ITU-ATU Workshop on Cybersecurity Strategy in African Countries

Khartoum, Sudan (Republic of the),

24 – 26 July 2016

African Union Perspectives on Cybersecurity and Cybercrime

Souhila Amazouz

Senior policy Officer , AUC

Cyber Security Challenges for Africa

- As African countries increase access to broadband Internet , issues relating to cybersecurity and cybercrime are emerging and there is a need to ensure that citizens , governments and business are protected .

- African governments are at different level of establishing policy instruments and legislative framework .

    - Lack of know-how in terms of cyber security and inability to monitor and defend national networks , making some African countries vulnerable to incidences of cyber terrorism and cyber espionage .

    - Inability to develop the necessary cyber security legal frameworks to fight cybercrime and while many countries have proposed legislations the level of deployment of security systems in both the private and the public sector is low.

- Considerable progress has been made in developing regional model legislation in the area of Cyber Security , notably related to data protection, e-transactions and cybercrime (**ECOWAS Cybersecurity guidelines, ECCAS Model Law/CEMAC Directives on Cybersecurity, SADC Model Law on data protection, e-transactions and cybercrime).**

AU response to Cyber Insecurity issue

❑ African Union aims to build an information society that respects cultural values and believes of the African Nation ,guarantees a high level of legal and technological security to protect rights and freedoms online and effectively control risks due to the misuse of Information communication Technologies (ICTs) .

❑ African Union works closely with Member States to promote a culture of Cybersecurity and develop National and Regional cybersecurity policies through multi stake holders approach involving governments, industry and civil societies, academies and all the organizations concerned by Cybersecurity issues in an integrated and comprehensive manner.

❑ Enforce the existing national criminal laws and adapt them to the reality of digital environment of the information society , consolidate and elaborate a common African strategy and to reinforce regional and international cooperation.

❑ Develop general principles and specific provisions related to cyber legislation and build up national cybersecurity frameworks based on legal and technical measures to fight against all kind of cybercrime and cyber-attacks at national and continental level.

AU response to Cyber Insecurity issue

- Ministers in charge of communications and Information technologies adopted a declaration [EXT/CITMC/MIN/Decl. (I)] (Olivier Tambo Declaration) in 2009 in which they ” requested the African Union Commission to develop jointly with the United Nations Economic Commission for Africa, a convention on cyber legislation based on the Continent’s needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection”. This Declaration has been endorsed by the 14th AU Summit of Head of State and government in 2010 [Assembly/AU/11(XIV)] and confirmed again by the third ordinary conference of Ministers in charge of ICT held in Abuja in August 2010 in their declaration ([AU/CITMC/MIN/Decl.(III)].

- The African Union Commission (AUC) and the Economic Commission for Africa (ECA) have spearheaded the development of the African Union Convention on Cybersecurity and personal data protection, which was adopted by the African Union Heads of States and Governments Summit in June 2014 in Malabo.

- The objective of the AU Convention is to get a common approach on the security of the cyberspace in Africa and set up a minimum standards and procedures to define a credible digital environment for developing the electronic communications and guarantee the respect of the privacy on line .

Development of the AU Convention the Confidence and Security in Cyberspace

- AU organs Decisions (Ministerial conferences and Summit of Heads of States and governments

- A draft Convention on Cyber Security has been developed (2010-11)

- Regional Workshops have been organized on Cyber Legislation and on the AU Draft Convention on Cyber Security:

  - **ECCAS**: Libreville, Gabon, November 2011
  - **ECOWAS**: Abidjan, Côte d'Ivoire, February 2012
  - Tripartite [**COMESA, SADC, CEAC**] + **UMA** (Northern Africa): Addis-Ababa, Ethiopia , June 2012

- Final Expert Group meeting to finalize the Draft Convention before the CITMC-4 Addis- Ababa, Ethiopia, August 2012

- Endorsement of the AU Final Draft Convention on Cyber legislation by the 4th Ministerial Conference of the African Union Ministers in charge of Communication and Information Technologies (CITMC-4).

- Adoption of the convention by the Conference of Ministers in charge Justice and Legal Affairs

- **The African Union Convention on Cyber security and personal data protection has been adopted by the 23 rd Assembly of Heads of States and Governments held in Malabo , Equatorial Guinea in June 2014**

AU Convention on the Confidence and Security in Cyberspace

The convention embodies the treatment of Cybercrime and cybersecurity but it’s not only confined in these elements it embraces important elements of electronic communications and protection of personal data .

- Define key cyber terminologies in legislation
- Develop general principles and specific provisions related to cyber legislation
- Outline cyber legislative measures required at Member State level
- Develop general principles and specific provision on international cooperation as related to cyber legislation
- Protect the rights of persons during data gathering / processing against the threats and attacks capable of compromising their privacy .
- Protecting Institutions against the threats and attacks capable of endangering their survival and efficacy.

The Convention main parts

PART I: ***ORGANIZATION OF ELECTRONIC COMMERCE***

PART II: ***PROTECTION OF PERSONNAL DATA***

PART III: ***PROMOTING CYBER SECURITY AND COMBATING CYBER CRIME***

PART IV: ***COMMON AND FINAL PROVISIONS***

PART I: Electronic Transactions

Section I : Electronic Commerce

Section II: Contractual Obligation in Electronic Form

Section III :   Security of Electronic Transactions

PART II: Personal Data Protection

Section I : Personal Data Protection

Section II : Institutional framework for the protection of personal data

-

Section III : Obligation relating to conditions governing personal data processing

Section IV : The Data Subject Rights

Section V : Obligation of personal data controller

PART III: PROMOTING CYBER SECURITY AND COMBATING CYBER CRIME

Section I : Cyber Security Measures to be taken at National Level.

Chapter 1: National cyber security framework

Chapter 2: Legislative measures

Chapter 3 : National cyber security system

Chapter 4 : National cyber security monitoring structures

Chapter 5 : International cooperation

- Harmonization
- Mutual assistance
- Exchange of information
- Means of cooperation

Section II: Criminal Provisions

Chapter I: Adapting certain ICTs offenses

Chapter II: Adapting certain sanctions to the ICTs

Chapter III : Offenses specific to ICTs

- Attack on computer systems
- Attack on computerized data
- Offenses relating to electronic message security measures.
- Content related offenses / definition of cyber threats against children

Signature, Ratification and Entry into Force

❑ This Convention is now open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures.

❑ This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.

❑ Upon entry into force of this Convention, the Chairperson of the Commission shall register it with the Secretary General of the United Nations, in accordance with Article 102 of the Charter of the United Nations.

❑ Eight Countries have already signed the convention : Benin , Chad , Congo, Guinea Bissau, Mauritania , Sierra Leone, Sao Tome & Principe and Zambia.

Considering the main goal of this Convention which is to address the need for Harmonized legislations in the area of Cyber Security and Personal Data Protection in Member States of the African Union, and to establish in each country a mechanism capable of combating Cybercrime and violations of privacy that may be generated from personal data collection, processing, transmission, storage and use.

The implementation of Malabo Convention covers notably the following areas:

- Ratification of the AU Cybersecurity Convention by at least 15 countries .
- Transposition of the convention's provision into National and Regional Cyber-legislations (Organization of National and Regional workshops en Cyber legislation)
- Human and institutional Capacity Building on Cybersecurity, Cybercrime, e-transaction and personal data protection and public awareness campaign
- Development of National and Regional Computer Emergency Readiness Team (CERTs) (provide countries with the capability to identify, respond and manage cyber threats)

Cooperation at Regional and International level

- African Union Commission is committed to promote the culture of Cyber Security and coordinate activities with the African Regional Economic Communities and Specialized Institutions to provide guidance to African countries on cybercrime and cyber security policies.

- African Union Commission is open for cooperation with relevant partners , regional and international organizations working in cyber security domain for the establishment of cooperation mechanisms to address the cyber security issue, combat different forms of cybercrime and ensure security and stability in the global Cyberspace .

- Memorandum OF Understanding (MOU) between African Union Commission and AfricaCERT is being finalized .The purpose of this MOU is to create a framework for cooperation and collaboration between AUC and AfricaCERT for the advancement of the information security ecosystem development in Africa.

- The AUC is member of the Global Conference Cyber Space 2015 initiative the Global Forum Capacity Expertise (GFCE) which is a global platform that contributes to cyber capacity building and sharing of experiences and best Practices : http://www.thegfce.com/initiatives

Cooperation at Regional and International level

- The African Union has started cooperating with the USA government , notably in promoting cyber security due diligence in Africa .
  - This Initiative builds on previous U.S-AUC efforts to promote a culture of cyber security on the continent by raising awareness and building cyber capacity on of African Experts to develop the key components of a national cyber security framework required to support national and international engagement on cyber policy .
- Three partite collaboration AUC / USA and Symantec to produce a report that collects and presents detailed technical data on cyber security threats and trends in Africa.

  - The report assess the major trends in the region in terms of threats to the cyber domain and the potential impact they could have on those that utilize it from government institutions to private enterprises to individual users.
  - The report will serve as a comprehensive document on cyber security matters in Africa, from which members of the African Union can draw useful conclusions and gain a more nuanced understanding of the major cyber trends in Africa as well as the current capacity to deal with those threats.

Cooperation at Regional and International level

The African union Commission is collaborating with United Nations Institute for Disarmament Research (UNIDIR) and take part to the International Cyber security conferences which refers to inter-governmental efforts to prevent the use of ICTs in a way to affect the international security.

- ❑ Took part to the Africa Regional Seminar on **the International Law and State Behavior in Cyber Space with special focus on the current mechanism for addressing cyber issue at Africa regional level** .

- ❑ Also, AUC participated in the UNIDIR **Cyber Stability Conference 2015 specifically on a panel discussion global approach to cyber stability and the future Inter Regional Collaboration .**

- ➢ The AUC is collaborating with ICT4peace foundation in the domain of International Cybersecurity Diplomacy and co-organized in February 2016 a Course for African diplomats . The training provided a view of the most imminent **Foreign Policy considerations regarding Cyber Space.**

Cooperation at Regional and International level

- □ Given the current state of cybercrime in general which constitutes a real threat to the security of computer networks and the development of the Information Society in Africa, **there is need to implement the AU convention on Cybersecurity and define broad guidelines of a continental Cyber Security strategy taking into account the existing commitments at sub-regional, regional and international levels for the repression of cybercrime in Member States of the African Union.**

- □ Cyber crime cannot be defeated by any law or convention alone , it becomes clear that the collaboration of all stakeholders in the governance and operation of the Internet is required to preserve the security and stability of Cyberspace .

- □ Considering the multiple dimensions and complexity of Cyber security , The African Union believes that **by creating an appropriate legal framework and harmonized legislations at National, Regional and Continental level to secure and build confidence in the use of internet as a global public good we contribute to protect all the internet related human rights which include online privacy and free flow of information.**

THANK YOU FOR YOUR ATTENTION

AU Commission

http://pages.au.int/infosoc/cybersecurity