



## **Building trust and security in the use of ICTs**

### *Executive summary*

During the last years, the Arab countries have achieved successful developments in the areas of information and communication technologies and have displayed significant interest in technology initiatives. However, Arab States are facing several challenges in addressing cyber threats and implementing appropriate legislative frameworks and national infrastructures to effectively combat cyber threats. The following areas have been analyzed and the main issues have been highlighted:

#### **a) National and Regional Regulatory policies and frameworks for data privacy and fight cybercrimes:**

- Legislative prescriptions concern specific cyber threats and are mostly linked to e-commerce.
- In some countries there is no comprehensive Cybersecurity law enacted or adopted yet.
- Regional cooperation is critical to fight cybercrimes and no special laws counter them.
- Incorporation of international standards in national legal systems avoids the evolution of legal "safe havens".

#### **b) Establishment of national Computer Incident Response Team (CIRT) and their coordination**

- Few national centers for fighting cyber attacks: some of them are a top priority of the agenda; some others will be done after setting up legislative and regulatory framework.
- Two big regional initiatives, i.e. Cooperation Council for the Arab States of the Gulf – computer Emergency Response Team (GCC-CIRT) and Organization of Islamic Cooperation would help to coordinate national Computer Emergency Response Team.

#### **c) Protection of Arab children and youth from harmful content on the internet**

- Some countries have actively addressed these issues of protecting children online, promoting online safety at the national level.
- Other countries still need to develop their national strategies on child online protection such as proactive measures, common standards, legislation or raising awareness.

### **Summit Objectives**

1. Establishment of national legal frameworks harmonized at the regional level in all Arab countries, within the period of 5 years
2. Establishment of Computer Incident Response Teams (CIRTs), in the Arab countries that do not have it, within the period of 3 years
3. Development of a national cybersecurity strategies, aligned with international cooperation principles, including Critical Information Infrastructures Protection (CIIP), within the period of 5 years
4. Establish cybersecurity related curriculum aimed at build capacity and raise awareness in the various constituencies (e.g. Governments, Academia, Private Sector, Schools).
5. Establish a pan-arab agreement on cybersecurity and cybercrime, harmonized with existing international norms and principles, and in support to global cooperation on the topics
6. Emphasize the importance of Child Online Protection (COP) and safety of children and youth, through awareness programmes and establishment of technical measures

\*\*\*\*\*