The State of African Cybersecurity Capacity

AiCE Africanism & Pan-African Studies — Where Africa stands, and the Malabo Convention

Where Africa Stands

The Global Cybersecurity Index (GCI), published by the International Telecommunication Union, assesses countries on five dimensions of cybersecurity: legal measures, technical measures, organisational structures, capacity building, and cooperation. African countries' scores on the GCI have improved significantly over the past decade, reflecting genuine investment in cybersecurity capacity across the continent. But the majority of African countries remain in the lower half of the global ranking, and the gap between cybersecurity threats and cybersecurity capacity remains large.

African Cybersecurity Capacity: The Landscape
Most advanced African cybersecurity systems: South Africa, Egypt, Kenya, Ghana, and Mauritius rank in the upper tier of African GCI scores.
National Computer Emergency Response Teams (CERTs): approximately 30 African countries have established national CERTs — up from fewer than 10 in 2014.
Cybersecurity legislation: approximately 35 African countries have passed cybercrime laws; approximately 20 have data protection legislation.
The gap: most African CERTs are severely under-resourced — limited staff, limited technical tools, limited threat intelligence sharing.
Skills shortage: Africa faces a shortage of an estimated 100,000 cybersecurity professionals — the largest skills gap relative to GDP of any region.
Critical infrastructure protection: most African countries lack specific cybersecurity frameworks for power grids, financial systems, and water treatment.
Private sector leadership: many African banks and telecoms have stronger cybersecurity than their governments, driving capacity in some countries.

The AU Malabo Convention: Africa's Cybersecurity Framework

The African Union Convention on Cyber Security and Personal Data Protection — known as the Malabo Convention after the Equatorial Guinea city where it was adopted in 2014 — is the continental legal framework for African cybersecurity and data protection. It covers four areas: electronic transactions and e-commerce; personal data protection; cybersecurity and cybercrime; and child online safety. It requires member states to pass national laws implementing these standards.

The Malabo Convention is a serious and ambitious document. But its impact has been limited by the pace of ratification: as of 2024, only a minority of AU member states have ratified it, meaning it does not yet have continental legal force. The reasons for slow ratification include genuine resource constraints — implementing the convention's requirements is expensive — political resistance, since some governments may be reluctant to constrain their own surveillance activities, and the technical complexity of enacting the required national legislation.

Accelerating Malabo ratification and implementation is one of the most important cybersecurity and digital rights priorities for Africa. A continental legal framework that protects African citizens' data, establishes clear cybercrime definitions and penalties, and requires member states to build minimum cybersecurity capacity would significantly strengthen Africa's collective digital security posture.

Key Takeaways

African cybersecurity capacity has genuinely improved over the past decade — more CERTs, more legislation, better GCI scores — but remains dramatically insufficient given a 100,000-person skills shortage and chronically under-resourced institutions. The Malabo Convention offers a serious continental framework, but its slow ratification since 2014 limits its actual legal force. The next lesson turns to the specific rights this framework is meant to protect: data protection.