***African Union Perspectives on Cybersecurity and Cybercrime***

Africa has witnessed during the last decade remarkable achievements in developing ICT infrastructures and services and therefore issues relating to cybercrime are emerging and there is a need to ensure that citizens, governments and business are protected.

Cyber-security (and Cyber Stability) is particularly challenging for African countries, especially least developed countries (LDCs) lacking adequate legal and regulatory frameworks, human capacity and expertise as well as financial resources to implement concrete measures.

While 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 cyber-security guidelines, ECCAS Model Law/CEMAC Directives on Cyber-security, SADC Model Law on data protection, e-transactions and cybercrime), more remains to be done especially in the area of implementation and transposition of these models at national levels.

In Africa , There is a growing need to elaborate further national cyber-security frameworks, harmonized at regional level and in line with existing international standards and practices so that trust and confidence in the use of ICTs is facilitated at all levels. In this regard, the African Union Commission (AUC) and the Economic Commission for Africa (ECA) spearheaded the development of the African Union Convention on Cyber-security and personal data protection, which was adopted by the African Union Heads of States and Governments Summit in June 2014 held in Malabo. Therefore, the African union through the operationalization of the Convention on Cyber-security aims to get a common approach at continental level on the security of the cyberspace and set up minimum standards and procedures to define a credible digital environment for developing the electronic communications and guarantee the respect of the privacy online.