



**Tenth
United Nations Congress
on the Prevention of Crime
and the Treatment of Offenders
Vienna, 10-17 April 2000**

Distr.: Limited
16 April 2000

Original: English

Agenda item 5

Effective crime prevention: keeping pace with new developments

Report of Committee II

Workshop on crimes related to the computer network

Introduction

1. The workshop on crimes related to computer networks, organized by the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders, was held on 15 April 2000. The workshop had before it a background paper on the subject (A/CONF.187/10).
2. An introductory statement was made by the Director of the Institute, Mr. Mikinao Kitada.
3. In a keynote address, The Honourable Ms. Anne McLellan, Minister of Justice and Attorney-General of Canada, noted the growing seriousness of domestic and transnational computer crime and the importance of developing effective laws and procedures for controlling it without unduly interfering in the legitimate and beneficial effects of the new technologies.
4. The workshop held a series of panel discussions. The first panel reviewed the criminology of computer crime. The second panel discussion comprised a case-study scenario of the technical and legal issues that arise from a legal search for and seizure of data from computer networks. The third panel discussion consisted of a case-study scenario of the tracing of computer communications in multinational networks. The fourth and final panel discussion dealt with the relationship between law enforcement and computer and Internet industries. During the discussions, statements were made by the representatives of 9 Governments and by 17 experts.*

General discussion

5. It was pointed out that the development of new technologies had created new opportunities for criminal offenders. The term "computer-related crime" has been

* The list of experts is contained in the annex to the present report.

developed to encompass both the entirely new forms of crime that were directed at computers, networks and their users, and the more traditional forms of crime that were now being committed with the use or assistance of computer equipment. A review was undertaken of the legal response to the new crimes. In that regard, it was stressed that, given the ease with which these crimes could be committed across national borders, it was important to develop adequate criminal laws in every country.

6. It was noted that the new environment created by computer networks challenged many of the conventional assumptions of legal systems. The need to modernize laws in order to keep pace with technology was discussed. It was pointed out that legal concepts, such as property, theft and possession, were all commonly applied in the criminal laws of countries but did not necessarily apply to computer data which were by nature intangible. The ease with which data could be modified had also created new legal problems associated with their collection, preservation and use as evidence in legal proceedings.

7. It was noted that the powers and techniques needed for effective investigations of computer networks also raised significant concerns of human rights and privacy, both because of their intrusive nature and the vast amounts of personal and other information stored and transmitted on such networks. It was agreed that one of the fundamental issues confronting Governments at present and in the future was the need to find the proper balance between the individual citizen's right to privacy and the interests of law enforcement. It was noted that privacy issues might arise in a number of situations. It was also noted that the laws of some countries made a distinction between searching for and intercepting data in transmission and searching for stored data, while in other jurisdictions, that distinction might be unclear. It was pointed out that, where data were considered to be communications in transmission and therefore subject to interception rather than seizure, there might be a need for more stringent requirements for obtaining the necessary authorizations and for safeguards governing the conduct of the search. In that regard, it was considered that evidence sought by law enforcement agencies might be commingled with other materials, such as the business or medical records of the subject, or those of a third party.

8. It was noted that many issues arose when law enforcement authorities sought to gain information from Internet service providers. These included the practical question of finding a person at such a provider who could be contacted when required, and the legal question of whether a provider might disclose information voluntarily or not. It was pointed out that the privacy or data protection laws of some countries prohibited providers from disclosing some or all information concerning the communications of their customers without a court order, and that laws might also be unclear as to whether a provider should retain content or transaction records so that they could be recovered if subsequently needed for an investigation.

9. A number of participants observed that, when evidence sought by law enforcement was in the computer systems of a legitimate business, the search might cause harm to the business if it interfered with computer operations. It was agreed that, in such cases, the challenge was to execute the search effectively but without disrupting normal business operations.

10. It was considered that the transnational dimension of much computer crime might give rise to even greater complications, not the least of which involved jurisdiction. The questions of which country's laws applied, the investigative power to obtain evidence and trace or identify offenders, the power to extradite offenders and subsequently try them before a court all depended to some degree on where the offence had been committed; the

determination of place would be unclear if the crime were committed in more than one location by the use of computer network technologies. An example was cited of a Web site in one country which contained fraudulent speculation about a company whose shares were traded on the stock exchange of another country. The offence might therefore have occurred in one country, the other country, both countries or neither of them, depending upon the laws of the countries concerned.

11. It was observed that search and seizure measures also became complicated when the searchers were located in one jurisdiction and the evidence was found in another. A network search, for example, could lead to evidence that was stored in a different country, which raised the questions of whether the permission of authorities in the second country was needed to obtain the evidence, or whether the authorities in the second country should be notified that such a search was in progress. It was noted that, where it was necessary to request assistance through formal mutual legal channels, the time needed to obtain such assistance could be substantial. The question of how that process could be expedited might be crucial in dealing with cases in which a computer-related offence was in progress, or where evidence could be destroyed during the time needed to obtain legal assistance through existing channels.

12. It was noted that another issue posed by the transnational nature of computer-related crime and the ease with which electronic evidence could be altered was the problem of determining the authenticity of evidence obtained in a cross-border search. That determination might require the establishment of procedures or protocols for use in computer searches in order to ensure the authenticity of data retrieved, as well as transparent and secure procedures that would make it possible to establish authenticity. It was observed that, in some countries, there might be formal requirements that impeded the use of electronic data as evidence.

13. There was general agreement that States should seek harmonization, where appropriate, of the relevant provisions on criminalization, evidence and procedure.

Conclusion

14. The workshop reached the following conclusions.

- (a) Computer-related crime should be criminalized;
- (b) Adequate procedural laws were needed for the investigation and prosecution of cyber-criminals;
- (c) Government and industry should work together towards the common goal of preventing and combating computer crime so as to make the Internet a secure place;
- (d) Improved international cooperation is needed in order to trace criminals on the Internet;
- (e) The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks.

Annex I

Experts participating in the panel discussions

Mr. Shri L. C. Amarnathan, Sikkim Police Headquarters, India

Mr. Cormac Callanan, European Internet Service Provider Association, Ireland

Mr. Peter N. Grabosky, Institute of Criminology, Australia

Mr. Masahito Inoue, University of Tokyo, Japan

Mr. Nigel Jones, Association of Chief Police Officers, United Kingdom of Great Britain and Northern Ireland

Mr. Ekkehart Kappler, Federal Crime Office, Germany

Mr. Henrik W. K. Kaspersen, Professor, Vrije Universiteit Amsterdam, Netherlands

Ms. Margo L. Langford, Barrister and Solicitor, Canada

Mr. Victor Lo, Hong Kong Police Force, China

Mr. Keith Mitchell, London Internet Exchange, United Kingdom of Great Britain and Northern Ireland

Mr. Hans G. Nilsson, Council of the European Union

Mr. Donald K. Piragoff, Department of Justice, Canada

Ms. Mary Riley, United States Secret Service, United States of America

Mr. Gregory P. Schaffer, Computer Security Consultant, United States of America

Mr. Ulrich Sieber, University of Munich, Germany

Mr. Vittorio Stanca, National Computer Crime Unit, Italy

Mr. Michael Sussmann, Department of Justice, United States of America