UNITED NATIONS INFORMATION SERVICE

**Twelfth United Nations Congress on Crime Prevention and Criminal Justice**

**(Salvador, Brazil, 12-19 April 2010)**

For information only – not an official document

UNIS/CP/605E
13 April 2010

**12th UN Congress on Crime Prevention and Criminal Justice**
**Committee II**
**2nd & 3rd Meetings (AM & PM)**

# Delegates Consider Best Response to Cybercrime as Congress Committee Takes Up Dark Side of Advances in Information Technology

Subsidiary Body Divided over Whether To Expand Existing Convention or Start Negotiations on New Treaty

SALVADOR, 13 April (UN Information Service) – While advances in information technology held many benefits for society, its dark underside -- computer-based fraud and forgery, illegal interception of private communications, interference with data and misuse of electronic devices -- required States to develop an organized, international response, delegates said today at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice.

But in their discussion on the use of science and technology to combat crime, speakers remained undecided about the nature of the required response, with supporters of the Council of Europe's Budapest Convention on Cybercrime suggesting an expansion of the treaty, and others floating the idea of fresh multilateral negotiations.

Leading the discussion, titled "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime", was Matti Joutsen (Finland), Chairman of Committee II of the Congress. He said that initially the subsidiary body had focused largely on laws, policies and national capacity-building exercises aimed at stemming cybercrime, and on the need to boost the ability of less developed countries to fine-tune technology through training and learning from experimental projects.

Some within the Committee had underscored the usefulness of the Budapest Convention as a platform for international cooperation, while others had spoken of a need for a brand new global convention, he said. But, regardless of their stance on a possible new instrument, delegates were largely in agreement on the importance of cross-border cooperation to tackle a crime that knew no boundaries.

Brazil's representative, speaking for the host country, pointed to the hacking of personal information on various sites, saying his Government was working with national banks to maintain the privacy of online users, as well as training law-enforcement, judiciary and other public officials in cybercrime matters to create a safer society. Stronger, broader international cooperation was crucial, he said, calling on Member States to negotiate a new global legal instrument, under United Nations auspices, and to address regional concerns on cybercrime.

The representative of the Republic of Korea noted that social networking sites such as Twitter and Facebook, were increasingly being used not only to commit "traditional" crimes such as sex offences and bullying, but also to spread debilitating computer viruses. "These have become serious threats to the safety of our society," he added, calling on the Congress to take seriously the need for international cooperation. "Criminals can change their location from one country to another within seconds in cyberspace, irrespective of their physical location."

He said the possibility of cyber attacks on his country's key computer networks had prompted the creation of elaborate defensive mechanisms by its National Cyber Security Centre. The Office of the Supreme Prosecutor was the seat of a vanguard Internet crime investigation centre that was establishing an international cooperation system, he added, noting that an online forum had already been formed to provide training in cybercrime investigations, an initiative sponsored by the United Nations Office on Drugs and Crime (UNODC) and used mainly by countries in Asia.

India's representative said the alarming increase in security breaches, web defacements and bot-infected systems in that country had prompted it to update the 2008 Information Technology Act in order better to address everything from data theft, to child pornography, to digital piracy, to the blocking of web content. India had also joined the Cyber Crime Technology Information Network System, an initiative by the Government of Japan.

However, other speakers said that, before the international community could begin to create global guidelines, the capacity of individual States to embrace new technology must be stepped up. Poland's representative pointed out that law enforcement authorities sometimes lacked know-how, and needed a "nudging" from the private sector or research institutes to generate ideas on how best to use modern technology to fight crime -- with full respect for civil liberties. Poland's national homeland security initiative, for example, used technology to record proceedings against organized criminal groups at all stages of the legal process, from court appearances to execution of penalties, he said, adding that a portion of that information was classified.

South Africa's representative agreed with that assessment, and supported the plea by the representatives of Botswana and Angola for aid to help developing countries build capacity. For its own part, South Africa had recently published a draft cybersecurity policy that would set a framework for the creation of relevant structures, boost international cooperation, build national capacity and promote compliance with appropriate cybercrime standards. Over the last five years, South Africa had focused on modernizing and expanding information technology equipment, applications, and centralized hosting capabilities and network infrastructure, as part of its strategy to fully modernize and integrate the national criminal justice system to the maximum benefit of society and at minimum cost to crime prevention agencies.

Spain's representative, speaking on behalf of the European Union, suggested that the time was not yet ripe to formulate a new convention, and that a more logical step would be to build on current achievements while using existing agreements, such as the Budapest Convention, as a legal reference point.

Argentina's representative said he had submitted a formal request to join the Convention in March because it was consistent with his country's constitutional safeguards. The Budapest Convention was not incompatible with any new accord that might arise, he added.

Similarly, Colombia's representative emphasized that the Convention was the best launching pad, and expressed support for the call by the Council of Europe for a clear definition of its objective and scope, as well as the sharing of best practices and experiences to determine a suitable Government response to effectively stamp out cybercrime. The Convention formed the basis of a Colombian law adopted in 2009 which set new standards of conduct, in addition to punitive measures, judicial guidelines on information protection, and equipment to enforce them. Colombian officials had also formed bilateral cooperation mechanisms on cybersecurity with Chile, Mexico and other countries.

But Oman's representative said the best way forward was to revert to the June 2008 proposal set forth in Qatar on developing an international convention on cybercrime as the foundation for international cooperation. Most regional preparatory meetings, had endorsed that proposal, he stressed.

To address the concerns of those nations, the International Association of Prosecutors had set up the Global Prosecutors E-crime Network in 2008, that body's representative said. The web-based tool, guided by the Budapest Convention, aimed to strengthen the capacity of prosecutors to address cybercrime through training packages, a library and a database of cybercrime experts in the jurisdictions of network members.

The Chair, summarizing the day's meeting, noted the broad agreement among participants on the many benefits that technological development brought to individuals and society, though it was also used for criminal purposes, which must be tackled as a matter of priority. The advent of cyberspace had created a new and rapidly changing environment that was difficult even for youth to understand, while allowing the commission of many "old" crimes in new ways, he said, adding that Governments were having a tough time keeping pace, and their responses were sadly lacking. Cybercrime damaged economies and State credibility, impeding national development, he said, emphasizing that cooperation in stamping it out was vital at all levels of law enforcement, the judiciary and the private sector.

Turning to organizational matters, he said negotiations were continuing in two regional groups concerning the appointment of the Committee's Vice-Chair and Rapporteur.

Also speaking today were the representatives of Azerbaijan, Mexico, Indonesia, Angola, Argentina, Peru and Zimbabwe.

* *** *

For further information:

To download the press kit and other information (also in Portuguese), visit:
www.unis.unvienna.org/unis/en/events/2010/12th-crime-congress.html
www.un.org/en/conf/crimecongress2010/

**For live webcast: www.un.org/webcast/crime2010**