**OPENING SPEECH**

**Titled**

# FOSTERING DIGITAL SOVEREIGNTY THROUGH NATIONAL CYBERSECURITY FRAMEWORKS: CASE STUDY NIGERIA CYBERSECURITY FRAMEWORK

**by**

**DR. AMINU MAIDA**
**EXECUTIVE VICE CHAIRMAN /CEO**
**NIGERIAN COMMUNICATIONS COMMISSION**

at the

**6th EDITION OF AFRICAN CYBER DEFENSE FORUM (ACDF)**

With the Theme

**"TOWARDS A SECURE AND SOVEREIGN DIGITAL AFRICA"**

**October 2025**

**Protocols**

Esteemed Ministers, distinguished regulators, respected industry leaders, partners, and stakeholders from across Africa and beyond, it is an honor to stand before you today at this year's Annual Cyber Defense Forum, here in this beautiful city of Kigali in Rwanda. This city is a shining example of Africa's commitment to digital transformation and resilience, and it provides the perfect backdrop for a conversation of this magnitude.

I bring warm greetings from Nigeria, and from the Executive Vice Chairman and Chief Executive Officer of the Nigerian Communications Commission, the Regulator of the Communications Sector in Nigeria, who has given me the privilege to represent him at this momentous gathering of stakeholders.

Let me also seize this opportunity to thank our host and the convener of this event, the Africa Cyber Defense Forum ACDF, Dr Gilbert Nyandeje on the 6th Edition of the ACDF. This event and others under the auspices of the ACDF have become a fundamental part of the fabric of African cybersecurity awareness, highlighting the challenges and opportunities therein and building capacities especially for our young and vibrant youths across the continent.

The theme of this year's forum, ***"Towards a Secure and Sovereign Digital Africa"*** could not be timelier. Africa is amid an extraordinary digital revolution, from fintech to e-health, from smart agriculture to artificial intelligence. Our people are innovating, our youth are creating, and our economies are being reshaped before our very eyes. Yet, alongside these opportunities, we also face profound risks: ransomware, phishing, e-fraud, sextortion, cyberbullying and attacks on critical infrastructure, and the reality that dependency on foreign technologies often leaves us vulnerable.

There is no better time than now for African countries to deliberately align their national priorities with policies that safeguard the digital ecosystem, secure critical infrastructure, nurture indigenous innovation, and strike a balance between technological advancement and national interest.

In Nigeria, the issue of digital sovereignty is being accorded the utmost priority, with the clear objective of ensuring that the nation retains independence over its digital infrastructure, safeguards its data, and exercises full control over its decision-making processes.

This commitment to digital sovereignty naturally extends to cybersecurity, where safeguarding our digital assets and infrastructure has become a national imperative.

## Nigeria's Cybersecurity Journey

In 2021, Nigeria launched its National Cybersecurity Policy and Strategy (NCPS), a landmark framework designed to safeguard the nation's digital ecosystem. Among its key provisions, the NCPS established the National Cybersecurity Coordination Centre (NCCC) under the Office of the National Security Adviser (ONSA), serving as the central hub for coordinating national cybersecurity efforts. It also created the Nigeria Computer Emergency Response Team (ngCERT), which functions as the national umbrella CERT, harmonising the activities of sector-specific CERTs mandated by the policy—such as the NCC-CSIRT for communications, NITDA-CERT for government, NFI-CERT for financial institutions, and sectoral CERTs for healthcare and other critical domains.

The NCPS also identified various Critical National Information Infrastructure (CNII) as well as mandated all owners and operators of such infrastructure to share information on threats, vulnerabilities, solutions and other mitigating actions for a safer national cyberspace. Law Enforcement Agencies are also tasked with ensuring the protection of CNII with the Nigerian Security and Civil Defence Corp (NSCDC) given the critical role of physical protection of CNII.

At the Nigerian Communications Commission (NCC), as the regulator of the communications industry and host of the sectoral CERT, we have recognised the need for a sector-specific framework on cybersecurity. In response, we developed the Cybersecurity Resilience Framework for the Nigerian Communications Sector (CRF-NCS), designed to strengthen preparedness, enhance response, build resilience, and safeguard our digital sovereignty. Supported by the World Bank and in collaboration with our Licensees, this comprehensive framework will tackle the challenges before us while setting bold new ambitions for the future.

The framework also emphasizes sovereignty, local capacity building, and regional solidarity. Although we are still refining its details, five foundational pillars are already clear, and which I believe carry lessons that resonate across our continent.

Let me share these five key pillars, that not only reflect our national direction but also offer valuable lessons for other African nations.

### 1. **Aligning National Strategies with Continental Goals**

Our first pillar is alignment with national and continental goals. Nigeria is working to synchronize its cybersecurity strategy with continental instruments such as the African Union's Digital Transformation Strategy (2020–2030) and the Malabo Convention on Cybersecurity and Personal Data Protection. By doing so, we ensure that our efforts do not stand in isolation but rather strengthen Africa's collective digital defence. This approach also helps reduce over reliance on external platforms while encouraging the growth of solutions rooted in African realities. To buttress this fact, we have developed a Governance, Risk and Compliance (GRC) software to track the implementation and performance of the earlier mentioned Cybersecurity and Resiliency Framework which will enable reporting and tracking of compliance while contributing to threat information sharing in the communications sector.

### **2. Strengthening Regional Cooperation through CERTs**

Secondly, recognizing that cyber threats hold no borders, as a phishing attack launched in one country today could cripple services in another tomorrow, Nigeria is establishing the groundwork for an interconnected Computer Emergency Response Teams (CERTs) across multiple sectors. These CERTs will enable real-time intelligence sharing, joint incident responses, and regional capacity building. Our wider vision is of a continental CERT network capable of confronting threats with one voice and one strategy. This will serve as a shield that will respond in real time to cyber threats across the continent which will ultimately serve both as a model of cross-border and African cooperation as well as a platform for cyber-solidarity amongst member states.

### 3. Promoting Local Innovation for Africa-Specific Threats

Africa loses billions annually in a double whammy fashion by losing due to various cybercrimes such as ransomware, phishing and BEC while also losing money to foreign solutions providers to help protect our IT assets and infrastructure. Clearly, we must accept that imported solutions alone will not save us. We must develop our local solutions, encourage our entrepreneurs and support our developers and talents across the continent to ensure that manpower and capacity development in cybersecurity is entrenched in institutions and workplaces.

Our approach in Nigeria prioritizes homegrown innovation through encouraging startups, universities, and cybersecurity experts to develop context-specific tools. Through public-private partnerships, incubation hubs, and targeted investments, we are creating a cybersecurity ecosystem that is authentically African, globally competitive, and future-ready. The NCPS introduced earlier specifically encourages the use and adoption of local content through collaboration with relevant stakeholders to create cybersecurity technology incubation platforms, innovation centers, and laboratories.

These foundations will drive initiatives and provide support and incentives for projects focusing on the indigenous cybersecurity technology market in Nigeria.

It also calls for a centralized licensing and registration of cybersecurity professionals in Nigeria. Thus, ensuring that cybersecurity training centers and institutions as well as security service providers are registered and licensed before they can operate in Nigeria.

Financial incentives, tax holidays, innovation grants and pioneer status shall also be granted for indigenous innovation and development of cybersecurity technologies and cybersecurity research as outlined in the policy.

### 4. Enhancing Critical Infrastructure Protection

The security and availability of critical infrastructure is paramount in safeguarding cyberspace. We understand that without critical infrastructure protection, our sovereignty remains fragile. In addition to the identification of critical national information infrastructure nationally, the President of the Federal Republic of Nigeria, President Bola Ahmed Tinubu has also signed a Presidential Order designating the ICT systems and infrastructure of 13 vital sectors—including telecommunications—as critical assets that must be protected. These assets, which range from data centres, telecoms facilities, manufacturing and healthcare facilities, rail and power infrastructure amongst others are giving a special status for prioritization and protection.

In giving effect to the CNII Presidential Order, the Nigerian Communications Commission has taken deliberate steps to safeguard the nation's telecommunications infrastructure. One of these efforts is the establishment of the Cybersecurity Advisory Group (CSAG)—a body comprising C-level executives of MNOs, ISPs, Data Centres, as well as representatives of law enforcement agencies—which meets quarterly to deliberate on cybersecurity issues and strengthen industry-wide resilience. This not only reinforces good cyber hygiene amongst players but creates a good rapport and understanding between players. We have also rolled out a minimum cybersecurity standard for telecom operators, reinforcing resilience in one of our most vital sectors. This initiative not only strengthens Nigeria's communications backbone but also offers a template for other sectors such as energy, finance, and transport. Our belief is simple: a strong Africa must secure its digital foundations.

### 5. Embracing Ethical AI in Harmony with African Values

Finally, we cannot ignore the role of artificial intelligence in shaping the future of cybersecurity. Yet, as we adopt AI, we must ensure that it operates within ethical boundaries that reflect our own cultural and moral frameworks. Nigeria's National Artificial Intelligence Strategy (NAIS) which was launched in 2024, introduces AI governance guidelines that emphasize transparency, accountability, fairness, and above all, human dignity. We must ensure that technology serves our people and not the other way around. The vision entrenched in our national AI strategy is clear: to establish Nigeria as a global leader in AI and to foster sustainable development through ethical innovation and collaborative efforts.

Our national AI strategy is guided by principles that emphasize responsible and ethical AI development to ensure that AI technologies are designed with societal impact in mind. These principles include, amongst others, a commitment to transparency, accountability, human-centric approaches, inclusivity and shared prosperity.

## Conclusion

Our journey has reinforced one fact, that cybersecurity is not a solitary mission. Governments, private innovators, regional bodies, and international partners all have roles to play. We need public-private partnerships to drive innovation, regional solidarity to ensure no African country is left behind, and global collaboration to build our capacity without surrendering our independence.

The road to a sovereign digital Africa is not an easy one but it is within reach if we act together, with urgency and with purpose. Let us not merely adopt technologies but master them. Let us not simply react to threats but anticipate them. And above all, let us craft a digital destiny that is truly African in its design, resilient in its defense, and sovereign in its execution.

Ladies and gentlemen, Nigeria's journey is far from over, but our experience offers valuable lessons on public-private partnership, regional collaboration and capacity building. Our cybersecurity framework is our contribution to a stronger African strategy. As I conclude, let me emphasize that digital sovereignty is also about our future. We invite our brothers and sisters across the continent to join us in co-creating a secure, inclusive, and sovereign digital space.

On behalf of the Nigerian Communications Commission, I reaffirm our commitment to working hand in hand with fellow Africans and other global partners to build a digital Africa where our people are safe, our data is valued, and our future is firmly in our hands.

Thank you.

**Dr. Aminu Maida**
Executive Vice Chairman/ Chief Executive Officer
Nigerian Communications Commission