A global approach on Cybersecurity and Cybercrime in Africa

I: **Introduction:**

1. During the last decade the African continent has witnessed big achievements in building ICT infrastructures and Internet access has been growing very rapidly. From less than 5% in 2007, Internet penetration has reached 28% in 2015, bridging Africa's gap to the rest of the world. If this growth rate is sustained, Africa should have access rates comparable to the developed world within the next decade.

2. It is clear that the Internet, mobile networks, and related information and communications technologies (ICTs) have become indispensable tools for governments, businesses, civil society, and individuals across the globe. These technologies have spurred tremendous economic development, increased the free flow of information, and promoted gains in efficiency, productivity and creativity across Africa.

3. The use of ICTs, and in particular the Internet, has become a matter of strategic importance. A free, open and secure Internet is an engine for economic growth and social development that facilitates communication, innovation, research and business transformation. However, the increased importance of internet has also presented our global community with new challenges: As our societies become more interconnected and dependent on the Internet and ICTs, we become more vulnerable to the misuse of these technologies and we need to ensure that the security of our ICT infrastructure is continually improved in order to maintain its integrity as well as end users' trust in its reliability.

4. The rapid growth of the Internet has created new opportunities for perpetrating cybercrime on a global scale, to exploit the inherent vulnerabilities in constantly evolving technology. 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.

5. The increasing global cyber threats and cyber-attacks already constitute a threat to the national, regional and international peace and security. Cyber threats represent global problems and they need global frameworks as instruments to promote security and stability in cyberspace. Cyber security concerns are broader than national security and yet, few cybersecurity initiatives have been implemented at continental level. A strategy and cybersecurity frameworks based on a common approach and common understanding are needed among Member States of the African Union.

6. Africa is facing several Internet-related challenges in relation to security provisions to prevent and control technological and informational risks; such

threats can only be fully addressed by developing a strong culture of cybersecurity, creating robust response capabilities and enacting appropriate and effective national policies.

7. Considering the multiple dimensions and complexity of Cybersecurity, Protection and prevention against worldwide criminal activities in cyberspace requires cooperation and coordination among a wide variety of stakeholders both within and between countries. In light of the importance of the ICT sector and its positive impact on the social and economic development of the African Countries, there is an urgent need to develop a global approach and coherent strategy on cybersecurity issues at continental level to promote peace and security in the information society.

II: Background:

2.1. The African Union Convention on Cybersecurity and personal data protection

8. To address the legislative challenges posed by criminal activities committed over ICT networks in a regional and continental compatible manner and in response to the need for Harmonized legislations in the area of Cyber Security and Personal Data Protection in Member States of the African Union, the AU 23rd Assembly of Heads of State and Government, held in Malabo on 26-27 June 2014 adopted The African Union " *Convention on Cybersecurity and personal data protection"* know now as The Malabo Convention.
9. The Malabo convention seeks on the establishment of a Legal Framework for Cyber-security and Personal Data Protection and sets broad guidelines for incrimination and repression of cybercrime and related issues. It embodies the existing commitments of African Union Member States at regional, continental and international levels to build an information society that respects cultural values and beliefs of the African Nation, guarantees a high level of legal and technological security to ensure respect of online privacy and freedoms while enhancing the promotion and development of ICTs in Member States.
10. The Convention sets forth the essential security rules for establishing a credible digital environment and strengthening existing legislations on Information and Communication Technologies (ICTs) of AU Member States and the Regional Economic Communities (RECs)**.**

2.2. Recalling the recommendations of the First Ordinary Session of the STC-CICT-1

11. The First Ordinary Session of the Specialized Technical Committee on Communication and Information &Communication Technologies (STC-CICT-1) held in Addis Ababa, Ethiopia, from 31 August to 4 September 2015 requested:

- The African Union Commission to ensure the follow up of the signing and ratification by Member States of the African Union Convention on Cyber-Security and Personal Data Protection and ;
- Member states to accelerate the signature and the ratification of the AU Convention, the development of National Cyber-Security legislations and creation

of national and regional Computer Emergency Response Team (CERT) and/or Computer Security Incident Response Team (CSIRT).

III: Cybersecurity policy priorities for Africa:

3.1 Strategic approach:

12. Cyber security has become a major concern across the world, the sophistication of the cyber-attacks and the monetary damage has been increasing at exponential rates for several years. In fact the rapid pace of innovation in the ICT sector can result in gaps in the legislative and regulatory cybersecurity framework since the challenge for the legislator is the delay in the recognition of the new types of offences and the adoption of amendments to the applicable legislation.
13. Due to the cross border and international nature of Cybercrime, national legislations cannot be drafted in isolation and national governments must seek to harmonize national legislation, regulations, standards and guidelines on Cybersecurity issues in order to create effective regional and international frameworks for fighting Cybercrime.
14. Therefore, Cybersecurity and cybercrime cannot be treated as any other regulatory topic or subject matter. Cybersecurity has become a priority for all governments around the world and many have developed strategies to address the emerging security issues associated with the criminal use and political abuse of ICTs. For African countries there is a need to consider Cybersecurity as significant national and regional problem that affects their sovereignty, their National security as well as the protection of their societies and their critical infrastructures.
15. An effective strategy to combat cybercrime and malicious activities in Cyberspace requires a multi stakeholder approach where the role and responsibilities of government agencies and other potential partners should be defined at higher level. In addition, the strategy must reflect the cultural values and beliefs of the African Nations; it must have a clear set of principles that help frame the decisions about how to identify, manage and mitigate Cybersecurity risks.
16. Finally, the complexity and international dimension of Cybersecurity policy making and the international and regional policy discussions and debates on Cybersecurity for the creation of a global framework on cybersecurity and cybercrime should be taken in account while drafting the national and regional legislations by considering the international instruments and best practices.

3.2 National Cyber security framework:

17. Cyberspace has become an essential component of modern society, yet its merits are accompanied by threats. The growing number of reported cyber-incidents demand governments to come up with a strategic response to counter cyber-threats.
18. African governments are at different level of establishing policy instruments and legislative framework. For the majority, the lack of know-how in terms of cyber

security to monitor and defend national networks and the inability to develop the necessary cybersecurity legal frameworks to fight cybercrime as well as lack of financial resources are the main factors that contribute to making African countries vulnerable to incidences of cyber terrorism and cyber espionage.

19. While many countries have proposed legislations, the level of deployment of security systems in both the private and the public sector is low. To promote Cyber Security culture and achieve effective measures and enhance confidence and security in the use of Telecommunication Networks /ICTs, the AU Member States need to accelerate the ratification and transposition of the AU Convention's provision into their National Cyber-legislations.

20. At continental level there is a need to achieve high degree of harmonized policies, legislations and Regulatory procedures to prevent and fight against illicit use of Internet and ICTs.

21. At National Level, Member states may consider the following actions:

i. Develop National cyber-security strategies, in line with international standards and practices taking into account the AU convention on Cyber Security and Personal Data Protection;

ii. Support the creation of national governance for Cyber-security and defining roles and responsibilities of the stakeholders;

iii. Develop Legal and Regulatory frameworks and specific provisions related to cyber legislations;

iv. Enhance technical capabilities to monitor and defend national networks;

v. Develop National Computer Emergency/Incident Response Teams (CERTs / CIRTs).

vi. Encourage efficient sharing of information and digital evidence on bilateral or multilateral basis;

vii. Protect relevant Institutions and the integrity of critical National Infrastructures against the threats and attacks capable of endangering their survival and efficacy;

viii. Provide long term capacity building and technical assistance to strengthen the national authorities to deal with cybersecurity issues;

ix. Member States that do not have agreements on mutual assistance in Cybercrime to undertake signing agreements on mutual Legal assistance;

x. Designate a focal point to facilitate regional and international cooperation.

3.3 Fighting all kinds of cybercrime at continental level:

22. Cyber threats are evolving and increasing at a fast pace, for preventing and fighting cybercrime, African countries need to urgently scale up efforts to

effectively combat all kind of criminal activities in the African Cyberspace through multi-stakeholder approach involving governments, industry, academia, civil society and organizations in an integrated and comprehensive manner.

23. To counter the criminal use of Internet and ICT networks, African governments may consider the preparation and adoption of complete and effective legislations to enhance cybercrime components within the National Cybersecurity strategy. In addition, the legislations should support the national efforts to ensure an effective criminal justice response to ICT offences.

24. To efficiently investigate and combat Cybercrime at national level, Governments may consider the following actions:

a) Enforce the existing national criminal laws and adapt them to the reality of digital environment to effectively fight against all kind of cybercrime and cyber-attacks;

b) Enhance the capacities of criminal justice authorities, such as law enforcement, Prosecutors and Judges, in order to enable them to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence and computer forensic;

c) Improve procedures for cybercrime investigation, the handling of electronic evidence and cooperation between law enforcement agencies;

d) Facilitate the public/private sharing of information and foster the cooperation between law enforcement and Internet Service Providers (ISP);

e) Evaluate on a regular basis the effectiveness of the legislations and the criminal justice response to Cybercrime and maintain statistics.

3.4 Personal Data Protection (PDP)

25. In today's digital world, personal data have become the fuel that drives much of online activities. Every day a big amount of data are collected, stored and transmitted across the globe.

26. As more and more economic and social activities shifts into connected information space, the importance of data protection and privacy online are recognized as essential for the development of the digital economy.

27. At the same time, the volume of trans-border data flows, more specifically personal data is increasing every year, making data protection regulations a central component of the electronic transactions.

28. In addition to the model laws on data protection developed at regional level within the regional economic communities (RECs), the AU convention embodies a part on the relevance of data protection in the digital environment and highlights the importance to ensure an effective protection of personal data and privacy online and guarantee that any form of data processing within the Member states of the African union respects the fundamental freedoms and rights of natural persons.

29. At Continental level the convention aims to create a uniform system of data processing and determine a common set of rules to govern cross-border transfer of personal data to avoid divergent regulatory approaches between the AU Member States.
30. The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently and in all cases processing of personal data shall be done with respect to the Principle of transparency and confidentiality. To do so, each Member State shall develop a legal and institutional framework for the protection of personal data and establish the national protection authority as an independent administrative authority with the task of ensuring that any processing of personal data is conducted in accordance with the provisions of the Convention within AU Member States.
31. Any interconnection of personal data files should be subject to appropriate security measures to prevent such data from being altered or destroyed, or accessed by unauthorized third parties. National protection authorities shall ensure that ICTs do not constitute a threat to public freedoms and the private life of citizens by regulating the processing of data files, particularly files related to sensitive data and by establishing mechanisms for cooperation with the personal data protection (PDP) authorities of third countries and participating in international negotiations on PDP.
32. Most African Countries lack legislations on personal data protection (PDP), to ensure the online privacy and personal data protection as to allow African citizens to use ICTs and internet for their socio-economic development (Health, education, governance etc.)

To address the data protection issue at continental level it is necessary to implement the AU convention and establish legal and institutional frameworks at national level to create trust online.

3.5 Capacity Building and Awareness:

33. To create an online climate of trust and enable an open sharing of knowledge, information and expertise between African citizens, it is a fundamental challenge for securing networks and information systems and promoting the culture of cybersecurity among all stakeholders, namely, governments, enterprises and the civil society which develop, own, manage, operationalize and use information systems and networks.
34. For protecting the critical infrastructure and to enable the country to respond to the growing number of cyber-threats especially in critical sectors, it is necessary to build national competencies for cybersecurity. Developing knowledgeable workforce is critical to reduce national cyber risks. Every employee in the government or business enterprises should have cybersecurity responsibilities to ensure that systems and networks are adequately protected.
35. While it is important to develop strong cybersecurity skills and awareness for professionals, Member States shall undertake leadership role in the development

of the cybersecurity culture within end users and contribute to sensitize and disseminate information to the public.

36. The national strategy should identify an agency or entity for raising public awareness on the several threats when using computers and this should include improving the human capacities of the individual users by providing training and education on the measures that they can take in their everyday life to ensure the safe use of cyberspace.

37. As part of the promotion of the culture of cyber security, Member State may adopt the following measures:

i. Elaborate and implement programs and initiatives for sensitization of users on the security of systems and networks within national institutions;

ii. Encourage the development of cyber-security culture in enterprises and foster the involvement of the civil society;

iii. Launch comprehensive and detailed national sensitization programs including public awareness campaigns and preventives measures at all levels to mitigate Cyber risks for Internet users, small business, schools and children;

iv. Set up national efforts on training and education by introducing Cyber Security degree programs or classes in universities and academic institutions.

3.6 Enhancing Regional and International Cooperation:

38. The world today is complex, globalized and above all dominated by the intensive use of ICT devices, infrastructures and services. The growing dependence on ICTs and the interconnection of critical infrastructures have introduced new vulnerabilities for the societies and made the security of cyberspace essential for the functioning of modern states.

39. Nowadays, Information Technologies have become the common denominator for all disciplines; everyone is using the same Internet for private, personal and professional applications, for health, education, energy and even for personal safety and security. This has raised the level of complexity of how we can secure, protect and defend our vital activities carried out at political, economic, societal and individual levels.

40. In this context, there is a necessity to understand that cyber risks have become a planetary emergency amplifying the traditional risks like terrorism and there is a necessity to act in consequence to tackle the security challenges of the digital era.

41. While a peaceful cyberspace provides us with many opportunities, it is reported that more than 100 states are actively developing military cyberspace capabilities, a prospect which threaten both the national and international security .The key aspect of cyber tools is the difficulty of attributing an attack to its perpetrators or sponsors and the dual use of the technology.

42. The International cooperation on Cybersecurity refers to inter-governmental efforts to prevent the use of ICTs in a way that will affect international peace and

security. There is an ongoing international debate on establishing international regulation and code of conduct or norms of state behavior in Cyberspace and its relation to the international security.

43. To promote the international stability in the global cyberspace and achieve a common understanding on cyber issues based mainly on transparency and online confidence, The UN Group of Governmental Experts (UNGGE), agreed in June 2013, on a consensus report where it is stated that international law, especially the UN Charter, is applicable in Cyberspace. In addition, the group agreed that confidence building measures and high level communication and timely information sharing can increase trust and assurance among states. The group also highlighted the importance of capacity building to enhance the international cooperation in securing the cyberspace and reaffirmed the importance of the getting an open, free and secured global cyberspace as it is an enabler for economic and social development .

44. In line with the international discussions, an effective response to the Cybersecurity complex issues cannot be addressed effectively on a purely local level; it requires transnational cooperation by developing an appropriate cybersecurity culture and by enhancing complementary and coherent measures in a holistic and global way. At a continental level, it is essential to promote exchange of information and communication between countries at foreign policy level (not only technical) and developing cyber diplomacy capabilities and holding consultations in order to reduce the risks of criminal use of ICTs, notably the cyber espionage and Cyber terrorism. A continental and harmonized approach on the main cybersecurity issues is required from a strategic perspective to enhance regional, continental and international cooperation that are necessary in cross-border investigating and prosecuting of cybercrime.

45. The global and harmonized approach shall provide the African Countries a clear understanding for the future risk and vulnerabilities in smart technology and the Internet of Things (IoT) and support the countries to create a secure and resilient Cyber environment by providing assistance in developing the key components of a national cyber security framework required to prevent and counter all malicious activities carried out over Internet.

46. To combat global cyber-attacks, cybercrime and abusive or inappropriate uses of the ICT networks, and in line with the existing international cooperation mechanisms and best practices, the African Union Commission, Regional Economic communities and AU specialized institutions may adopt the following measures:

i. Develop Regional mechanisms for sharing experiences and best practices on Cybersecurity issues between AU Member States to increase Regional and International cooperation;

ii. Develop Regional Computer Emergency/ Incident Response Teams (CERTs / CIRTs); and promote the formal and informal exchange of information;

iii. Work with Member States on the harmonization of the Cybercrime Laws at regional and continental level and strengthen law enforcement cooperation both at regional and continental levels;

iv. Design a model for cybersecurity capacity building which takes in consideration all aspects (policy, technology, skills development…) and can be easily adapted to Member State's needs;

v. Support inter-governmental organizations and private companies to achieve norms and standards for exchanging of information during the investigation and prosecution of transnational cybercrimes;

vi. Encourage AU Member States in developing cyber diplomacy capabilities and Participating in discussions carried out at international level such the UN Group of Governmental Experts.

IV: <u>Conclusions and Recommendations</u>:

47. The expanding use of Information Communication Technologies and the increasing access to internet for delivery of services like e-government, banking, healthcare or education has inevitably resulted in the emergence of risks related to Cyber-attacks, which occur rapidly and spread across the globe in minutes regardless of borders, geography, or national jurisdictions and Africa accounts for 10% of the global cyber incidents.

48. Cybercrime cannot be defeated by any law or convention alone, it has become clear that the collaboration of all stakeholders in the governance and operation of the Internet is required to protect the security and privacy of the Internet users. A secure and safe digital environment is a shared and collective responsibility within the continent and it is a necessary condition for reaping the benefits of the digital transformation of Africa and supporting its positive impact on human and economic development.

Recommendations:

49. **At national level :**

a) Accelerate the ratification and implementation of the AU Convention on Cybersecurity and personal data protection; (1).

b) Develop a National Strategy on Cybersecurity and an operational action plan for combating cybercrime and cyber terrorism;

c) Draft or review the cyber legislation to criminalize the offences related to the illicit use of ICTs;(1)

d) Create national Computer Emergency Readiness Teams (CERTs) for monitoring networks and exchanging best practices on their effective utilization and collaboration; (1)

e) Develop legal and institutional frameworks for personal data protection and establish the national protection authority;

f) Develop and promote robust culture of cybersecurity that recognizes and effectively responds to the global threats and challenges associated with Internet, the interconnected mobile networks and related technologies;

g) Develop cyber diplomacy capabilities and Participating in discussions carried out at international level such the UN Group of Governmental Experts.

50. **At Régional Level:**

a) Establish Regional Cyber Security Centers with the aim to serve as catalysts for enhancing regional cooperation, coordination and collaboration to address the escalating Cyber threats;

b) Develop Regional Computer Emergency/ Incident Response Teams (CERTs /CIRTs); and promote the formal and informal exchange of information between countries; [(1)]

c) Work with Member States on the harmonization of the Cybercrime Laws at regional and continental level and strengthen law enforcement cooperation both at regional and continental levels.

51. **At Continental Level:**

a) Develop a global and harmonized approach on the main cybersecurity issues and promote the creation of a secure, robust and resilient Cyber environment at continental level;

b) Promote dialogues within the Cybersecurity actors in Africa and coordinate all the initiatives related to Cybersecurity.

1: Part of the recommendations of the First Ordinary Session of the STC-CICT-1