



UNECA

Sub Regional Office For Eastern Africa

SRO-EA

2010 EAIGF

11-13 August 2010, Kampala, Uganda

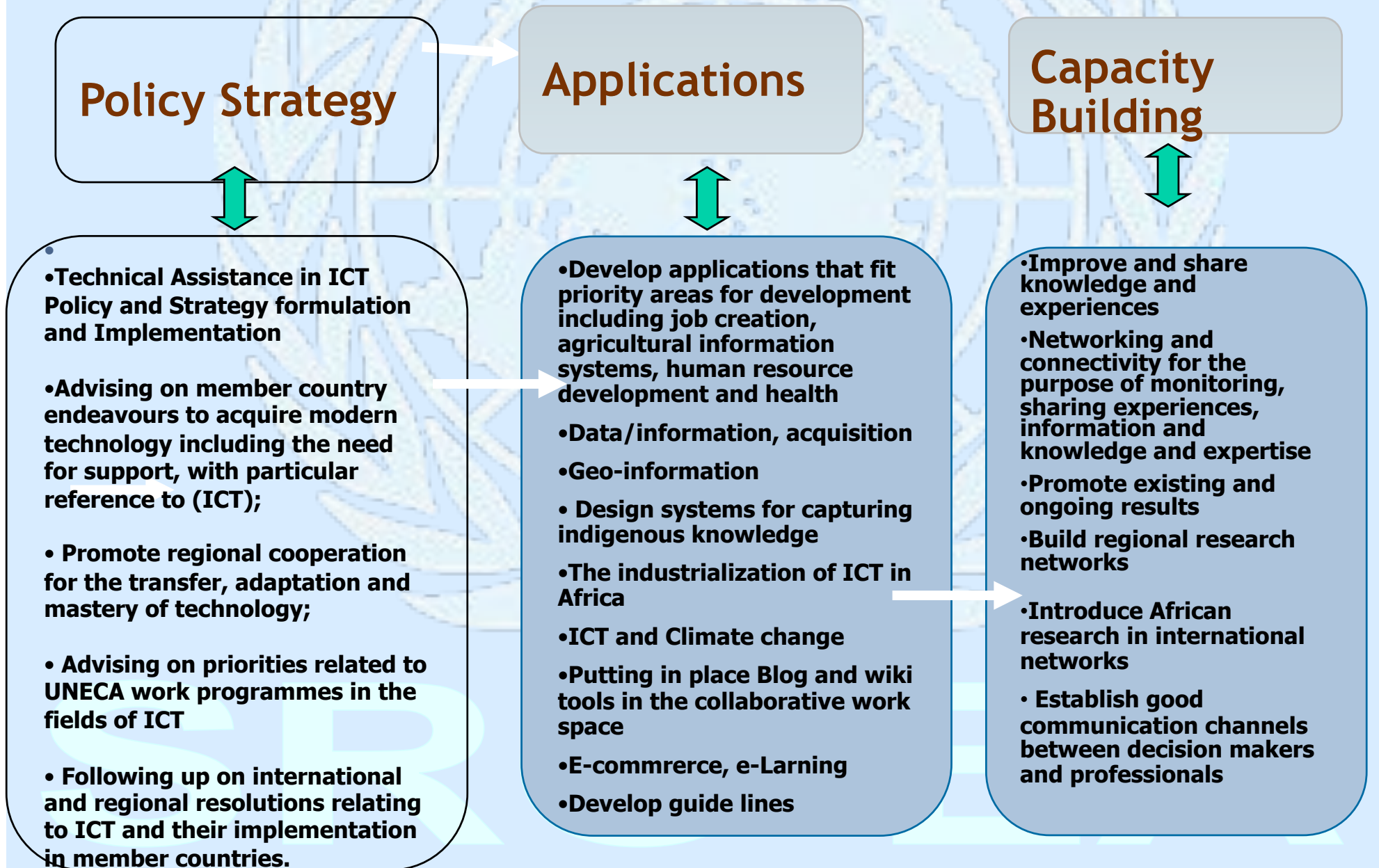
SRO-EA's Cyber security Initiatives in Eastern Africa

Mr Mactar SECK

United Nations ECA SRO- EA

SRO-EA

Key Categories on ICT in ECA/SRO-EA work Programme



Institutional framework

information

background



WSIS Action Lines (International partnership)

- **C1: The role of public governance authorities and all stakeholders in the promotion of ICTs for development**
- **C2: Information and communication infrastructure**
- **C3: Access to information and knowledge**
- **C4: Capacity building**
- **C5: Building confidence and security in the use of ICTs**
- **C6: Enabling environment**
- **C7: ICT Applications: e-government, e-business, e-learning, e-health, e-employment, e-environment, e-agriculture, e science**
- **C8: Cultural diversity and identity, linguistic diversity and local content**
- **C9: Media**
- **C10: Ethical dimensions of the Information Society**
- **C11: International and regional cooperation**

SRROEA

Implementation of WSIS Action Line 5 in Africa

Building confidence and security in the use of ICTs

- **The WSIS Action Plan recommends**

“cooperation among the governments at the United Nations and with all stakeholders at other appropriate forums to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues”

SRO EEA

AISI and e-Security

Security is vital for trust and confidence in the Information Society and must be considered at all layers. This includes:

- Information Security Management;
- Standards of Information Security;
- Threats and Attacks to Information;
- Education and Curriculum for Information Security;
- Social and Ethical Aspects of Information Security;
- Information Security Services;
- Applications of Information Security;
- Infrastructure for Information Security;
- Legislation for Information Security;
- Modeling and Analysis for Information Security; and
- Tools for Information Security.

What is e-security policy?

- A plan of action for tackling security issues, or a set of regulations for maintaining a certain level of security
- Practices for securing computers, buildings, or vital infrastructure
- Strategies articulated at both the organizational & national
 - Organisational level - a high-level document outlining management commitment to IT security by defining IT security & its supporting sub-policies;
 - National level - a government's approach to ensuring the security of its national interests through legislation, regulations, training, investment & awareness

SRO EEA

ECA Survey on the implementation of WSIS Plan of Action

ICT Security Issue	Addressed in the country ICT policies and plans	Existence of Legislation to enforce this issue
Information security and network security issues	58%	12%
Education and raising awareness on security and use of ICTs	58%	18%
Prevention, detection and response to cyber-crime and misuse of ICTs	50%	2%
Effective investigation and prosecution of misuse of ICTs	43%	1%
Government to actively promote user education and awareness about online privacy and the means of protecting privacy	47%	1%

Deployment of ICT Security and Level of Awareness

- The level of deployment of security systems in both the private and the public sectors to combat cyber-crime is low
- Most countries also rated the level of awareness of ICT-related security issues, with some of the relevant initiatives only just beginning

SRO EEA

Top Concerns

- Lack of publicly stated National Information Security Policy.
- Lack of trained & qualified manpower.
- Non existent or weak institutions.
- Lack of Assurance framework (standardization, Accreditation and Certification)
- Lack of awareness & culture of cyber security

SRO EEA

An African Cyber Security Strategy

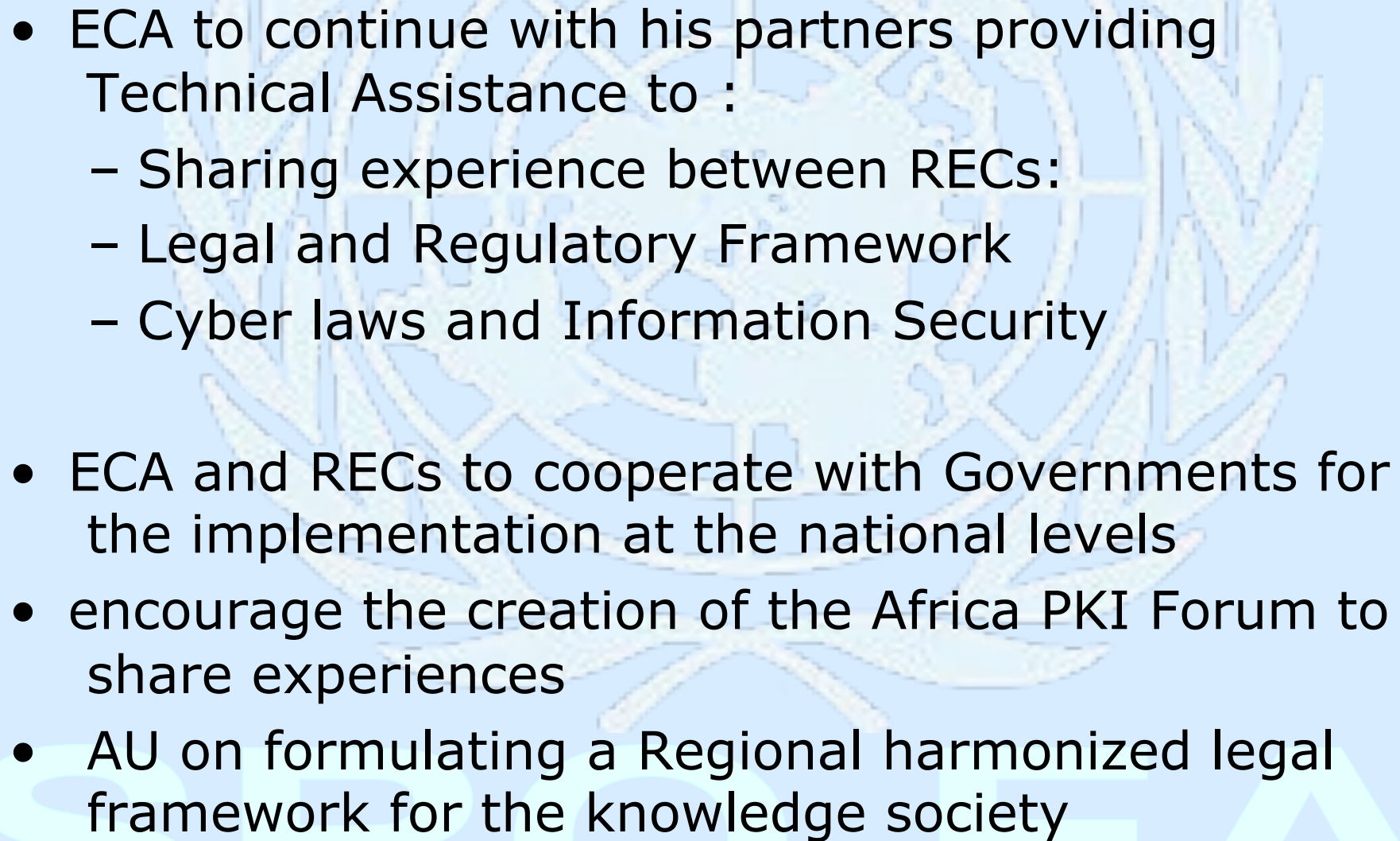
- **ECA** involved in the development of a cyber security framework fora programme that looks at the policy, legislative, regulatory and infrastructure requirements;
- Policy requirements set out duties and responsibilities of the various domestic, regional and international stakeholders and beneficiaries of this security policy;
- Legislative and regulatory requirements - sets limits, establishes a code of conduct, defining standards and some of the technical issues which may be imposed on stakeholders such as service providers, financial institutions, vendors/merchants, as well as work towards building the necessary trust and confidence demanded by users, key stakeholders, both within Africa and from around the world.
- Infrastructure requirements will provide for minimum security standards and ensure providers are able to address the evolving demands of users and protect their networks against increasingly sophisticated attacks, originating from around the world.

Concrets ECA initiatives

- Harmonized Legal Framework for the Knowledge Society
 - ECA provided Assistance to EAC on formulating an ICT harmonized legal Framework
 - Assistance is requested from other RECs to adapt the Framework
- Cooperation with the AU for a regional harmonized legal Framework for the knowledge society including guidelines on :
 - Cybercrime
 - Personal data protection
 - Electronic Transactions
 - e-Signature/ Certification
 - Cybersecurity

SRRO EEA

- 
- Cooperation on cybersecurity
 - Assistance on the formulation of national Cybersecurity Policies for :
 - Project for cooperation on cybersecurity in the Eastern Africa
 - Trainings Courses (Crackers/Hackers, Telephones and Computer Attacks, CCTLD, cybersecurity Policy, etc.)
 - Understand the Internet and its protocols
 - Useful methods and best practices for assessing operational risk to a ccTLD
 - Preparing basic attack and contingency response plan
 - Formulating a contingency communication plan for a ccTLD
 - Experience building network systems
 - ECA launched an African Cyber Security Strategy programme in Kenya to strengthen member States' capacities to meet policy, legislative, regulatory and infrastructure requirements
 - Launching of the Academy for ICT Essentials for Government Leaders in Africa

- 
- ECA to continue with his partners providing Technical Assistance to :
 - Sharing experience between RECs:
 - Legal and Regulatory Framework
 - Cyber laws and Information Security
 - ECA and RECs to cooperate with Governments for the implementation at the national levels
 - encourage the creation of the Africa PKI Forum to share experiences
 - AU on formulating a Regional harmonized legal framework for the knowledge society

Conclusion

- Cyber security is shared responsibility of government, service providers, software and hardware makers, and users (large and small)
 - Government Policies should Identify short and mid term security objectives, support to key players, investments in security technology and training, and awareness initiatives
 - Industry Policies should address acceptable usage, minimum security standards, and commitments by organisation to educate and support users
- Cyber security strategy has many components:
 - industry standards and best practices
 - information sharing
 - awareness, education
 - R&D
 - obligations under civil law
 - criminal law

SRRO EEA

WAY FORWARD

- Launching KM Platform : November 2010
- Design and Implement Regional ICT Cybersecurity Project
- AEGM Outcomes WSIS+5 for Eastern Africa Countries :
 - Djibouti February 2011
 - ICEICT Meeting

SRD EEA