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

OEA/Ser.K/XXXIV
CIBER-V/doc.3/07 rev. 1
20 November 2007
Original: English

V Meeting of the Group of Governmental Experts on Cyber-Crime
November 19 and 20, 2007
Washington, DC

RECOMMENDATIONS

The Group of Governmental Experts on Cyber-Crime met at the Organization's headquarters in Washington D.C., on November 19 and 20, 2007, in accordance with the agreements reached at the Sixth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA-VI) and with OAS General Assembly Resolution AG/RES. 2266 (XXXVII-O/07).

Based on the mandate that was assigned to this Group by REMJA-VI, the Group of Governmental Experts concluded its deliberations at this meeting with agreement on the following recommendations to strengthen and consolidate hemispheric cooperation in the prevention and fight against cyber-crime:

1. That the states that have not yet done so, as soon as possible, establish specific units or bodies charged with the direction and development of the investigation and prosecution of cyber-crimes, and that they be assigned the necessary human, financial and technical resources in order to carry out their functions in an efficient, effective and expeditious manner.

2. That the states that have not yet done so, as soon as possible, provide the OAS General Secretariat with information identifying the prosecutorial and police authorities that serve as points of contact for international cooperation for cyber-crime and electronic evidence matters. Similarly, that the OAS General Secretariat, based on the information received from the states, continue consolidating the directories of the aforementioned points of contact.

3. That the states that have not yet done so, as soon as possible, examine their legal systems and adopt the specific legislation and procedural measures necessary to criminalize the different modalities of cyber-crimes, ensure the efficient, effective and timely investigation and prosecution of those crimes, and enable states to cooperate with each other in the investigation and prosecution of cyber-crimes.

4. That the states that have not yet done so, as soon as possible, adopt legislation and procedural measures necessary to ensure the collection and safe custody of all forms of electronic evidence, enable states to assist each other in matters involving electronic evidence and their admissibility in criminal proceedings and trials, including the development of provisions for service providers which guarantee the preservation and recovery of information that is stored or in transit.

5. That the states that have not yet done so, as soon as possible, take the measures necessary to join the G-8 "24 hours/7 days Emergency Network of Contacts for High Tech Crime".

6. That the OAS General Secretariat continue to consolidate and update the Inter-American Cooperation Portal on Cyber-Crime via the OAS Internet webpage, and that the states provide the OAS General Secretariat with the information required for this purpose. Similarly, that the use of other technological tools be considered in order to facilitate the exchange of information between the governmental experts on cyber-crime.

7. That, based on the information furnished by the states, the OAS General Secretariat continue to compile in a systematized fashion, the cyber-crime laws of the OAS member states, including their substantive and procedural aspects as well as the area of mutual legal assistance, and make this information available to the OAS member states on the Internet Portal.

8. That, bearing in mind the recommendations adopted by this Group at its Third and Fourth Meetings and by REMJA V and VI, the states consider applying the principles of the Council of Europe's Convention on Cyber-Crime, acceding thereto, and adopting the legal and other measures required for its implementation. Similarly, to this end, that technical cooperation activities continue to be held under the auspices of the OAS General Secretariat and the Council of Europe.

9. That the states, the OAS General Secretariat, and this Group continue to strengthen bilateral and multilateral exchange of information and cooperation with other international organizations and agencies in the area of cyber-crime.

10. That, as part of the efforts designed to facilitate and consolidate cooperation to prevent, investigate and punish cyber-crimes, states further develop the partnership between the officials responsible for investigating and prosecuting such crimes and the private sector, especially with those companies that serve as providers of information and communications technology, particularly Internet service providers.

11. That this Group expresses its satisfaction with the results of the three training workshops held under the leadership of the United States Department of Justice, and with the support of the United States and cooperation of Brazil, Costa Rica, and Barbados, for the purposes, among others, of facilitating the development of the technical and legal capacity for states to join the "24 hour/7 day emergency network" and the management of electronic evidence, which took place in Brasilia, Brazil, San Jose, Costa Rica and Christ Church, Barbados, during 2006 and 2007.

12. That this Group accept the offer of the United States Government to continue to develop, in coordination with the General Secretariat of the OAS, through the Office of Legal Cooperation of the Department of International Legal Affairs, training programs to strengthen the capacity of the OAS Member States with respect to the continued development of legislation and procedural measures related to cyber-crime and electronic evidence, or the investigation and prosecution of cyber-crimes, and request that the next meeting of the Group be informed of the progress made in this respect.

13. That the Group of Governmental Experts on Cyber-Crime continue to meet at least once between one REMJA and the next, within the framework of the OAS, and that at its next meeting, it discuss, among other topics, the progress made in the implementation of these recommendations, as well as the Comprehensive Cybersecurity Strategy.