic identity fraud, deepfake abuse and social engineering. In African contexts where digital literacy, law-enforcement capacity and institutional coordination vary widely, AI-enabled cybercrime can scale faster than conventional policy response cycles.

Cross-reference: *This supports Policy Question 3, which asks how AI-assisted, federated and human-in-the-loop cyber governance systems can support cooperation while preventing surveillance, exclusion, dependency and regulatory fragmentation*.

5.0 Legal and Data Protection Landscape

Africa has made important progress in cybersecurity and data protection law, but enforcement and harmonisation remain uneven. The African Union Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, was adopted in 2014 and entered into force on 8 June 2023, after the deposit of the fifteenth instrument of ratification. The African Union status list records 55 AU countries, with 21 signatures, 20 ratifications and 20 deposits as reflected in the treaty status document (African Union, 2023).

At the national level, data protection laws are expanding. Code for Africa reported that, by the end of 2025, 44 African countries had enacted data protection laws, covering about 80% of AU member states, and 38 countries had fully operational data protection authorities, up from 34 a year earlier (Code for Africa, 2026). However, the same analysis notes that capacity, funding and coordination gaps remain, meaning that legal adoption does not automatically translate into practical protection or regulatory maturity.

This legal landscape creates a strong case for AI-Sentinel's proposed regulatory interoperability and deployable indicator approach. African countries need a governance system that can map laws, sector rules, standards, data residency obligations, cyber incident responsibilities and institutional mandates into operational decision support.

Cross-reference: *This supports the legal pillar of the Cybersecurity Governance Variables Framework and the expected output on sovereign resilience indicators*.

6.0 Cybersecurity Capacity and the Need for Measurable Governance

The ITU Global Cybersecurity Index measures country-level cybersecurity commitment across five pillars: legal measures, technical measures, organisational measures, capacity development and cooperation (ITU, 2024). The ITU states that

cybersecurity cuts across industries and sectors, and that national engagement is assessed across these pillars before being aggregated into an overall score (ITU, 2024).

This is highly relevant to AI-Sentinel. While the ITU GCI provides a global reference point for cybersecurity commitment, AI-Sentinel is designed to extend the governance logic into a more adaptive, Africa-focused and operational framework. Its seven ACGM-derived pillars; risk assessment, cultural factors, technology, geopolitical factors, economic factors, gaps across global blocs and legal factors; provide a more context-sensitive basis for assessing African cybersecurity governance across national systems, sectors and communities.

The seven derived pillars are derived from the *Adaptive Cybersecurity Governance Model (ACGM) for an Interconnected Society*, a research-based study conducted at a University. The derivative AI-Sentinel documentation states that the Cybersecurity Governance Variables Framework organises the significant independent governance variables used in the ACGM study into seven deployable pillars, supported by measurable indicators for assessment, alignment, execution and evaluation[2]. The documentation further identifies the empirical foundation of the model, including R^2 = 0.64 and SEM pillar-weighting logic, as the basis for translating the ACGM into AI-Sentinel's adaptive cyber governance architecture.

The model explains 64% of the observed variation in the cybersecurity governance outcome measured in the study. While the $R^2 = 0.64$ means that the ACGM explains a substantial share of the governance conditions that shape cybersecurity resilience, in practical terms, the model shows that cyber resilience is not determined by technology alone; it is strongly influenced by legal readiness, institutional coordination, cultural behaviour, economic capacity, geopolitical exposure, risk assessment, and global digital power dynamics. The remaining unexplained variation reflects local context, emerging threats, institutional politics, funding constraints, and other factors that must still be considered by human decision-makers.

The *SEM pillar weighting* means the model uses empirical relationships to estimate each pillar's relative influence. AI-Sentinel translates this into an adaptive cyber governance architecture by using weighted indicators to score national resilience, identify structural vulnerabilities, prioritise policy alerts, and support regulatory or institutional response. This enables policymakers to move from generic cybersecurity reporting to evidence-informed governance action, while preserving human oversight and multistakeholder accountability.

R^2 = 0.64 indicates that the ACGM has strong value for understanding cybersecurity governance, while SEM pillar weighting enables AI-Sentinel to convert the most

[2] *The seven-pillar structure used in AI-Sentinel is derived from the author's proprietary Adaptive Cybersecurity Governance Model research on cybersecurity governance in interconnected societies. The framework translates research-based governance variables into deployable pillars for assessing, aligning, executing and evaluating cybersecurity governance across national, sectoral and regional systems. The model, taxonomy, indicators and AI-Sentinel architecture remain the intellectual property of Olusegun Hamed Olugbile. Full academic citation will be provided after formal dissertation approval, institutional deposit or publication.*

influential governance factors into practical dashboards, resilience scores, policy alerts, and human-authorised cyber sovereignty decisions.

By practical implication, the difference is important. A country may have a cybersecurity strategy, cybercrime law, or a national CSIRT, but still lack real-time visibility into digital public infrastructure exposure, AI-enabled fraud, informal market harms, data residency risks, sector regulator coordination, or public trust decline. AI-Sentinel's value is therefore not only measurement, but the transformation of measurement into policy action.

Cross-reference: *This supports Policy Question 2, which asks what indicators should be used to measure cyber governance maturity, AI safety, data residency and digital trust*.

7.0 Bridging the AI Governance and Cybersecurity Governance Gap

AI governance is becoming central to cyber sovereignty. The Oxford Insights *Government AI Readiness Index 2024* ranks Sub-Saharan Africa ninth among regions, with an average score of 32.70. Mauritius scored 53.94, South Africa 52.91 and Rwanda 51.25, leading the region, while the Technology Sector pillar averaged only 23.98, indicating a major investment and capability gap (Oxford Insights, 2024).

The same report identifies emerging AI policy momentum in Africa, noting that Ethiopia, South Africa, Nigeria, and Zambia have released AI strategies, while the African Union released its continental AI strategy in July 2024, with the stated aim of harnessing AI for Africa's development and prosperity (Oxford Insights, 2024).

These figures support the need for a practical bridge between AI governance and cybersecurity governance. AI increases both opportunity and exposure: it can improve threat detection, policy simulation and regulatory monitoring, but it can also intensify fraud, surveillance, disinformation and automated exploitation. For this reason, AI-Sentinel is framed as AI-assisted rather than AI-autonomous. It must remain human-in-the-loop, rights-preserving and accountable.

Cross-reference: *This supports the workshop's emphasis on AI safety controls, human authorisation, model accountability and safeguards against misuse*.

8.0 Why a Multistakeholder Path Is Necessary

Cyber sovereignty cannot be built by governments alone. It requires coordinated participation from ministries, regulators, CSIRTs, telecom operators, banks, cloud providers, digital public infrastructure operators, civil society, academia, technical experts, development partners and affected communities.

The IGF's own multistakeholder logic is relevant here. The 2005 Working Group on Internet Governance defined Internet governance as the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet. The IGF 2026 review process also assesses whether proposals are relevant to the evolving relationship between AI, the future of the Internet and governance, and whether they provide concrete, innovative and diverse perspectives.

AI-Sentinel's multistakeholder value lies in its ability to provide a common operating language. Governments need policy visibility; CSIRTs need incident coordination; regulators need compliance intelligence; private operators need assurance and certification; civil society needs safeguards against misuse; donors need measurable impact; citizens need protection and trust.

9.0 Data Snapshot for the Workshop

Evidence area	Latest figure/data point	Governance implication
Global connectivity	Almost three-quarters of the world's population is online; 2.2 billion people are offline	Digital inclusion and cybersecurity must be jointly governed (ITU, 2025).
African mobile broadband	56 mobile broadband subscriptions per 100 inhabitants in Africa	Africa remains mobile-first, but connectivity depth is uneven (ITU, 2025).
5G adoption	Africa and CIS have two or fewer 5G subscriptions per 100 mobile broadband subscriptions	AI, cloud and advanced cyber governance must account for infrastructure gaps (ITU, 2025).
Mobile economy	Mobile contributed US$240 billion, or 7.8% of Africa's GDP, in 2025	Cyber risk now directly affects economic growth and digital trade (GSMA, 2026).
Mobile Internet usage gap	Almost 1 billion Africans are still not using the mobile Internet	Cyber governance must avoid excluding low-income and informal users (GSMA, 2026).
Cybercrime burden	Cybercrime accounts for more than 30% of reported crime in Western and Eastern Africa	Cybersecurity is now a public safety and institutional governance issue (INTERPOL, 2025).

Law-enforcement capacity	90% of African countries report needing significant improvement in cybercrime prosecution or law enforcement capacity	Human capacity and institutional coordination are critical (INTERPOL, 2025).
Malabo Convention	In force since 8 June 2023; 20 ratifications and 20 deposits recorded	Continental legal alignment exists, but implementation must deepen (African Union, 2023).
Data protection laws	44 African countries with data protection laws; 38 operational authorities by end-2025	Enforcement maturity and coordination must be strengthened (Code for Africa, 2026).
AI readiness	Sub-Saharan Africa average AI readiness score: 32.70; Technology Sector: 23.98	AI governance requires infrastructure, skills, data and safeguards (Oxford Insights, 2024).

10.0 AI-Sentinel Governance Logic

Figure 1. AI-Sentinel as a Multistakeholder Cyber Sovereignty Loop

This logic shows that AI-Sentinel is not proposed as a surveillance system or automated enforcement mechanism. It is a governance architecture for converting signals into accountable policy intelligence.

Interpretation of the AI-Sentinel Governance Logic:

AI-Sentinel Governance Logic presents a structured pathway for converting digital risk into accountable, rights-preserving cyber sovereignty outcomes. It shows how AI-Sentinel functions not merely as a cybersecurity monitoring tool, but as an adaptive cybersecurity governance pathway that connects technical risk signals with policy intelligence, institutional review, multistakeholder coordination and public-interest outcomes.

First Stage: The logic begins with **Digital Risk Signals** because effective cyber governance must respond to real-world indicators of change in the digital environment. These signals may include cyber incidents, data breaches, AI-enabled fraud, ransomware, misinformation, platform abuse, critical infrastructure vulnerabilities, digital public infrastructure failures, cross-border cybercrime trends or geopolitical technology dependencies. By placing digital risk signals at the start of the flow, AI-Sentinel establishes itself as an evidence-driven system that responds to observed risks rather than relying only on periodic audits or static compliance reports.

Second Stage: **Seven-Pillar ACGM Assessment**, applies the Adaptive Cybersecurity Governance Model to interpret the risk signal through seven governance lenses: risk assessment, cultural factors, technology, geopolitical factors, economic factors, gaps across global blocs and legal factors. This stage ensures that a cyber incident is not treated as a purely technical matter. Instead, it is assessed as a broader governance issue involving law, institutions, economic exposure, human behaviour, technology dependency, sovereignty and international digital power dynamics.

Third Stage: **Sovereign Cyber Resilience Indicators,** translates the assessment into measurable indicators. These indicators help policymakers, regulators, CSIRTs, private sector actors and development partners understand whether a country, sector or institution is resilient, exposed, vulnerable or in need of urgent intervention. This converts abstract cyber governance concerns into decision-ready evidence that can support national dashboards, sectoral reviews, regulatory action and donor-supported capacity-building programmes.

Fourth Stage : **AI-Assisted Policy and Risk Intelligence**, represents the analytical engine of the AI-Sentinel model. At this point, AI does not replace human judgment; it supports it. The system may generate risk interpretation, policy options, regulatory alerts, institutional response recommendations, critical infrastructure advisories, public communication guidance or scenario-based forecasts. This is where AI-Sentinel differentiates itself from conventional cybersecurity tools: it does not merely detect threats; it helps convert risk signals into governance intelligence.

Fifth Stage: **Human-in-the-Loop Review**, is essential for legitimacy, accountability and rights protection. Cyber governance decisions can affect citizens, businesses, public institutions, data rights, national security and democratic freedoms. For this reason, AI-Sentinel is designed to support human-authorised decision-making. Public authorities, regulators, technical experts or designated oversight bodies must review, validate and approve recommended actions before implementation. This prevents automated overreach and reduces the risk of surveillance misuse, discriminatory enforcement or policy errors.

Sixth Stage: **Multistakeholder Coordination**, reflects the Internet Governance Forum principle that digital governance should involve governments, private sector actors, civil society, the technical community, academia, youth, development partners and affected communities. Cyber sovereignty cannot be achieved by the state alone. Banks, telecom operators, cloud providers, digital public infrastructure managers, CSIRTs, data protection authorities, civil society groups and citizens all hold part of the risk picture. This stage ensures that response is coordinated, inclusive and institutionally balanced.

The final stage: **Rights-Preserving Cyber Sovereignty Outcomes**, defines the ultimate purpose of the AI-Sentinel logic. Cyber sovereignty is not framed as digital isolation or state control over the Internet. Rather, it means the capacity of societies to govern digital risk, protect human rights, secure critical systems, preserve lawful data agency, sustain public trust and cooperate across borders on fair and accountable terms. The desired outcome is a cyber governance environment that is secure, inclusive, interoperable, accountable and respectful of rights.

The AI-Sentinel Governance Logic, therefore, demonstrates a full transition from **risk detection to governance action**. It begins with observable digital risk signals, applies the seven-pillar ACGM assessment, produces resilience indicators, generates AI-assisted policy intelligence, subjects' recommendations to human review, coordinates stakeholders and delivers rights-preserving cyber sovereignty outcomes.

This makes AI-Sentinel a practical framework for moving African and Global South countries from reactive cybersecurity compliance toward adaptive, evidence-based and multistakeholder cyber governance.

11. Evidence Based that Support for the Proposed Workshop

Workshop component	Evidence base
Policy Question 1: Cyber sovereignty, openness and rights	▪ Connectivity gaps, data residency concerns, Malabo Convention, data protection growth
Policy Question 2: Governance indicators	▪ ITU GCI pillars, ACGM seven pillars, AI readiness gaps
Policy Question 3: Federated, human-in-the-loop governance	▪ INTERPOL cybercrime data, law-enforcement capacity gaps, AI-enabled threats
Expected output: Pilot roadmap for the Global South with Africa as initial pilot region	▪ Mobile-first economy, uneven capacity, continental legal frameworks
Expected output: Deployable indicator checklist	▪ ACGM pillars, ITU GCI model, data protection and cybercrime evidence
Safeguards against misuse	▪ AI surveillance risk, data extraction risk, human rights concerns, data protection enforcement gaps

The workshop would focus on cyber sovereignty as a governance capacity, not as an isolationist agenda, with clarity that cyber sovereignty means the ability of societies to govern digital risk, protect rights, secure critical systems, preserve data agency and cooperate across borders on fair and accountable terms.

Therefore, the AI-Sentinel model would be presented as:

i. Federated cybersecurity governance system wherw sensitive national data remains under national or lawful institutional control.
ii. Multistakeholder involving governments, private sector, civil society, technical community and development partners participate according to their roles.
iii. Human-in-the-loop, where AI supports policy intelligence but does not replace lawful decision-making.
iv. Rights-preserving by ensuring data protection, transparency, proportionality and anti-misuse safeguards are built into the model.
v. Africa-first, Global South-relevant approach in which Africa serves as the initial pilot region, while the methodology can inform other Global South contexts facing similar capacity, sovereignty and inclusion challenges.

13. Concluding Statement

The available evidence shows that Africa and the wider Global South face a converging governance challenge as a result of rapid digital transformation, rising cybercrime, uneven institutional capacity, emerging AI risks, fragmented legal systems and growing concern over data sovereignty. AI-Sentinel offers a structured approach to bring these issues into a single multistakeholder governance framework. By linking ACGM-derived indicators, AI-assisted risk intelligence, human-in-the-loop oversight, federated data governance, and rights-preserving safeguards, the workshop can provide a practical roadmap for cyber sovereignty that is open, inclusive, accountable, and globally relevant.

References

i. African Union. (2023). *African Union Convention on Cyber Security and Personal Data Protection: Status list*.

ii. Code for Africa. (2026). *Africa's data protection laws began to bite in 2025*. Source: https://medium.com/code-for-africa/africas-data-protection-laws-began-to-bite-in-2025-322285625315

iii. GSMA. (2026). *The Mobile Economy Africa 2026*. Source: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/africa/?utm_source=chatgpt.com

iv. INTERPOL. (2025). *New INTERPOL report warns of sharp rise in cybercrime in Africa*. Source: https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

v. International Telecommunication Union. (2024). *Global Cybersecurity Index*. Source: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx

vi. International Telecommunication Union. (2025). *Facts and Figures 2025: Measuring digital development*. Source: https://www.itu.int/itu-d/reports/statistics/facts-figures-2025/

vii. International Telecommunication Union. (2025). *Facts and Figures 2025: Mobile broadband subscriptions and 5G adoption*. Source: https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-subscriptions/

viii. Oxford Insights. (2024). *Government AI Readiness Index 2024*. Source: https://oxfordinsights.com/wp-content/uploads/2024/12/2024-Government-AI-Readiness-Index-2.pdf

ix. Olugbile, O. H. (2026). *Adaptive Cybersecurity Governance Model for an Interconnected Society*, Doctoral dissertation, Nassara State University

x. Olugbile, O. H. (2026). *Adaptive Cybersecurity Governance Model for Interconnected Society: Empirical foundation for AI-Sentinel Africa and the Cybersecurity Governance Variables Framework* (doctoral research-derived framework).

xi. Olugbile, S. H. (2026). *AI-Sentinel as a multistakeholder path to cyber sovereignty: Background material for UN IGF 2026 workshop proposal*. Global Network for Cybersolution.

xii. World Bank. (2026). *Digital Economy for Africa Initiative*. Source: https://www.worldbank.org/en/programs/all-africa-digital-transformation)