Cybersecurity Governance

- Political Will and Leadership
- Institutional Governance
- Infrastructure and Equipment – Capability, Interoperability, Standards, Protocols
- Skills and Training – Capability
- Incident Response – Capability and Maturity
- Resources and Budget Allocations
- International, National, Sectoral and Inter-sector cooperation
- Enforcement – Legal Frameworks that identify offences and sanctions and co-operation with State Powers – Surveillance, Interception, Search, Seizure
- International Powers - Surveillance, Interception, Search, Seizure
Cybersecurity Governance

- UNCITRAL
- Budapest Conv.
- EU
- ITU
- UNCTAD
- UNECA
- AU
- SADC
- EAC

Globally, there are multiple initiatives, efforts, models at international, national and regional levels. Particularly to:

  - Promote harmonised, global, coherent and co-ordinated approaches;
  - Address legal barriers to electronic transactions; and
  - Promote trust and confidence in (international) electronic transacting methods
Africa Acronyms

Initiatives by, for instance:

- AU (African Union)
- SADC (the Southern African Development Community)
- UNECA (Economic Commission for Africa)
- UNCTAD (Commission Trade and Development)
- ECOWAS (Economic Community of West African States),
- EAC (East African Community)
UNCITRAL (1996)

- MLEC – Model Law on Electronic Commerce
- Promote greater consistency in national and regional approaches.
- Create a more secure legal environment for electronic commerce for providing a model reference for legislators
- Implemented by several countries
- In Africa – implemented by South Africa, Cape Verde, Mauritius
Encoding Cybersecurity Norms and Principles – African Union Convention
According to the Website:

The Draft Convention gives effect to a Resolution of the last session of the Assembly of Heads of State and Government of the African Union, and seeks to harmonize African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cyber crime control.

In pursuance of the principles of the African Information Society Initiative (AISI) and the African Regional Action Plan for the Knowledge Economy (ARAPKE), the Draft Convention is intended not only to define the objectives and broad orientations for the Information Society in Africa, but also to strengthen existing legislations in Member States and the Regional Economic Communities (RECs). It defines the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa. It lays the foundation for an African Union-wide cyber ethics and enunciates fundamental principles in the key areas of cyber security. It also defines the basis for electronic commerce, puts in place a mechanism for combating intrusions into private life likely to be generated by the gathering, processing, transmission, storage and use of personal data and sets broad guidelines for incrimination and repression of cyber crime. Its adoption would capitalize African and international experiences in cyber legislations and speed up relevant reforms in African States and the RECs.

Source/ Read More: http://au.int/en/cyberlegislation
The objective of this Convention was to propose the adoption at the level of the African Union, a Convention establishing a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime.
Information security impacts on the security of the digital and cultural heritage of individuals, organizations and nations;

The vulnerability in the normal functioning of institutions can compromise the survival and sovereignty of States;

Addressing cyber security calls for clear-sighted political will to define and implement a strategy for development of digital infrastructure and services (eservices) and articulate a coherent, effective and controllable multi-disciplinary cyber security strategy.
Achieve a level of **technological security** adequate enough to prevent and effectively control technological and informational risks;

Build an information society that respects **values**, protects **rights and freedoms**, and guarantees the security of the property of persons, organizations and nations;

Contribute to the knowledge economy, guarantee equal access to information while stimulating the creation of **authentic knowledge**;

Create a climate of confidence and trust, that is:

- **Predictable** in terms of prevention and resolution of disputes; and evolving because it takes into account continued technological evolution;

- **Organized**: covering the relevant sectors;

- **Protective**: of consumers and intellectual property (civil and penal) of citizens, organizations and nations;

- **Secured**: striking proper balance between legal and technological security;
Provisions relating to legality of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combatting cybercrime
Provisions: too much power to the government, particularly in accessing private information. Processing of personal data and sensitive data without consent of the owner for the purpose of state security and public interest could be misused. Broad and unchecked powers to “investigating judges”. Such powers include the power to issue search and seizure warrants for any electronic records. Prosecution of anyone seen to promote “theories” of racism and xenophobia. Only approved e-commerce payments may be used in a country. This requirement would force popular global platforms, such as Paypal, to seek regulatory approval, considerably slowing down the rate at which they could spread their services across Africa.
Encoding Cybersecurity Norms and Principles – Regional Model Approaches
SADC Cybersecurity , 2012

- SADC Model Laws - adopted at a SADC Ministerial meeting in Botswana in 2012
  - SADC Model Law on Data Protection, 2012
  - SADC Model Law on Cybercrime, 2012
  - SADC Model Law on Electronic Transactions, 2012
- Commenced with a regional and international assessment
- Technical Assistance was offered by ITU for the drafting of the Model Laws and in-country transpositions
- SADC countries have adopted the models
Establishment of Harmonized Policies for the ICT Market in the ACP

DRAFT Southern African Development Community (SADC) MODEL LAW ON ELECTRONIC TRANSACTIONS AND ELECTRONIC COMMERCE

HIPSSA – SADC Model Law on Electronic Transactions & Electronic Commerce

Support for Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)
Directive on Fighting Cybercrime, 2009
Incorporation of legal framework for Member States
Emphasis on cybercrime, data protection, search and seizure


Enabling legal framework as a critical factor: e-transactions, cybersecurity

Harmonized regional and national legal frameworks

Creation of an EAC Task Force (2008)


The EAC legal framework for Cyber Laws (Phase I) covering electronic transactions; electronic signatures and authentication, cyber crime, and data protection and privacy have been adopted by the Council of Ministers (2012)

http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf
“The East African Development Strategy (2011/12 – 2015/16) proposes the key drivers for the realization of the EAC regional integration agenda in the next five years to include, among others, creation of a strong legal framework (…)"

The development of cyber laws in the region is critical to underpin the realisation of full potentials in regional e-commerce, electronic financial transactions and business processes outsourcing.”

Hon. Musa Sirma, Chairperson of the Council of Ministers of the East African Community and Minister for East African Community, Republic of Kenya, at the occasion of the presentation of the budget of the EAC for the financial year 2012/2013 to the legislative assembly
<table>
<thead>
<tr>
<th>Country</th>
<th>eContracting/administration &amp; evidence</th>
<th>Data privacy</th>
<th>Consumer protection</th>
<th>Copyright</th>
<th>Domain name mechanisms</th>
<th>Internet &amp; mobile payment systems</th>
<th>Cyber crime &amp; cyber-security</th>
<th>Content control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burundi</td>
<td>Pending</td>
<td>Pending</td>
<td>Pending</td>
<td>✓ (2005 Act)</td>
<td>Not reported</td>
<td>No regulations</td>
<td>(2009 Act &amp; Bill)</td>
<td>Pending</td>
</tr>
<tr>
<td>United Republic of Tanzania</td>
<td>No regulations</td>
<td>Partial under 2010 Law</td>
<td>No regulations</td>
<td>✓ (1999 Act)</td>
<td>No regulations</td>
<td>No regulations</td>
<td>No regulations</td>
<td>Partial under 2010 Law</td>
</tr>
</tbody>
</table>

Source: UNCTAD forthcoming study on cyber-legislation in EAC.
ICT Ministers call for harmonized policies and cyberlegislations on Cybersecurity

Khartoum Ministerial Declaration – emphasises the need for African countries to accelerate the formulation of cyberlegislation...

Addis Ababa, 05 September 2012 (ECA) - The fourth African Union Conference of Ministers in charge of Communications and Information Technologies opened today in Khartoum, Sudan, under the auspices of His Excellency the President of the Republic of Sudan, Field Marshal Omer Hassan Ahmed Albashir.

Addressing the Ministers and invited guests during the opening ceremony, President Albashir stated that African countries need to "enact the required legislation for ICT related investments, build the capacity of the youth and put in place incentives to promote science and technology in Africa".

During her opening remarks, Ms Aida Opoku Mensah, Director of ICT, Science and Technology Division of the United Nations Economic Commission for Africa reminded participants that "while Internet users have more than doubled to 2.5 billion worldwide since 2005, Africa which is home to 14 percent of the world's population accounts only for 6.2 percent of the world's internet users."

Ms Opoku-Mensah also drew the attention of delegates to the "African Union Convention on Cybersecurity developed with the technical support of ECA and which will require approval of the Ministers for further consideration by African Heads of States and Governments".

Also speaking at the opening ceremony, Ms Elham Ibrahim, Commissioner for Infrastructure and Energy at the African Union Commission reaffirmed that "ICTs will transform Africa and will drive the continent's renaissance."

At the end of the two days Conference, ICT Ministers will adopt the Khartoum Ministerial Declaration which emphasizes among other issues, the need for African countries to accelerate the formulation of cyberlegislations; implement the recommendations of the feasibility study on the African Space Agency; proactively participate and agree on common positions on global issues related to Internet Governance as well as accelerate the transition from analogue to digital terrestrial broadcasting.

Experts adopt Declaration of Addis Ababa on harmonization of cyber legislation

ECA Press Release No. 103/2012

Addis Ababa, 22 June 2012 (ECA) - Over 80 experts from Eastern, Southern and Northern Africa regions concluded a three day consultative workshop with the adoption of the Addis Ababa Declaration on harmonization of cyber legislation in Africa. The declaration is bolstered by a series of recommendations to the African Union Commission and the United Nations Economic Commission for Africa.

The recommendations focused on taking into account the views of Member States in finalizing the draft AU Convention on Cyber Security; intensifying awareness-raising and organizing tailored capacity building programmes on cyber legislation to law enforcement institutions and agencies. Further, the experts urge Regional Economic Communities to support harmonization of cyber security policies and legislation, among others.

Speaking at the closing session, Ms. Aida Opoku-Mensah, Director of the ICT, Science and Technology Division (ISTD) lauded the participants for their “collective support and commitment to the declaration adoption process”.

Also speaking in the concluding session, Ms. Eskedar Nega, Programme Officer at the ICT, Science and Technology Division of ECA reflected on the conference discussions and highlighted how ECA will take the outcomes of the conference forward in its upcoming work and set deadlines for each activity.

Ms. Opoku Mensah emphasized that the road map would feed into that the Convention, which will be tabled at the fourth Conference of Ministers in September 2012.

The workshop was organized by the Economic Commission for Africa and the African Union Commission in collaboration with Regional Economic Communities from 20-22 June at the United Nations Conference Centre in Addis Ababa. Over 80 experts in cyber legislation from ICT, justice, interior and Commerce ministries, law enforcement agencies, policy makers, including experts from legislative bodies, courts, the United States Department of Justice, Microsoft and the academia in the sub-region were in attendance.

Issued by:

ECA Information and Communication Service
P.O. Box 3001
Addis Ababa Ethiopia

For Consideration

- Political will, drivers, objectives
- Budget – Implementation of cybersecurity institutions, centres and capabilities requires finances
- Impact of cybersecurity readiness on trade (and development)
- Impact on rights and freedoms – privacy, access to information, neutrality of the internet –
- Limitations of rights
- Balancing of interests