United Nations A/CONF.213/L.4/Add.1

# Twelfth United Nations Congress on Crime Prevention and Criminal Justice

Salvador, Brazil, 12-19 April 2010

Distr.: Limited
14 April 2010

Original: English

## Report of Committee II on agenda item 8 and Workshop 2

**Addendum**

### Agenda item 8. Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime

1. At its 1st to 3rd meetings, on 12 and 13 April 2010, Committee II held a general discussion on agenda item 8, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime". For its consideration of that item, the Committee had before it the following documents:

(a) Working paper prepared by the Secretariat on recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime (A/CONF.213/9);

(b) Discussion guide (A/CONF.213/PM.1);

(c) Reports of the regional preparatory meetings for the Twelfth Congress (A/CONF.213/RPM.1/1, A/CONF.213/RPM.2/1, A/CONF.213/RPM.3/1 and A/CONF.213/RPM.4/1).

2. At the 1st meeting, on 12 April, the Chair of Committee II made an introductory statement. A representative of the Secretariat introduced the item. Statements were made by the representatives of China, Algeria, Canada, Argentina, the United States of America, Saudi Arabia, the Russian Federation, Germany, Botswana, Cuba and Chile. Statements were also made by the observers for the Ibero-american Legal Assistance Network (IberRed), the Council of Europe and the World Society of Victimology. A statement was also made by an individual expert from Norway.

3. At the 2nd meeting, on 13 April, statements were made by the representatives of Spain (on behalf of the European Union), Poland, the Republic of Korea, Azerbaijan, Mexico, Indonesia, Angola and Argentina.

V.10-52733 (E)

4. At the 3rd meeting, on 13 April, statements were made by the representatives of Colombia, South Africa, India, Peru, Zimbabwe, Oman and Brazil. A statement was also made by an observer for the International Association of Prosecutors.

**General discussion**

5. In opening the discussion, the Chair highlighted the challenges arising from cybercrime and the capacity of organized criminal groups to misuse the opportunities presented by the rapidly evolving technology. He noted the cross-border nature of cybercrime, the lack of knowledge of the extent of the problem and the differences in national systems.

6. In her introductory statement, the representative of the Secretariat referred to cybercrime as one of the greatest challenges for law enforcement and mentioned that Member States, members of academia and others had called for the development of a relevant international convention. States needed to develop capacities; and UNODC could assist in that effort by providing technical expertise and operational support. A global capacity-building action plan, involving key institutions and partners, might prove an effective means for States to build all-round and sustainable capacities with a view to stemming cybercrime.

7. In the discussion, the many undeniable benefits of rapid technological development were recognized. At the same time, however, those developments made it possible to commit traditional forms of crime in new ways, including fraud and the dissemination of child pornography, and also to commit new forms of crime, such as hacking, spamming, "phishing" (using counterfeit websites (or messages directing users to them) for fraudulent purposes), digital piracy, the malicious spreading of viruses and other attacks on critical information infrastructure. It was noted that terrorist organizations and organized criminal groups used rapidly evolving technologies to facilitate their criminal activities. There was agreement that cybercrime threatened economies, critical infrastructure, the credibility of institutions and social and cultural well-being.

8. Speakers underlined the challenges faced in combating cybercrime. New technologies evolved and became widely available so rapidly that policies and laws could not keep pace. Differences in legal systems and insufficient international cooperation hampered the investigation and prosecution of cybercrime. Complex technology had become a mass phenomenon, and cybercrime mirrored its legitimate use. One speaker stated that cybercrime was often not reported because of limited trust in the investigation process and, in the case of corporate victims, the fear of reputational risk.

9. Various speakers reported on measures taken by their Governments to combat cybercrime, including criminal and money-laundering legislation, regulations on Internet cafes, capacity-building, awareness-raising, strengthening of reporting mechanisms and the protection of vulnerable groups. Speakers mentioned the creation of emergency response teams, specialized units and inter-institutional platforms for law enforcement, the military, academia and the private sector. Speakers also referred to the opportunities offered by information technology for law enforcement, such as electronic surveillance and monitoring systems, artificial intelligence and electronic tools to detect suspicious financial transactions and track Internet protocol addresses. However, investigating and prosecuting cybercrime

required new skills and procedural tools, such as the capacity to collect and analyse digital evidence and to use that evidence in criminal proceedings. Speakers underlined the importance of protecting privacy and human rights while combating cybercrime.

10. Many speakers stressed that cybercrime could be combated successfully only through international cooperation. A number of speakers called on States to make mutual legal assistance and law enforcement cooperation more efficient. Many speakers referred to the Council of Europe Convention on Cybercrime (the Budapest Convention) as the most far-reaching international legal framework for international cooperation against cybercrime. Reference was also made to the Global Cybersecurity Agenda launched by the International Telecommunication Union in 2007 and to initiatives of the Organization of American States, the Group of Eight, INTERPOL and the Commonwealth Secretariat. It was noted that networks of practitioners were useful for exchanging operational information, experience and lessons learned. Existing regional networks should be strengthened and more closely interconnected.

11. It was recognized that developing countries were the ones most vulnerable to cybercrime. Developed countries should urgently step up capacity-building assistance, especially for law enforcement personnel, prosecutors and judges. The private sector, in particular service providers, should assume its responsibility. Reference was made to a number of available tools, including a virtual forum for Asian countries, established with the assistance of UNODC, a Web-based training package of the International Association of Prosecutors and a toolkit on cybercrime legislation provided by the International Telecommunication Union. Speakers referred to the work of UNODC in the area of identity-related crime and the recommendations of a core group of experts on that issue. A number of speakers called for the development of an action plan for capacity-building at the international level, with participation by all international stakeholders.

12. There was discussion on the recommendation made at the regional preparatory meetings for the Congress that the development of a global convention against cybercrime be given careful and favourable consideration. Some speakers strongly supported the initiation of negotiations for a new international instrument to harmonize national legal approaches and foster international cooperation. It was argued that the existing initiatives had only limited bilateral or regional reach. An international instrument, which could be an additional protocol to the United Nations Convention against Transnational Organized Crime or a separate convention, would build on and enrich existing bilateral and regional treaties or agreements on cybercrime, including the Budapest Convention. One speaker proposed that a new instrument could be negotiated in the framework of the International Law Commission, of which UNODC would be a member.

13. Other speakers were opposed to the initiation of negotiations on such an instrument. They considered the Budapest Convention an adequate framework, which was used, including by States not parties, as a model for legislation that had enabled States to conduct successful investigations. Concern was expressed that a global instrument might not set equally high standards and ongoing modernization efforts might stagnate during the negotiation of a new instrument. Problems encountered in combating cybercrime were considered mostly operational, calling for improved information exchange and capacity-building. It was noted that the

limited expertise available in many countries to respond to cybercrime should focus on such operational matters, and not on the negotiation of a new convention.

14. A number of speakers expressed the view that it was too early to commit to the idea of a new convention, as several fundamental issues needed to be considered first. Several speakers called for a clarification on the focus and scope of such a new instrument, and one speaker recommended a pilot analysis of existing standards. The challenges to be faced in the negotiation of a new convention included issues of extraterritorial jurisdiction and the national sovereignty issues resulting from it; issues pertaining to human rights, privacy and national security; and the necessary involvement of the private sector in an intergovernmental negotiation process.

**Conclusions and recommendations**

15. During the discussion on cybercrime, there was agreement on a number of conclusions and recommendations and on the need for States and international organizations to follow up on those recommendations with swift and concrete action.

16. There was agreement that the development of technology brought both benefits and threats to society and that countering cybercrime required urgent attention. The contributing factors and links between technology and crime should be carefully analysed in order to develop efficient strategies.

17. States should develop and strengthen long-term and sustainable capacities. Technical assistance, in particular for capacity-building and legislative drafting, as well as material resources and trained experts, were urgently needed in developing countries. UNODC should continue to cooperate with key partners to provide technical assistance in that regard, including with the Council of Europe as custodian of the Budapest Convention. The development of an action plan for capacity-building at the international level should be given careful consideration.

18. States should make every effort to enhance cooperation between national institutions, between States and with the private sector. This required the full political commitment of Governments. Exchange of information and best practices between States needed to be enhanced by, inter alia, the strengthening of relevant networks.