MEETING OF MINISTERS OF JUSTICE OR
OF MINISTERS OR ATTORNEYS GENERAL
OF THE AMERICAS

OEA/Ser.K/XXXIV
CIBER-III/doc.4/03
24 June 2003
Original: Spanish

III Meeting of the Group of Governmental Experts on Cyber-Crime
June 23-24, 2003
Washington, D.C.

RECOMMENDATIONS

RECOMMENDATIONS
OF THE THIRD MEETING OF GROUP OF GOVERNMENTAL EXPERTS ON CYBER-CRIME[1/]

Governmental experts on Cyber-Crime of the OAS Member States met in Washington D.C, during the days of June 23 and 24, 2003, in accordance with the recommendations adopted at the Fourth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA-IV) and with OAS General Assembly resolution AG/RES. 1849 (XXXII-O/02).

Taking into account the mandate that was assigned to this Group by REMJA-IV, in concluding its deliberations within the framework of this initial meeting, the Group of Governmental Experts agreed to the following recommendations in relation to the areas in which major developments are required in order to strengthen and consolidate hemispheric cooperation in the fight against cyber-crime:

1. That, in accordance with the recommendation prepared by this Group and adopted by REMJA-III, States that have yet not done so, as soon as possible, identify or, when necessary create or establish, the specific units or bodies charged with the direction and development of the investigation and prosecution of the different modalities of cyber-crimes and that they be assigned the necessary human, financial and technical resources in order to comply with their responsibilities in an efficient, effective and expeditious manner.

2. That States that have yet not done so, as soon as possible, examine their legal systems to determine whether it adequately applies to combat cyber-crime and collect and keep in safe custody electronic indicia and/or evidence.

3. That the States that have yet not done so adopt legislation that is specifically required for criminalizing the different modalities of cyber-crimes and to set the procedural measures which ensure the collection and preservation in safe custody of electronic indicia and/or evidence, as well as the efficient, effective and expeditious investigation and prosecution of cyber-crimes.

4. That, in order to assist the States in the preparation or improvement and adoption of legislation on cyber-crime, technical meetings be held, within the OAS framework, on legislative drafting in this field, in which specific actions that must be undertaken be considered, among others, in substantive, procedural and mutual legal assistance areas to write or improve national legislation and provide a legal framework that allows and ensures efficient, effective and expeditious hemispheric cooperation in the handling of electronic evidence and of the fight against the different modalities of cyber-crimes.
5. That, based on the information provided by the States, the OAS General Secretariat prepare and maintain an updated directory of points of contact for each one of the countries that make up

---

1. This document was approved during the plenary session held on June 24, 2003, within the framework of the Third Meeting of Group of Governmental Experts on Cyber-Crime, held through June 23 and 24, 2003, at the OAS Headquarters in Washington, DC. USA. **NOTE**: The report of the present meeting along with its annexes are published in the following Internet address: www.oas.org/juridico/english/cybGE_IIIrep.pdf

the Governmental Group of Experts on Cyber-crime, as well as a directory of authorities responsible for the investigation and prosecution of cyber-crimes.

6. That the States that have yet not done so, adopt the necessary decisions for membership, as soon as possible, to the "24 hours/7 days Emergency Network," having first taken the steps in item 1, if necessary.

7. That taking into account progress made through the OAS website, information regarding developments in the fight against cyber-crime be consolidated into a comprehensive information system that provides both public access to information and restricted access to sensitive information for government officials with responsibilities in this field. Likewise that, based on the information provided by the States, the General Secretariat compile and post on the OAS website the applicable national laws and identify the common thematic areas.

8. That the States incorporate specific materials on cyber-crime and the handling of electronic evidence in general into their training programs, directed to judges, prosecutors and law enforcement officials and that the Member States of the OAS and Permanent Observers to this Organization provide the broadest mutual technical assistance and cooperation among themselves.

9. That information exchange and cooperation continue to be strengthened with other international organizations and agencies on cyber-crime like the United Nations, the Council of Europe, the European Union, Asian Pacific Economic Cooperation forum, the OECD, the G-8 and the Commonwealth, giving the OAS Member States the opportunity to know and use the developments in said organizations and agencies.

10. That the Group of Governmental Experts on Cyber-Crime meet at least once a year, within the OAS framework, and that in its following meetings:

    a) Examine the results of the technical meetings mentioned in paragraph 4 and that, taking into account their results, consider what adjustments, if any, should be adopted for future meetings of this nature, and further actions that should be taken to facilitate the adoption and application of legislation described above.

    b) Prepare recommendations to identify and describe the various types of cyber-crimes.

    c) Prepare recommendations to identify and describe the legal investigative powers that States shall possess to investigate cyber-crimes. These legal investigative powers shall:

        i) Apply not only to investigation of cyber-crimes, but also to the collection and safe custody of indicia and/or evidence in electronic form of any other criminal offense.

        ii) Ensure an adequately balance between the funded and motivated exercise of these powers and the need to guarantee the rules of due process, in the framework of the respect of fundamental human rights and freedoms.

iii) Apply, as permitted by national law, to respond to requests for international cooperation and domestic investigations.

iv) Be able to trace the communications of criminals suspects, through computer networks involving multiple service providers in order to determine the path, origin or destination of the communication.

d) Recommend measures to prevent the creation of cyber-crime heavens in accordance with laws of the States and international treaties.

e) The States report on the measures that they have taken between one meeting and the other.

Washington D.C., United States of America, June 24, 2003.