Capacity Building Workshop on Promoting a Safer Cyberspace in the Arab region

Muscat, Oman, 8-9 December 2014

Preliminary Information Note

1. Background

A safe and reliable cyberspace is considered as one of the pillars of building trust in information and communication technologies (ICT), whether it is the Internet, e-services, or ICT applications. Building trust in cyberspace is crucial to further the Information Society and achieve overall socio-economic development.

Unfortunately the benefits of cyberspace can potentially be marred by malicious activities that jeopardize the safety of systems, data, networks, and users. By the end of 2013, the number of Internet users exceeded 2.8 billion[1] and it is estimated that, by the year 2020, the number of networked devices will be six times the number of users[2]. With the ever-growing importance of cyberspace in daily life and the continuous development of new technologies that depend on it, such as cloud computing and social media, the effects of malicious acts could be devastating and far-reaching. As such, in order to safeguard the cyberspace, it is important to develop measures to combat cybercrime and to promote and improve cybersafety.

Cybercrime and cybersafety are complex issues that require action, national and regional, through the development of frameworks and integrated approaches that include policies, legal and regulatory frameworks, procedural laws, institutional structures, human resource capacities, harmonization of efforts and data-exchange. Combating cybercrime and enhancing cybersafety for individuals and groups, such as children and women, is not just the responsibility of a few, but rather all stakeholders that make use of or provide service via the cyberspace. Such stakeholders include government, private sector, civil society and educational institutions.

ESCWA has been involved with issues related to cybersafety and cybercrime since 2009 with the project entitled "Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World" that had produced a set of directives designed to assist Arab countries in the development of national cyber laws and to harmonize cyber legislation at the regional level. These directives were further

[1] Source: Internet World Stats, December 31, 2013, http://www.internetworldstats.com/stats.htm
[2] Source: UNODC, Comprehensive Study on Cybercrime: draft. February 2013.

supported with the development of a policy note titled "Development and Harmonization of Cyber Legislation in the Arab Region". In continuing the work done by ESCWA in this area a new study has been completed titled "Policy Recommendations on Cybercrime and Cyber Safety for the Arab Region", which specifically looks at the issues and complexities of combating cybercrime and promoting cybersafety in the Arab region.

The ITU Regional Cyber Security Center was established by the International Telecommunication Union (ITU) and the Omani Government, represented by the Information Technology Authority, within the framework of the ITU-IMPACT initiative, with a vision of strengthening the role of ITU in building confidence and security in the use of information and communication technologies in the region. The Regional Cyber Security Center acts as ITU's cybersecurity hub in the region localizing and coordinating cybersecurity initiatives and it is hosted, managed and operated by Oman National CERT (OCERT).

With the growing number of threats levelled against all sectors in the community national and regional stakeholders in the Arab region should collaborate to protect not only their data networks and information, but also the citizenry. Cybercrime and the need for cyber safety is an issue that the nations of the region should not ignore.

2. Objectives

The main objective of the workshop is to build the capacity of decision makers in governments and Non Governmental Organizations (NGOs) in the Arab region on the procedural framework for implementing cybercrime law, combating cybercrime and enhancing cybersafety in the Arab region. It will also address regional and international cooperation for the implementation of national and regional policy for promoting cybersafety in the Arab World.

The participants of this workshop will also discuss the new challenges in cybercrime and cybersafety resulting from new emerging technologies, such as cloud computing, social media and the Internet of Things. Furthermore, this workshop will serve as a platform for the exchange of ideas, knowledge and good practices on issues related to cybercrime and cybersafety, and will promote inter-institutional networking and dialogue.

3. Topics

Following is a list of proposed topics that will be discussed during the course of the workshop on cyber safety and cybercrime:

(1) Policy recommendations and regional framework for promoting safer cyberspace and combating cybercrime in the Arab region – based on ESCWA's recent study.

(2) The status of legal and procedural measures for enhancing cybersafety and combating cybercrime in the Arab region.

(3) The challenges facing cybersecurity in light of recent technological developments and a review of selected technical solutions for protecting the cyberspace and ensuring cybersafety.

(4) Statistics related to the proliferation of cybercrimes in the Arab region and presentation of selected good practices on handling and managing threats for enhancing safety on cyberspace.

(5) Options to raise awareness and build capacity on confronting cybercrimes and promote cyber safety, using cases from the region and the international community.

(6) National, regional and international multi-stakeholder collaboration for promoting safer cyberspace in the Arab region.

(7) The economic aspects and impact of cybercrime.

4. Outcomes

The expected outcomes of the workshop are:

(1) Increased capacity of decision makers in developing procedural and legal frameworks for enhancing cybersafety and combating cybercrime.

(2) Increased knowledge on the status of procedural measures for cybercrime and cybersecurity in the Arab region.

(3) Exchange of knowledge, ideas, and expertise among the participants on good practices and success stories necessary to advocate for effective national policies for cybersecurity.

(4) Raised awareness on potential cyber-threats that are resulting from new technological trends.

(5) Networking and improved opportunities for collaboration and cooperation in the fight against cybercrime and the promotion of cyber safety in the Arab region.

5. Participation and registration

Participants in the workshop will include decision makers from governments, representatives of NGOs, and the private sector involved in enhancing cybersecurity and confronting cybercrime in the Arab region. Experts from international and regional organizations will also contribute to this workshop, as well as experts from national and regional CERTs.

Participants are requested to register for the workshop by filling out the registration form and returning it by email, to escwa-ictd@un.org and dimassi@un.org before **20 October 2014**.

6. Organization, venue and dates

The workshop is jointly organized by the Technology for Development Division (TDD) at ESCWA and the Information Technology Authority in Oman. The workshop and will be held from 8 to 9 December 2014 at the Crown Plaza Hotel, Muscat, Oman.

It will include a number of general presentations and case studies from selected ESCWA member countries on the above topics as well as discussion sessions focusing on cybercrime and cyber security in the region.

7. Working language

Arabic and English are the working languages of the workshop. Simultaneous interpretation between both languages might be provided.

8. Travel and accommodation

All participants are expected to inquire on their visa requirement to Oman and secure one ahead of their anticipated travel date. ESCWA will cover the travel and daily subsistence allowance (DSA) of one participant from invited organizations in selected countries, especially least developed countries.

9. Additional information

Further information and documentation is available at the following URL:
http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=3518E

Inquiries and request for additional information from ESCWA should be addressed to:

Ms Nibal Idlebi
Chief of Section
Innovation Section
Technology for Development Division, ESCWA
Tel: +961-1-978540
Fax: +961-1-981510
Email: idlebi@un.org

Ms HaniaDimassi
Research Assistant
Innovation Section
Technology for Development Division, ESCWA
Tel: +961-1-978546
Fax: +961-1-981510
Email: dimassi@un.org

Inquiries and request for additional information from the ITA should be addressed to:

Ms Rahama Al Barashdi
Cyber Security Training & Awareness Specialist
Oman National CERT
Information Technology Authority
Tel: + 968 24166882
Email: Rahma.albrashdi@ita.gov.om

Ms Ruqiya Al Tobi
Cyber Security Executive
Regional Cyber Security Center
Information Technology Authority
Tel: + 968 24166554
Email: Raqiya.AlTobi@ita.gov.om