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

OEA/Ser.K/XXXIV
CIBER-X/doc.3/22 rev.2
29 April 2022
Original: English

Tenth Meeting of the Working Group on Cybercrime
April 28-29, 2022
Washington, D.C.

**RECOMMENDATIONS**

The Working Group on Cybercrime of the REMJA (the Working Group) held its Tenth Meeting online, from April 28-29, 2022, pursuant to the Document of Washington (document REMJA-VII/doc.6/08 rev. 4), the Conclusions and Recommendations of REMJA-XI (document REMJA-XI/DOC.2/21 rev. 1), and resolution AG/RES. 2975 (LI-O/21) of the OAS General Assembly.

Based on the mandate that was assigned to it by REMJA-XI, the Working Group concluded its deliberations at this meeting with agreement on the following recommendations to strengthen and consolidate hemispheric cooperation in the prevention and fight against cybercrime in accordance with principles of state sovereignty and relevant national legislation:

1. That the States that have not yet done so establish, as soon as possible, specific units or bodies charged with managing and conducting the investigation and prosecution of cybercrimes, and that these units or bodies be provided with the necessary human, financial, and technical resources to carry out their functions in an efficient, effective, and expeditious manner.

2. That the REMJA Technical Secretariat (Department of Legal Cooperation of the OAS Secretariat for Legal Affairs) continue consolidating and keeping up to date the directory of authorities designated by States that serve as points of contact for international cooperation in the area of cybercrime and electronic evidence and, to this end, the States that have not yet done so provide the REMJA Technical Secretariat, as soon as possible, with such updated information.

3. That the States that have not yet done so proceed, as soon as possible, to examine their legal systems and adopt or update the legislation and procedural measures that are specifically required to criminalize the different forms of cybercrime and that ensure the efficient, effective, and timely investigation and prosecution of cybercrimes and enable States to cooperate with one another in the framework of these same activities.

4. That the States that have not yet done so attempt to adopt or update, as soon as possible, procedural measures and legislation as may be necessary to ensure the collection and safe custody of all forms of electronic evidence and their admissibility in criminal proceedings and trials. Likewise, as soon as possible, States adopt the corresponding legal measures that enable States to assist one another in matters involving electronic evidence.

5. That the States that have not yet done so, seek to adopt, as soon as possible, legislation that ensures that service providers guarantee the preservation upon request and recovery of all forms of electronic evidence that is stored or in transit.

6. That the States that have not yet done so, develop and implement national strategies that include efforts to deter, investigate, and prosecute cybercrime, as well as capacity building efforts that include key principles for mainstreaming gender and inclusion. The foregoing is carried out as part of a broader and more coordinated effort to protect the information technology systems and networks of citizens, businesses, and governments.

7. To continue promoting the coordination and cooperation relationships among the REMJA Working Group on Cybercrime, the Inter-American Telecommunication Commission (CITEL) and the Inter-American Committee against Terrorism (CICTE), in order to make further progress in implementing the mandates that, within the framework of their respective competences, the Comprehensive Inter-American Strategy adopted by the OAS General Assembly pursuant Resolution AG/RES. 2004 (XXXIV-O/04) assigns to each of these entities.

8. That the States that have not yet done so consider the possibility of joining, as soon as possible, the G-7 "24/7 Network of High-Tech Crime Points of Contact".

9. That the REMJA Technical Secretariat continue to consolidate and update the Inter-American Cooperation Portal on Cybercrime (hereinafter, "the Portal"), and made available in the four official languages of the OAS, within available resources, via the OAS Web page and, to this end:

a. To continue completing and updating the information on the Portal, in coordination with the Working Group.

b. To request the OAS General Secretariat, in line with available resources, to continue advancing on the development of new virtual spaces for the exchange of information, experiences and good practices among the authorities designated by States in the area of international legal cooperation for investigation and prosecution of cybercrime.

c. To ask the States to respond to requests from the REMJA Technical Secretariat to complete or update the information disseminated on the Portal.

d. To give due consideration to the use of other technological tools in order to facilitate the exchange of information between governmental experts on cybercrime and in the area of international cooperation in investigating and prosecuting it. In addition, promote exchanges of information among agencies that conduct investigations and gather evidence about cybercrime, such as universities and research centers that promote the development of new information and communication technologies (ICTs), in such a way they can include in their design a perspective of usefulness and relevance for justice administration systems.

e. To establish reciprocal links between the Portal and the Internet pages that have been established or will be established in the future by the authorities designated by States for international legal cooperation, and that any

manuals or other information that is considered useful for facilitating cooperation in the areas of their responsibility be published thereon.

10. To continue promoting the exchange of information, coordination and cooperation between the REMJA working groups on Cybercrime and Legal Cooperation Criminal Matters (mutual assistance and extradition), as well as between the authorities designated by States with responsibilities in this area, in order to strengthen the cooperation in this field and avoid duplication of efforts.

11. That any unit or body the States have established or will establish to handle and conduct the investigation and prosecution of cybercrimes, set up and maintain Internet pages to provide citizens with information on how to avoid falling prey to cybercrimes and on how to detect and report such crimes to the competent authorities when they do occur. Similarly, that the REMJA Technical Secretariat make the necessary arrangements in order to establish reciprocal Internet links between those pages and the Portal.

12. That the REMJA Technical Secretariat, in line with available resources, continue supporting the legislative developments in the area of cybercrime, among others, through the systematization of the legislation of the OAS Member States in this field and their dissemination via the Portal, as well as proposals for legal cooperation for the drafting and consideration of model legislation in this area.

13. To recommend that the OAS member states that have not yet done so, consider evaluating to accede to the Council of Europe's Convention on Cybercrime, and adopt the legal and other measures required for its implementation, as well as to participate and contribute to the development of international instruments to combat and prevent cybercrime. Similarly, to this end, that technical cooperation activities be continued under the auspices of the REMJA Technical Secretariat and the Council of Europe.

14. That mechanisms for information exchange and cooperation continue to be strengthened between the REMJA and other international organizations and agencies in the area of cybercrime, such as the United Nations, the Council of Europe, the European Union, Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Co-operation and Development (OECD), the G-7, the Commonwealth, and INTERPOL, to enable OAS Member States to benefit from developments in those areas.

15. That, as part of the efforts designed to facilitate and consolidate cooperation to prevent, investigate, and punish cybercrimes, States jointly continue developing partnerships among the officials responsible for preventing, investigating and prosecuting such crimes and the private sector, especially with those companies that provide information and communications technology, in particular Internet service, in order to streamline and improve the obtainment of information in the context of mutual assistance proceedings, as appropriate under domestic laws.

16. That it expresses its satisfaction with the results of the cybercrime training workshops for judges, magistrates, public prosecutors, and investigators, held since the Ninth meeting, in order, Buenos Aires, Argentina; Santiago, Chile; Mexico City, Mexico; Miami, Florida; Asuncion, Paraguay; Santiago, Chile; Guatemala City, Guatemala; Montego Bay, Jamaica; Panama City, Panama; Lima, Peru; San Jose, Costa Rica; Quito, Ecuador; Asuncion, Paraguay; and in virtual form in October and December 2020; April, August and December, 2021; and February 2022, as well as the current meeting

of the group, under the leadership of the United States as Chair of the Working Group and with the financial support of the United States, the support of the states in which they took place, and the cooperation of the REMJA Technical Secretariat.

17. That it expresses its satisfaction with the organization of the virtual forums on Legal Cooperation against Cybercrime, that took place in June 2020; Adaptation of Legislation to International Standards against Cybercrime that took place in August 2020; Cryptocurrencies: Challenges to Cybercrime Investigations and Prosecutions that took place in July 2021; and Ransomware: Challenges and International Cooperation that took place in November 2021, which was part of a series of virtual sessions organized by the Secretariat for Legal Affairs on Inter-American Law in the Times of Pandemic.

18. That the cybercrime training program financed with external contributions, continue to be executed within the framework of the REMJA. As part of this program, accept the offer of the United States Government to continue conducting training workshops in this field, in coordination with the Technical Secretariat of the REMJA, taking into account the use of new information and communication technologies (ICTs) and emerging trends, as well as the suggestions and specific interests expressed by OAS Member States, and encouraging participation by those States in the training program, especially the participation by the authorities designated by those States.

19. To ask the REMJA Technical Secretariat to continue disseminating the progress achieved in the framework of the OAS and by the States in the area of cooperation in the fight against cybercrime through electronic means, such as social media. Similarly, to request States to contribute information on their developments in this field to be disseminated.

20. That those states that have not yet done so take the necessary steps to have statistics organized annually on the investigation, prosecution, and disposition of cybercrime cases, as well as on requests for mutual assistance sent and received and their outcomes. Furthermore, that those states that have not yet done so assign an entity the responsibility for compiling the aforementioned statistics and notify the REMJA Technical Secretariat of the contact details of that entity.

21. That the REMJA Working Group on Cybercrime continue consolidating itself as a hemispheric forum for the exchange of best practices among OAS member states in cybercrime and the handling of digital evidence.

22. To facilitate awareness, within the framework of the MISPA process (Meeting of Ministers Responsible for Public Security in the Americas) of the developments of the Working Group on Legal Cooperation on Cybercrime, in order to strengthen hemispheric cooperation in combating these crimes, so that they can be taken into account and used, as appropriate, by the authorities of the member states that participate in the MISPA.

23. That the Working Group meets prior to REMJA-XIII to consider, among other topics, the progress made in the implementation of these recommendations.