Theme "Towards an Open, Safe and Secure COMESA Cyberspace"

2-3 July 2015

INTRODUCTION

The rapid development of Internet and other information systems has given rise to a completely new economic sector and to new rapid flows of information, products and services across the internal and external borders in Africa. This has opened many new possibilities for criminals. A pattern of new criminal activities against the Internet, or with the use of information systems as a criminal tool, is clearly discernible. These criminal activities are in permanent evolution, and legislation and operational law enforcement have obvious difficulties in keeping pace. The cybercrimes are extremely variable computer scams: fake proposals of goods and services, hacker attack services, scams related to payment cards and accounts of electronic payment systems. The users of online auctions constitute 43% of victims. The other crimes are related to so-called black brides. The number of fake deals through the Internet shops is growing, where the payment is processed by the systems of WebMoney. New methods of electronic blackmail appeared.

The cyberspace is important to nearly all aspects of national life. Therefore, a secure cyberspace is vitally important to the nation, but cyberspace is far from secure today. New technologies and policies and their effective implementation can make cyberspace safer and more secure. Confidence and security in using ICTs are fundamental in building an inclusive, secure and global information society. Confidence and security are vital to use ICTs effectively, as acknowledged by the World Summit on the Information Society (WSIS). It will be also important to uphold human rights and the rule of law in cyberspace.

Background

The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. Current attempts to address these challenges at the national and regional levels are inadequate, as cyberspace is boundless and limited only by human imagination. The

boundaries of the information society have no direct correlation with existing geographical borders – cyber threats can arise anywhere, at any time, causing immense damage in a very short space of time, before they are tackled. To face these challenges there is a need to:

- developing a culture of cyber security
- demystify cyber security
- fostering regional co-operation
- encouraging and promoting information sharing

A regional framework through ARICEA is required to address cyber security concerns which are:

- Costs in ensuring cyber security;
- Rapid advances in deployment of new technologies (NGN standards, etc.); and
- Mapping legal and regulatory instruments with existing and new technologies.

COMESA has developed and adopted cyber security policy and legislation. Extensive work has been done on the public key infrastructure protection. An assessment of the current situation of cyber security report will be presented to the forum in addition to regional cooperation agreement, cyber security board establishment.

OBJECTIVE

The main objective of the Forum is to contribute to harmonization, consolidation and support for the regional and national efforts in strengthening the safety, security and resilience of COMESA Cyberspace. The specific objectives are:

1. Raise awareness of and train the policy makers, regulators, judges, prosecutors, police, investigators and security officers;
2. Assessment of cyber security current status in Member States;
3. Motivate development and adoption of regional cooperation agreement on cyber security
4. Facilitate establishment and operation of the COMESA Cyber Security Centre under

the umbrella of ARICEA

5. Motivate establishment of regional framework and mechanims for certificate authorization;
6. Establish a relation with Council of Europe for cooperation and support
7. Develop and adopt PKI regulations;

Expected Results

The expected results are:

- Awareness raised and stakeholders trained on cyber security;
- Stakeholders motivated to use ICT applications
- Identifications of cyber security gaps in Member States;
- Adoption of Regional cyber security strategy and update the Cyber security implementation road map;'
- Adoption of the PKI regulations;
- Adoption of the Criteria for regional and mutual recognition of Certificates for PKI;
- Adoption of regional cooperation agreement on cyber security; and
- Modelaties for cooperation with Council of Europe agreed upon.

MAIN TOPICS

The main topics of the forum will be as follows:

- Policy, regulatory and strategy framework

- Assessment of the COMESA region
- Development of policy and regulatory framework and institutional set up
- Judiciary system development in areas of enforcing legislation and regulations, prosecution, investigation, fighting against cybercrime and forensics
- Customer Safety, Security, Privacy and data protection

- Lessons learned in the design of National Cyber Security Strategies
- Model for Regional Cyber Security Strategy
- Establishment of the COMESA Cyber Security Center(CCSC)

- CERTS and cyber security in Eastern and Southern Africa

- Status of setting up CERTs in COMESA region
- Impact and operational needs
- Best practices in the region

- Cyber attacks and defences in critical infrastructure

- Necessary institutions and regulations for PKI
- Protecting National Critical Infrastructures from Cyber Threats
- Cyber security and finance sector e.g banking, Insurance
- Critical infrastructures increasingly impacted by cyber-attacks: Airports and energy cases.

- Criteria for the CAs regional and mutual recognition towards having a regional Certificates Authority
- Security Standardization

- **Security implications and adoption of evolving technology**
- Current Threat Landscape
- Advanced Persistent Threats
- Mobile Technology—Vulnerabilities, Threats and Risk
- Consumerization of IT and Mobile Devices
- Cloud computing security
- Digital Collaboration
- Knowledge Check

- Cybercrime: the cost of crime—the benefits of cooperation

- Regional and international cooperation for security and resilience in Cyberspace;
- Regional Cooperation agreement;
- Multilateral Legislative Frameworks: An Analysis of Budapest Convention
- Changing Legal Landscape in Cybersecurity: Implications for Business
- How Today's Security Leaders Leverage Event Metadata, Frequency and Relationships to Make Better Decisions

- ICT applications and E-Government

- E-payment
- E-services
- Digital signature
- Internet of Things (IoT)

PARTICIPANTs

The expected participants are policy makers, regulators, judges, investigators, prosecutors, police, security officers, private sector and non-governmental organization. The regional and international players such as ITU, AUC, ATU, UNECA, ADB, USAID, EU, will participate.

DATE AND VENUE

The venue will be Nairobi, Kenya and the date is 2-3 July 2015.