



## Workshop on the Harmonization of the Legal Framework for Cybersecurity in North Africa

Rabat, Morocco, 27-28 July 2010

### Aide-memoire

Societies of Africa Region, like societies in other parts of the world, rely more and more on information and communication technologies and are thus vulnerable to threats such as cybercrime.

Criminals such as hackers, organized crime groups, and terrorists see the potential of the ICT to facilitate their crimes. Meanwhile, consumers hesitate to transmit personal and credit card data across the Internet, with security and privacy their number one concern, and businesses face major losses of proprietary data, intellectual property, and online access to customers and suppliers due to security breaches.

Without appropriate criminal laws and regulations, as well as the law enforcement capability to investigate domestically and cooperate internationally, economies can become attractive as havens for bad actors, repositories for criminal data, and centres for money laundering and terrorist activities.

In order for the ICT to contribute to economic growth, human development, and democratization, it must be trustworthy and secure. A lack of trust and security jeopardizes many developments that could be supported by a widely accessible and widely trusted knowledge Economy and society.

- Growth of e-commerce -- among businesses and between businesses and consumers;
- Attraction of the foreign investment necessary to business creation, modernization of infrastructures, and innovation – capital will not flow to countries whose legal systems are unresponsive to computer security issues;
- E-government – efforts to make government more responsive and accessible are threatened by security glitches and fear of abuse;
- Job creation though development of "back-office services" – global companies seeking lower labour costs for data entry and "back room" data processing activities will not send their data to countries where the law leaves it unprotected;
- Critical infrastructure reliability – even in developing countries, power generation and distribution, transportation, banking, government, and health care operations are increasingly dependent on information systems;
- Protection of personal privacy and proprietary data – the communications and stored data of businesses and individuals alike must be protected from both illegal interception/access and arbitrary government surveillance;
- Development telemedicine and health care centres – people in underserved populations will not trust their medical information to an insecure communications medium;
- Use of information technology for distance learning – unemployment services, enhancement of workforce skills, and the development of small and medium-sized enterprises.

ECA have recognised the need to address this challenge at national sub regional and regional levels.

In this context SRO-NA and ISTD in collaboration with Council of Europe (COE), Microsoft joined forces to hold a workshop on the harmonization of legislation for cybersecurity in North Africa. That event will involve an analysis of current Cyber legislation in North Africa countries and identifies needs for reform.

The Workshop will help sharing experience in terms of the measures taken in different countries, to provide support and advice to reforms underway, and to discuss a plan of actions and measures to complementing legislation such as training and cooperation with service providers.

**The Workshop will concentrate on the harmonisation of the legislation on cybercrime, as a part of the cybersecurity agenda and the global effort for establishing confidence and security on the Knowledge Economy and Society.**

### **Objectives**

The objective of the Workshop is to support the strengthening and harmonisation of cybercrime legislation in North Africa Countries in line with international standards.

The proposed workshops would enhance participant's knowledge of legislative measures necessary to address crimes involving computers and the Internet. Attendees would assess the current state of their substantive and procedural laws, and then discuss the development (or refinement) of a legal framework for the investigation and prosecution of cybercrime.

The workshop will assist North African countries meeting their WISIS commitments to endeavour to enact comprehensive legal frameworks to combat cybercrime and enhance cybersecurity and identify or develop law enforcement cybercrime units capable of providing international assistance.

By the end of the Workshop, participants should:

- Have a better understanding on how to draft legislation on cybercrime;
- Have carried out an analysis of their cybercrime legislation as reflected in updated country profiles;
- Have identified the steps to be taken to further strengthen their national legislation;
- Be familiar with good practices regarding the cooperation between law enforcement authorities and internet service providers that may also be useful for North Africa countries; and
- Be familiar with concepts for the training of law enforcement, prosecutors and judges in matters related to cybercrime and electronic evidence;
- A concerted Plan of action for the implementation of an harmonised cyber legislation in the North African participating countries.

### **Participants**

Delegations will include experts in cybercrime from law enforcement, justice ministries, and policy makers, including experts from legislative bodies, courts, and academia. They will directly benefit by receiving valuable information and assistance in the development (or refinement) of comprehensive legal frameworks.

### **Content**

The deliverables of the workshop will be 3 days workshop that will include:

- An overview of emerging threats and the trends in criminal activity relating to the ICT.
- Discussion of existing multilateral cybercrime and cybersecurity efforts and how this work can be utilized to meet countries objectives.
- Discussion of legislation needed for gathering and using electronic evidence, as well as for improving international cooperation in cybercrime matters.
- Comparison of North Africa countries current laws with the Convention on Cybercrime;
- Discussion of the Countries previous efforts to develop comprehensive frameworks and experiences with particular statutory language; and
- Review, discussion, and refinement of existing draft legislation and way for harmonisation.
- Discuss and propose a plan of action for the harmonisation of the cyber legislation in North Africa

### **Langue**

The workshop sessions will be conducted in French, with simultaneous interpretation into Arabic.

### **Venue and date**

Rabat, Morocco, 27-28 July 2010

### **Contacts**

Mohamed Timoulali

Regional Adviser

ECA Office for North Africa

Tel + (212) 537 71 78 29 - Fax + (212) 537 71 27 02

E-mail mohamedt@uneca.org