ELEVENTH UN CONGRESS

ON CRIME PREVENTION AND CRIMINAL JUSTICE

Bangkok, Thailand 18-25 April 2005

Committee II
10th Meeting (AM)

BKK/CP/22
23 April 2005

‘AROUND-THE-CLOCK’ CAPABILITY NEEDED TO SUCCESSFULLY FIGHT CYBERCRIME, WORKSHOP TOLD

Speakers Stress Importance of International Cooperation; UNODC Urged to Provide Technical Assistance to Member States

The new trends, threats and challenges faced by the international community in countering cybercrime, bridging the digital divide among nations and harmonizing of laws dealing with cybercrime were among the issues discussed at the concluding session of a workshop on Computer-Related Crime held today at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice in Bangkok. The workshop was organized by the Korean Institute of Criminology.

The “considerable differences between nations, in standards, legal coverage and levels of protection” were an issue of concern, said Ambassador Henning Wegener of the World Federation of Scientists. Ambassador Wegener felt that internationally binding and effective prescriptive instruments were needed to guide and achieve degrees of uniformity in national crime codes and procedures, and effective international cooperation in the application of measures. “We need a universal framework of penal law” he said. That was a view endorsed by Ehab M. Elsonbaty, Judge of South Sinai Court, Egypt, who said “the international nature of cybercrime creates the need for an international solution that should cover substantive, procedures and international cooperation rules”.

The critical need for an “around-the-clock” capability to respond to cybercrime was stressed by Guy De Vel of the Council of Europe. He pointed out that, due to time-zone differences between countries and the fact that terrorist plans and other criminality involving computers could occur at any hour of the day, it was important to be able to move at unprecedented speed to preserve data and detect suspects. He said that countries who became party to the Council of Europe Convention on cybercrime, had to be able to show a 24-hour capability for cases involving electronic evidence, and said that it had been signed by 32 European and non-European States and ratified by 9. The Council of Europe Convention on Cybercrime is, so far, the only internationally binding legal basis for strengthened cooperation worldwide.

The need to bridge the digital divide between developing and developed nations was also stressed upon by the participants in the workshop. The United Nations Office on Drugs and Crime was strongly urged to provide technical assistance to developing nations. On the subject of technical assistance, a web-based 24/7 point-of-contact system to enlist help was proposed by Tae-Eon Koo, Public Prosecutor, Ministry of Justice, Republic of Korea. He felt that international and

(more)

intranational technical assistance was becoming the most important factor in capacity-building efforts.

The lack of training for law enforcement officials was an issue of concern -- Claudio Peguero (Chief, High Tech Crime Investigation Department, National Police), Dominican Republic, pointed out that officers with training were usually detectives or higher-ranking officials -- yet, it was often the patrol officer who was the first responder to a crime scene. “He or she is in a position to recognize and preserve (or inadvertently destroy or allow to be destroyed) valuable digital evidence”, he said. He also said that international law enforcement cooperation should be expedited, as digital evidence is, by its nature, very volatile.

Professor Roderic Broadhurst, Hong Kong University, also stressed the need for more research on the subject of cybercrime, and proposed an interdisciplinary and cross-sector approach, by setting up an international online forum on cybercrime research. That would help generate a critical research mass, and reduce duplication of effort by various nations. He felt such an approach would promote international coordination in the efforts against cybercrime.
Mr. Broadhurst also emphasized the need to learn more about victims and offender behaviour.
Stein Schjolberg, Chief Judge, Moss tingret Court, Norway reviewed the history of efforts in law-making in the cybercrime arena.

On the subject of a public-private strategy in the digital environment, Scott Charney, Vice-President, Trustworthy Computing, Microsoft, pointed to the tension between security and privacy issues. He said that Microsoft was working actively with the public sector by providing training and technical expertise to law enforcement and was conducting a global public campaign around the issue of Internet safety. As an example, he said the company had worked with Canada to set up a child exploitation web-tracking system.

While there was a wide consensus on the need for a combined approach, and better mechanisms of international cooperation, participants felt that a United Nations Convention on Cybercrime would be premature at this stage, and it was more critical to provide technical assistance to Member States, in order to provide a level playing field.

* *** *