Asia-Pacific Regional Workshop on Fighting Cybercrime

Seoul, Republic of Korea, 21-23 September 2011

Meeting Outcome Statement

Recognizing

- that there is a need for the criminalization of cybercrime including conventional crimes facilitated by electronic means;
- that there is a need for top level political commitment to support counter-cybercrime efforts;
- that participating countries are at different stages of development in countering cybercrime;
- that there is a need to acknowledge the importance of cooperation and coordination amongst different stakeholders at the national level;
- that there is a need to develop regional and international consensus and standards regarding cybercrime and digital evidence gathering;
- that there is a need to enhance emphasis on cooperation, nationally (public – private entities), regionally as well as internationally (international partners);
- that there is a need to ensure emphasis on education and prevention of cybercrime;

The meeting agreed as follows:

1. that – as a first step – countries are encouraged, where needed, to elaborate and undertake a comprehensive assessment of cybersecurity and cybercrime at the national level;

2. that for countries which are at the start of their response to the threat posed by cybercrime, a holistic approach should be adopted encompassing

   - Capability building: by ensuring necessary training for all relevant law enforcement officials prosecutors, judiciary, policy makers, regulators and technical organizations;

   - Establishing the legal framework: focusing not only on criminalization of cybercrime but also enacting laws on procedure, evidence , mutual legal assistance and extradition. Additionally, traditional criminal laws and other relevant laws should be reviewed to ensure applicability to the Information Society;

   - Cooperation: building partnerships between stakeholders such as those in the policy making and regulatory authorities, criminal justice system, private sector and civil society to effectively combat cybercrime; and building regional and international cooperation mechanisms between national law enforcement and prosecutorial agencies while leveraging and strengthening existing cooperation frameworks (e.g. Interpol's 24/7 network etc.);

   - Public awareness: giving due emphasis to educating service providers and users thereby preventing cybercrime;

3. that for countries which have a longer track-record of efforts to counter cyber crime, in addition to the above, their response should undertake legislation and capacity review to ensure countermeasures to the newer threats such as (a) ID theft, (b) online child sexual abuse and exploitation and (c) content crime (e.g., hate speech, etc.);

4. that countries – regardless of their stage of response – should pursue a multi-disciplinary approach at national level comprising of all relevant stakeholders dealing with legal, law enforcement, forensics, policy making, industry, education and civil society. This should include

developing capability for rapid response to coordinated cyberattacks (e.g. Computer Incident Response Teams (CIRTs));

5. that countries are encouraged to utilize technical assistance from international organizations with relevant expertise such as UNODC, ITU and Member States as well as other relevant players based on their own assessed needs;

6. that in order to promote consistent approaches against cybercrime, consideration should be given to building consensus on global cybercrime response, legislation and best practices in an appropriate form (e.g. a global agreement, model law or code of conduct);

The participants expressed their heartfelt thanks to the Republic of Korea, specifically the Supreme Prosecutors' Office, Korean Institute of Criminology and Korea Internet and Security Agency for bringing all the participants together and facilitating in achieving a successful outcome of this important Asia Pacific Regional Workshop on Fighting Cybercrime organized by the UNODC and the ITU.