United Nations A/CONF.203/L.4/Add.4

Eleventh United Nations Congress on Crime Prevention and Criminal Justice

Bangkok, 18-25 April 2005

Distr.: Limited
23 April 2005

Original: English

Report of Committee II: agenda item 5 and Workshops 4, 5 and 6

Addendum

Workshop 6. Measures to Combat Computer-related Crime

Proceedings

1. At its 9th and 10th meetings, on 22 and 23 April 2005, Committee II held Workshop 6: Measures to Combat Computer-related Crime. The workshop was organized in cooperation with the Korean Institute of Criminology. The Committee had before it the following documents:

(a) Background paper on Workshop 6: Measures to Combat Computer-related Crime (A/CONF.203/14);

(b) Discussion guide (A/CONF.203/PM.1 and Corr.1);

(c) Reports of the regional preparatory meetings for the Eleventh Congress (A/CONF.203/RPM.1/1, A/CONF.203/RPM.2/1, A/CONF.203/RPM.3/1 and Corr.1 and A/CONF.203/RPM.4/1).

2. At the first meeting, on 22 April, an introductory statement was made by a representative of the Secretariat, followed by a statement by the observer for the Korean Institute of Criminology. The keynote address for the workshop was delivered by the Permanent Secretary of the Ministry of Information and Communication Technology of Thailand. Presentations were made on the topic "Cybercrime: theory and practice". During the discussion, statements were made by the representatives of Canada, Ukraine, Austria, the Libyan Arab Jamahiriya, France, Spain, the United Kingdom, Argentina, Morocco and Chile. Statements were also made by three individual experts.

3. At the second meeting, on 23 April, presentations were made on the topic "Resources and international cooperation for combating cybercrime". During the discussion, statements were made by the representatives of Italy, Egypt, Canada, the Libyan Arab Jamahiriya, Algeria, the United States of America, the United Kingdom

V.05-83704 (E)

and Argentina. A statement was also made by the observer for End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes.

General discussion

4. In his introductory statement, the representative of the Secretariat outlined both the background to the workshop and United Nations activities in the more general area of prevention of computer-related crime and its links to the information society, including that input in the second phase of the World Summit on the Information Society, to be held in Tunis from 16 to 18 November 2005. The observer for the Korean Institute of Criminology stressed that the workshop would be a valuable forum to promote international cooperation.

5. During the workshop, speakers acknowledged the critical importance of responding effectively to the challenge of computer-related crime, noting in particular its rapid evolution and the diversity of offences encompassed by it. It was noted that the growth in electronic commerce (e-commerce) was dramatically increasing the possibilities for criminal exploitation. Two panellists outlined new trends and threats in the field of computer-related crime. The increasing sophistication of computer-related crime was illustrated by a number of new developments, including: the speed with which new computer viruses and worms could travel, infecting millions of computers worldwide in a short period; the development of new hacking tools that were more powerful and easier to use; the rise of "phishing" (using counterfeit websites (or messages directing users to them) for fraudulent purposes); the spread of false information; and the electronic theft of credit card data and other identity information. It was pointed out that new forms of technology were giving rise to new opportunities for criminal activity, including the exploitation of wireless networks. Advances in cryptography and steganography also enabled individuals to conceal their identities online or to impersonate other users. It was reported that another trend in computer-related crime was the combination of different criminal acts in furtherance of the same criminal enterprise (for example, the combination of "phishing", the use of false identities and extortion).

6. Several aspects related to the so-called digital divide were discussed by participants. At the outset, it was recognized that that concept was more complex than a simple divide between developed and developing countries. Research presented at the workshop indicated a clustering of "info-States" between the two extremes of the digital divide. Apparently, the overall divide was closing because those countries in the middle of the spectrum were making good progress. However, those countries with poorly developed computer and technology infrastructure were falling further behind all of the others. In short, the divide was widening at the bottom end of the spectrum. It was noted that the emerging nature of the digital divide provided new possibilities for computer-related crime. For example, countries at the lower end of the digital divide were used as staging grounds to launch cyber-attacks or as transit countries to mask the cybercrime trail. In addition, as the digital divide in some countries was closing rapidly, consumers were becoming more vulnerable to such crimes as tele-marketing fraud, "phishing" and online auction fraud. It was noted that, in cases where countries invested in technologies to upgrade state and other critical infrastructure, such as mobile telephone networks, new vulnerabilities would emerge. It was also noted that

different sectors of a society—such as an emerging middle class, the high-technology business sector or poor people being integrated into the formal banking system—would be exposed to different kinds of crime in countries where the authorities might have little capacity to respond. For those reasons, the development of appropriate legal frameworks and expertise in the developing world was of great importance.

7. Many participants highlighted the speed at which computer-related crime was evolving and the need for law enforcement and the private sector to be ahead of the perpetrators. Several speakers underlined the importance of the exchange of information on new and emerging trends and the resulting vulnerabilities and threats. Participants described experiences in countries in which trends in computer-related crime were being monitored. One related aspect raised by some speakers was the need to prevent computer-related crime. One critical step in that direction was to raise the awareness of such crime among law enforcement authorities, members of the business community and potential victims. A presentation by the observer for Interpol underscored the importance of data collection, analysis and exchange, with particular reference to the use of the Internet by paedophiles to exchange images. Other proposals were made regarding data collection and monitoring, including the formulation of indicators and criteria to be used to monitor the content of websites. One speaker suggested that an international network of experts for sharing experiences and new knowledge should be established.

8. The workshop considered the impact of computer-related crime on individual victims, in particular the impact of fraud and sexual exploitation. One panellist emphasized that special attention should be paid to the problem of sexual exploitation of children online. It was suggested that the information technology industry should seek to counter such crime by raising public awareness and setting new protection standards. It was argued that more attention should be given to finding out how victims could be protected and assisted, including in the course of the investigation, particularly in cases involving sexual exploitation and the circulation of pornographic material on the Internet. It became clear from the discussion that several critical grey areas remained, including the issue of how to respond to cases where pornographic images were digitally created, as well as the difficulties of determining the age of victims in cases involving child pornography. In addition, some questions were raised concerning what specific activities should be criminalized; for example, in the case of pornography, the question was whether the criminalized activity should be the viewing of the image or its electronic storage.

9. It was pointed out that the impact of computer-related crime went far beyond individual victims to include companies, organizations, governments and society in general. Computer-related crime often posed a threat to critical infrastructure, which in many countries was not controlled by the public sector, and such crime could have destabilizing effects on all segments of society. In that way, digital technology could also be misused for terrorist purposes.

10. One participant suggested that an inventory be conducted of the technological level and capacities of countries to respond to cases involving cybercrime. It was also suggested that a virtual forum of experts be created under the auspices of UNODC to facilitate the exchange of information on new trends and approaches in the area of computer-related crime. With regard to researching computer-related crime, it was suggested that many questions, including the extent of the involvement

of organized criminal groups in such crime, remained unanswered. More research was needed into those and other related policy areas so that future opportunities for criminal activity could be identified. It was stated that, even in developed countries, there was only a relatively small number of experts working in those areas and that initiatives such as an online research network, supported by international agencies and the private sector, would provide opportunities for more information exchange, comparative analysis and transfer of knowledge.

11. It was noted that, within national jurisdictions, four key requirements should be in place to effectively respond to cases involving computer-related crime: experts dedicated to cybercrime; experts available on a 24-hour basis; continuous training, including training of specialists from other countries; and up-to-date equipment. The fulfilment of those requirements would also improve the quality of inter-State cooperation.

12. There was general agreement that the provision of technical assistance to developing countries must be given priority. Such assistance could take on a variety of forms, including: the provision of experienced personnel and advice from Member States and the private sector; the development of training courses and material; and measures to ensure that law enforcement officials were well informed about developments in technology. The United Nations Manual on the Prevention and Control of Computer-Related Crime,[1] published in 1994, was praised as a useful tool; however, it was emphasized that there was currently an urgent need for new and updated material. Several speakers pointed to bilateral assistance activities and training that were currently being undertaken. One key issue highlighted by many speakers was the need to develop expertise in gathering and using evidence of computer-related crime. In a discussion on the development of training material, it was stated that training for criminal justice practitioners should be tailored and delivered in a format that was easily accessible. While the training of specialized police officers and prosecutors was a requirement, it was increasingly the case that all investigators and law enforcement officials should have more advanced knowledge of aspects of computer-related crime, particularly in regard to the preservation of evidence. It was also submitted that training should also be extended, particularly in developing countries, to include also legislators and policymakers.

13. Speakers underlined the importance of a partnership with the private sector to formulate and implement effective measures to counter computer-related crime. As suggested by several practitioners, relationships between commercial entities and law enforcement agencies needed to be developed further, not only to reduce the level of computer-related crime, but also to speed up the response once it occurred. It was pointed out that the role of the public and private sectors, including Internet service providers, in efforts to combat computer-related crime was constantly evolving. One possible partnership strategy could include assistance from business in identifying areas where existing law was inadequate; building capacity, for example, by providing training for law enforcement authorities and by raising awareness of new trends and technologies; working with law enforcement authorities in investigations and sharing general information; educating consumers about issues of online safety; preventive elements such as building effective security mechanisms into products; and providing incentives to the public to obtain information on the activities of perpetrators of computer-related crime.

14. Many speakers underscored the importance of effective international law enforcement cooperation. The global reach of the Internet and the spread of e-commerce had resulted in national borders being of little relevance in cases involving computer-related crime. For that reason, speed was essential to the success of investigations. That required building close relationships with key partners in other countries, the private sector and civil society. Participants described current international cooperative initiatives, such as the contact network originally established by the Group of Eight and consisting of computer crime units available to law enforcement agencies 24 hours a day, seven days a week (on a "24/7" basis). The contact network, currently operating in about 40 countries, had proved to be effective in cases involving computer-related crime. One speaker, however, indicated that the contact network was available only in countries that had the capacity to deal with computer-related crime and that there was a need to bolster the skills required to counter such crime in developing countries.

15. Several speakers indicated that the development and harmonization of national legislation was a prerequisite for effectively dealing with cases involving computer-related crime. That applied in particular to the procedural laws and rules on the gathering and admissibility of evidence. It was suggested that, for that reason, training programmes should also be made available for prosecutors and judges. It was noted that international cooperation in efforts to combat computer-related crime were complicated by the fact that many countries did not have any legislative provisions covering such crime. It was suggested that model laws on the subject should be developed, taking into account different legal systems.

16. Several panellists raised the issue of whether it was necessary to develop a new international instrument against computer-related crime. One panellist supported the idea of developing such an instrument, citing the importance of having a global legal framework and providing unified global standards in relation to computer-related crime. It was suggested that developing such an instrument might take a considerable amount of time and that it was preferable to begin the process earlier rather than later. Most speakers, however, argued that it might be premature to begin negotiations on such a convention. Numerous reasons were given for that, including the following: the Council of Europe Convention on Cybercrime had only recently entered into force and time was needed to evaluate its benefits; the Convention on Cybercrime was open for signature to all States, not only those in Europe; and that practical measures to enhance international cooperation should, for the time being, have the highest priority. One speaker noted that, while technical assistance constituted a significant element of the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption, the subject of computer-related crime was such that technical assistance would need to be provided and capacity-building would need to take place before negotiations on an international convention against computer-related crime could begin, in order to ensure the full participation of all States in the negotiation process. One speaker expressed the view that, while it was premature to speak of a negotiation process, if negotiations ultimately did take place, the process should generally follow the precedent established by the negotiation of the Organized Crime Convention and the Convention against Corruption. Several speakers underscored the importance of States ratifying the Convention on Cybercrime.

17. Several speakers pointed to the recommendations provided in the background paper on Workshop 6 (A/CONF.203/14), suggesting that they provided a useful basis for discussion. No objections were raised about any of the recommendations contained in the document and many participants indicated that they supported them in principle.

Conclusions and recommendations

18. The workshop made the following conclusions and recommendations:

(a) Technical assistance and training should be provided by UNODC to States in order to address the lack of capacity and expertise to deal with the problems of computer-related crime. Consideration should be given to updating the United Nations Manual on the Prevention and Control of Computer-Related Crime and the development of related training tools. Such tools should be made available internationally in order to share knowledge and information concerning ways and means of recognizing, protecting, preventing and handling new types of cybercrime;

(b) International cooperation should be developed in the areas of information exchange, research and analysis concerning computer-related crime. The United Nations should play a leading role in ensuring a global approach to combating computer-related crime to safeguard the functioning of cyberspace, so that it is not abused or exploited by criminals or terrorists. In this regard, consideration should be given to the establishment of a virtual forum or online research network to encourage communication among experts across the globe on the issue of computer-related crime;

(c) International law enforcement cooperation should be further enhanced, including by upgrading the capacity and skills of countries not currently linked to existing law enforcement networks that focus on cybercrime;

(d) States that have not done so should be encouraged to update and harmonize their criminal laws in order to counter computer-related crime more effectively, giving due attention to aspects related to the defining of offences, investigative powers and the collection of evidence. The sharing of experience among countries is critical to this endeavour. States should take into consideration the provisions of the Council of Europe Convention on Cybercrime;

(e) Governments, the private sector and non-governmental organizations should work together to counter computer-related crime, including by raising public awareness, engaging in preventive activities and enhancing the capacity and skills of criminal justice professionals and policymakers. Such cooperative efforts should include a strong focus on preventive aspects;

(f) The results of the workshop should be made available to the second phase of the World Summit on the Information Society, to be held in Tunis from 16 to 18 November 2005.

Notes

[1] *International Review of Criminal Policy*, Nos. 43 and 44 (United Nations publication, Sales No. E.94.IV.5).