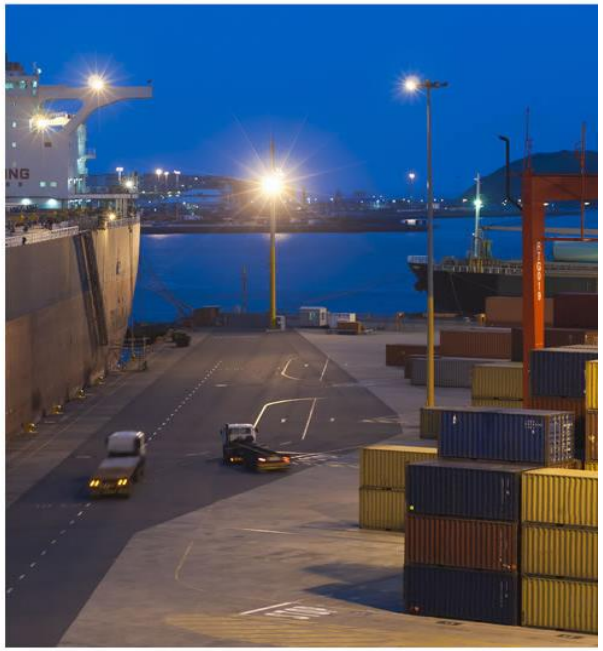
AUDA-NEPAD
AFRICAN UNION DEVELOPMENT AGENCY



AUDA-NEPAD Cybersecurity Assessments

PIDA WEEK JANUARY 18-21, 2021

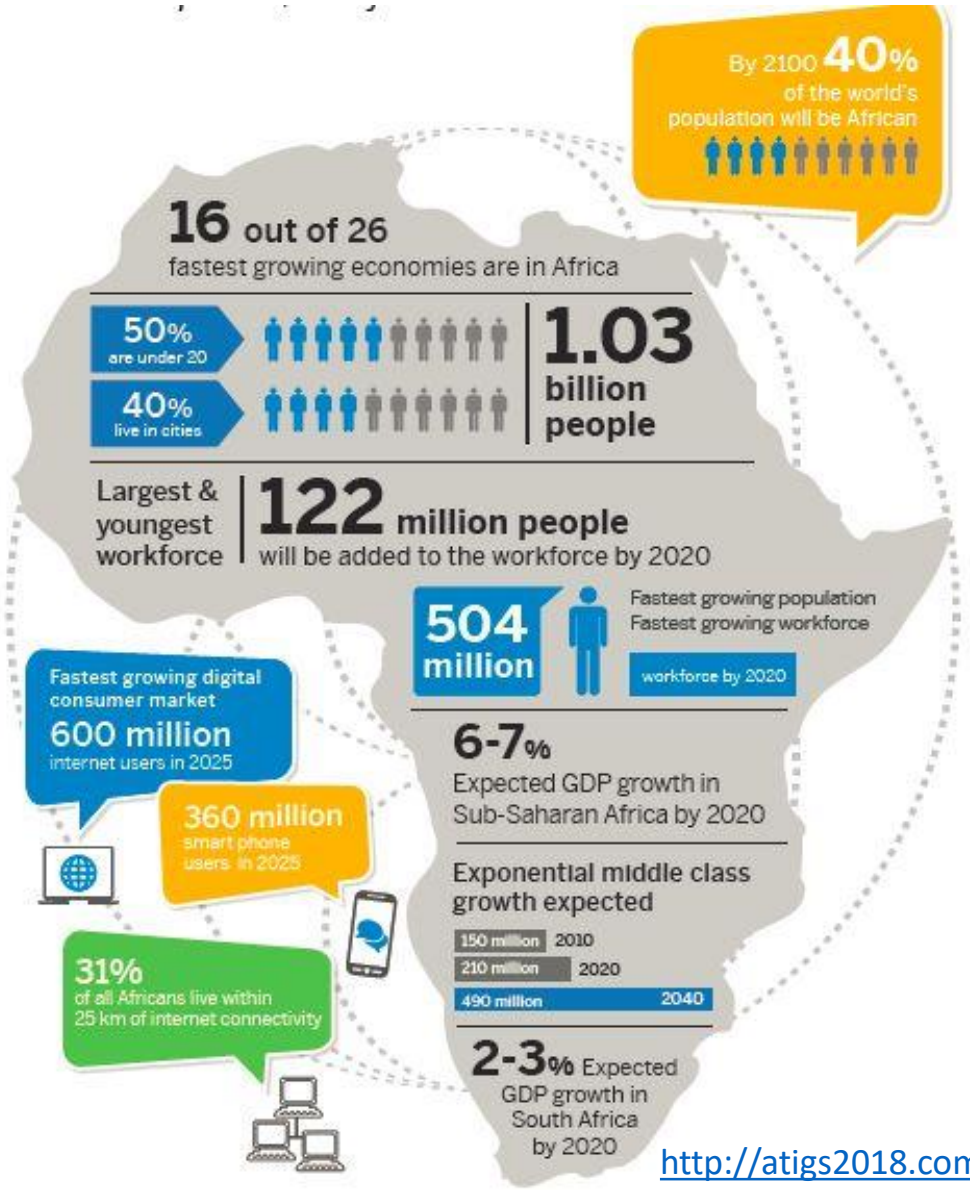
Cybercrime, Cybersecurity & Cyber-resilience

- Cybercrime - crime, illegal activities or criminal offenses that involve or are facilitated by the use of information and communication technologies, electronic communications and information systems.

- Cybersecurity - techniques and mechanisms to protect computers, networks, programs, personal data, etc., from unauthorized access, change, destruction and threats.

- Cyber resilience - ability to mitigate damage to systems, processes, reputation and to maintain operations once systems or data have been compromised.

Africa's Growth



http://atigs2018.com/africa-projection-facts/

Cybersecurity Challenges

- **Cybercrime Impact**
  - Losses of more than US$3.5bn annually
  - More than 90% of incidents unreported
  - Limited spending on cybersecurity measures

- **Cybersecurity challenges**
  - Multi-dimensional
    - Sovereignty, freedom of expression and privacy
  - Diversity among countries
    - Legislation, capacity, resources, languages, legal systems
  - Regional groupings & coordination
  - Intra-country coordination
  - Limited skills & expertise

African Union Convention on Cybersecurity & Personal Data Protection

- Establishes credible framework for cybersecurity in Africa
- Electronic transactions,
- Personal data protection,
- Cyber security and cybercrime
- Requires member states to:
  - develop national cyber security policy
  - develop legislation on cybercrime
  - ensure the protection of critical information infrastructure
  - enact personal data protection laws

Cybersecurity Measures

- Policy & Governance
  - Public private partnerships for promotion and enhancement of a cybersecurity culture
  - Cybersecurity Policy
  - National Cybersecurity
- Legislative & Regulatory
  - Data Protection Laws and Regulations
  - Electronic Commerce Laws and Regulations
  - Cybercrime Laws and Regulations

Cybersecurity Measures

- Institutional Measures
  - Computer Emergency Response Teams (CERTs)
  - *Data Protection Authority*
  - Electronic Signature Accreditation
    - Institutions responsible for *national and cross-border co-ordination of cybersecurity* problems as well as global co-operation
  - Institutions with the statutory *authority and legal capacity to respond to cyber security incidents*, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution
  - State/Government Department to:
    - *regulate and approve electronic commerce payment methods*
    - *regulate and undertake vulnerability and safety guarantee assessments of ICT product vendors*

AUDA-NEPAD Cybersecurity Assessment - Overview

- **advancement of Africa's Cybersecurity environment**
- **strengthening the legal & regulatory framework for electronic transactions and data privacy in Africa**

- analyzed the laws, policies and regulations of ten (10) African Union member states: ***Benin***, ***Chad***, ***Republic of Congo***, ***Democratic Republic of Congo***, ***Guinea***, ***Kenya***, ***Mauritania***, ***Morocco***, ***Senegal*** *and* ***Tunisia***

AUDA-NEPAD Cybersecurity Assessment - Methodology

Country selection

Countries with representatives in the PAP Committee on Transport, Industry, Telecommunications, Energy, Science and Technology which are collaborating with AUDA-NEPAD on the Cybersecurity project.

Countries that have signed and/or ratified the AU Convention.

Countries that are recognised ICT leaders within their respective regions (for benchmarking); and Regional and geographic balancing.

Assessment Criteria And Data Sources

Main criteria observed in each Selected African Union member states

Does the selected country have in place legislative/regulatory, policy and institutional measures in the areas of data protection, Cybersecurity and cybercrime and electronic transactions called for by the AUCC?

The study was conducted between July 2019 and January 2020

AUDA-NEPAD
AFRICAN UNION DEVELOPMENT AGENCY

Findings - Laws and Regulations

- **9/10 member states have instituted a law concerning data protection** (Benin; Chad; Republic of Congo; Guinea; Kenya; Mauritania; Morocco; Senegal; and Tunisia).

- **8/10 member states have instituted a law concerning cybercrime and cybersecurity** (Benin; Chad; Guinea; Kenya; Mauritania; Morocco; Senegal; and Tunisia).

- **8/10 member states have instituted a law concerning electronic transactions** (Benin; Chad; Guinea; Kenya; Mauritania; Morocco; Senegal; and Tunisia).

- **3/10 member states whose data protection, cybercrime and cybersecurity, and electronic transaction laws** are all **outdated** (dating from 2000 - 2008) and **require revision**.

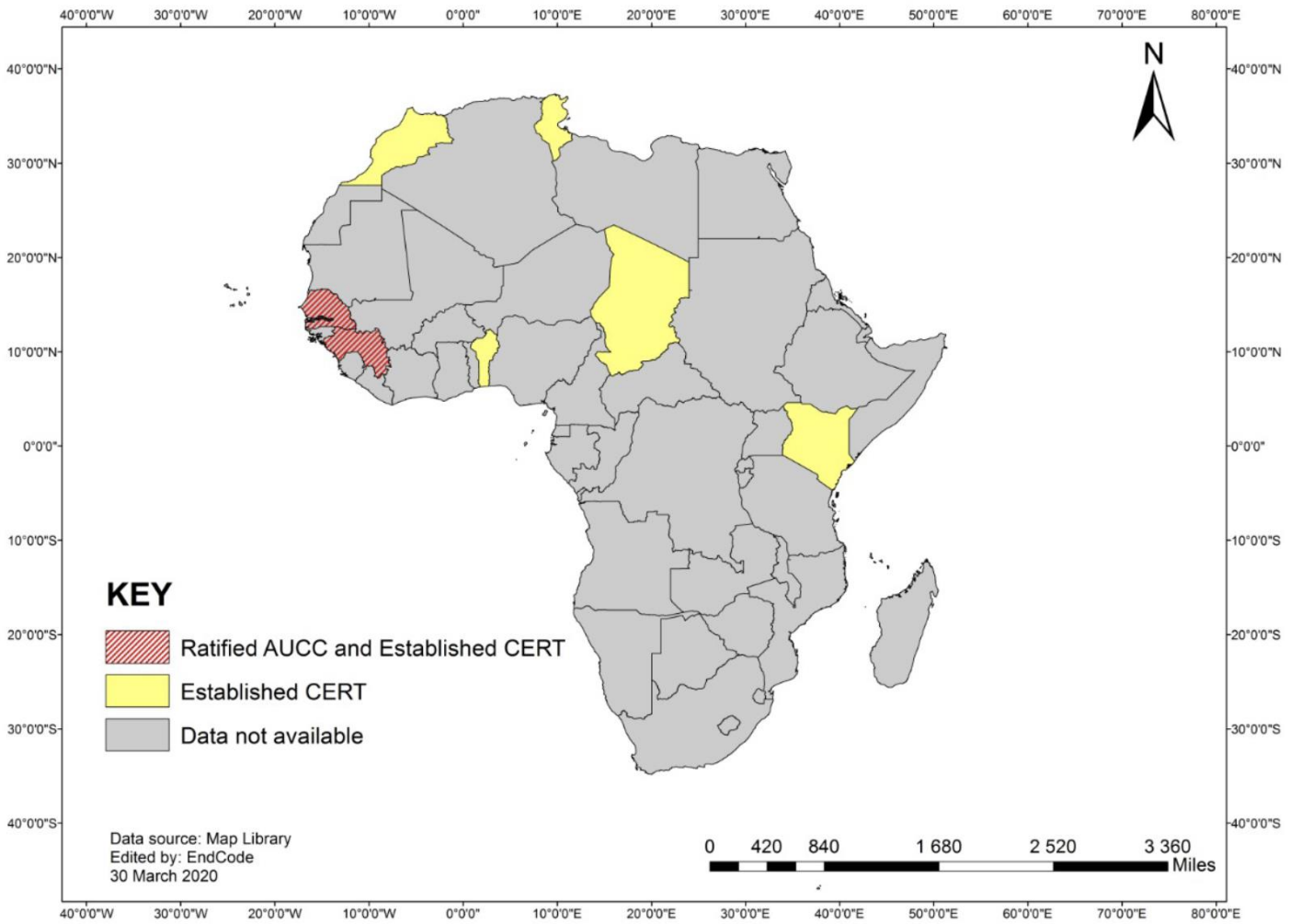
Findings - Institutional Measures

- **7/10 member states have established a Data Protection Authority** (Benin; Republic of Congo; Kenya; Mauritania; Morocco; Senegal; and Tunisia) – of the seven (7) Data Protection Authorities, only four (4) appear to be operational at the time of study.

- **5/10 member states have established a Cybersecurity Emergency Response Team (CERT)** (Benin, Chad, Kenya, Morocco and Tunisia) - however, all member states under study (with the exclusion of the DRC) have one or more alternative institutional measures in place responsible for responding to cybercrime and cybersecurity.

- **6/10 member states have established an institution for electronic transactions (electronic signature and certification providers)** (Benin; Chad; Republic of Congo; Morocco; Senegal and Tunisia).

Findings - Institutional Measures



Other Findings

- ***Cybercrime and cybersecurity institutional measures, as well as electronic transaction institutional measures, policies and strategies, are the weakest areas of implementation for the member states under study.***

- Whilst the majority of countries prioritised policy and legislation, **strategies to implement policies and institutions to support implementation of policies and strategies are not as widespread.**

- Of the African Union member states that have laws, policies & strategies in place, the study indicated that **7 of the member states have laws, policies and/or strategies that are in draft.**

- **Guinea, Kenya, Mauritania, Morocco and Tunisia** have a Cybersecurity Policy that recognises **Critical Information Infrastructure**, identifies the national security interests in cyberspace and recognises the need for mitigation measures. Kenya, Morocco and Tunisia have a national Cybersecurity Strategy to implement the Policy.

AUDA-NEPAD Cybersecurity Assessments - Recommendations

National level	Regional/Continental level
• Accelerate the ratification and implementation of the Convention	• Harmonized definitions of Cybersecurity
• Drafting or reviewing outdated legislative and regulatory frameworks	• Baseline and Annual Statistics
• Implement institutional frameworks provided for in legislative and regulatory frameworks	• Promote dialogues with national and regional stakeholders on the significance of the Convention and concerns pertaining to the ratification of the Convention.
• Balanced interests in Cybersecurity and human rights	
• Prioritise strengthening weaker areas of implementation	• Compatibility and Comparison with Other Models and Conventions
• Implement review procedures where laws and regulations are outdated	
• Prioritise the passing of draft laws, regulations, policies and strategies	• Broaden co-operation with Countries
• Operationalise laws and institutional measures	• Promote Cybersecurity in the context of cyber stability

Way Forward for the Assessments

- Extending the study to other countries
- Implementation support to countries - through information portals (websites), guides, checklists and capacity building for the drafting of legislation and policies and operation of institutional bodies.
- Further engagement is needed in the area of institutional measures considering financial and skills constraints .
- Preparation of roadmaps on how to align with the Convention by having a clear list of measures that still need to be implemented to meet the requirements of the Convention.

General Recommendations & Conclusion

- Awareness among stakeholders
- Coordination and communication at national and regional level
- Inclusiveness - need for all stakeholders (civil society, government, private sector, academic) to be involved in national and regional processes.
- Technical and institutional capacity building
- Examine and streamline ratification processes
- Financial resources – setting up of institutions, capacity building, monitoring and enforcement

شكرا

MERCI

OBRIGADO

THANK YOU

Contact Information

Towela Nyirenda-Jere, PhD

Email: towelan@nepad.org

Tel. : +27 11 256 3587