


OAS | REMJA

Funded by the European Union and the Council of Europe

COUNCIL OF EUROPE

Implemented by the Council of Europe

Version 7 December 2017

HEMISPHERIC FORUM ON INTERNATIONAL COOPERATION AGAINST CYBERCRIME

Santo Domingo, Dominican Republic, 5-7 December 2017

organized by the

Government of the Dominican Republic, the Council of Europe through the GLACY+ joint project with the European Union, the Organization of American States through the Department of Legal Cooperation (Technical Secretariat of the REMJA) and the United States Department of Justice with the support of the European Union, INTERPOL, AMERIPOL, the Department of Justice of Canada, CARICOM, and the Global Forum on Cyber Expertise

Forum summary

More than 150 representatives of governments and criminal justice authorities of [34] countries and territories of the Americas, private sector and international organizations participated in the Hemispheric Forum on International Cooperation against Cybercrime in Santo Domingo, Dominican Republic, from the 5th to the 7th of December 2017.

Participating countries and territories included Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bermuda, Bolivia, Brazil, Canada, Cayman Islands, Chile, Colombia, Costa Rica, Curaçao, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Montserrat, Nicaragua, Panama, Paraguay, Peru, Saint Lucia, Saint Martin, Suriname, Uruguay and USA.

International organizations and initiatives included AMERIPOL, CARICOM, CARICOM IMPACS, Council of Europe, European Union, Global Forum on Cyber Expertise, INTERPOL, Regional Security System, and the Organization of American States.

Speakers from the Argentina, Canada, Council of Europe, Dominican Republic, Guatemala, Interpol, the U.S. Department of Justice and Microsoft shared their experience.

The Forum was aimed at permitting participating countries to make better use of capacity building programmes of international organizations, to enhance cooperation and synergies between international organizations and initiatives, and to share experience on the strengthening of capacity building for criminal justice authorities.

Key take-aways include:

- Cybercrime and issues related to electronic evidence undermine the social and economic development opportunities of information technologies as well as human rights, democracy and the rule of law. A more effective criminal justice response and cooperation at all levels are needed.

- This is also true for cooperation between international organizations. Enhanced cooperation among them permits them to deliver the best possible service to States. The Forum was itself an illustration of international organizations joining forces to support countries and territories of the hemisphere in their efforts to meet the challenge of cybercrime.

- Legislation on cybercrime and electronic evidence is the basis for such a response. An increasing number of countries in the Americas have adopted or are in the process of adopting domestic legislation, often using the Budapest Convention on Cybercrime as a guideline. It is noted that the Council of Europe under the GLACY+ project is ready to support countries the region in this process upon request.

- Capacity building is an effective way to permit countries strengthen legislation, institutional capacities and cooperation at all levels. Examples of good practice and offers of further support include:

    - the GLACY+ project of the European Union and the Council of Europe on Global Action on Cybercrime Extended,
    - the Legal Cooperation Program of the Organization of American States within the framework of the mandates of the REMJA (Meetings of Ministers of Justice and Attorney General of the Americas) process.
    - UNODC Global Program on Cybercrime.
    - Cyber Americas Project by INTERPOL funded by the Government of Canada
    - Certification courses such as the ICSE (International Child Sexual Exploitation) database and the ICCACOPS platform by the INTERPOL and the USDOJ. States praised the usefulness of the certification of the police practitioners.

- Cooperation with the private sector

    - It should be recognized that combating cybercrime is not a sole responsibility of the public sector but also of the private sector. It is important to promote a platform for high levels of cooperation between the private and public sectors. Currently, geopolitical changes, the acceleration of technological developments and the evolution of attacks have caused a response gap between policies and real-time effective execution. All parties will need to participate in the creation of a pragmatic legal framework that will permit law enforcement to perform their duties while protecting individual privacy and facilitate cooperation between countries.

    - INTERPOL is focusing resources to expand its information sharing agreements with private sector to produce actionable intelligence for member countries. Participating countries to the Cyber Surge urged INTERPOL to continue producing and disseminating intelligence through its official channels.

- Dark net and bitcoin, criminal money flows.

  - Cybercrime related cases are complicated and require tenacity, resources, intelligence, patience by the investigators, and coordination between the different governmental institutions. This will seek to ensure the success of tracking, investigating, capturing, and processing of criminals.
  - Occasionally, criminals make mistakes. Those mistakes in turn can be used for the investigation and prosecution of said criminals and bring them to justice.
  - International cooperation in cyber related cases is very important for the exchange of experiences and technical assistance. In particular, in cases that have not been encountered before.
  - It is the responsibility of investigators and prosecutors to explain the technical aspects of complex issues in clear and simple terms to judges and juries.

- Access to evidence in the cloud

  - As electronic evidence is increasingly stored on servers in the cloud, specific measures are needed to secure such evidence for criminal justice purposes. The work of the Cybercrime Convention Committee within the framework of the Budapest Convention is noted, including the negotiation of a Protocol on access to evidence in the cloud which started in September 2017. It is also noted that private sector entities are prepared to cooperate with public authorities. Governments may consider following the work of the Cybercrime Convention Committee on a Protocol to the Budapest Convention and accession to this treaty.

- Cooperation between international organizations

  - The developments of an international and national level call of consciousness are the grounds for effective actions. There is a need to reassess and renew the current international legal frameworks, to offer a forum for broader international discussion expressing an outlook towards increasing and advancing international law-enforcement and judicial cooperation among the national authorities and between international and regional organizations. These developments should consider the influences of new and emerging issues in respect of international law-enforcement and judicial cooperation in criminal matters, alongside with recommendations on capacity-building. These recommendations should show an equal concern for the situation in countries at different stages of development in order to avoid a chaotic future.

In terms of the way ahead:

- States should adopt appropriate domestic legal frameworks on cybercrime and electronic evidence, in line with international standards, such as the Budapest Convention;

- States – with the support of international organizations – should continue to build capacities and skills of law enforcement agencies, prosecution services, and judiciary;

- Criminal justice authorities should strengthen cooperation with the private sector that will enable timely access to data;

- Streamline procedures involved in the processing of mutual legal assistance requests. States may consider accession to the Budapest Convention as a framework for international cooperation;

- International organizations should further enhance their cooperation with each other and seek synergies in capacity building activities.

- Speakers repeatedly emphasized the importance of communication and cooperation between governments and the private sector, particularly in the case of countries that do not yet have firmly established relationships with common providers.

- There was an agreement among the participants on the need to work on capacity building strategies for operators of the criminal justice system about the challenges of computer-related crime and digital evidence. To promote interdisciplinary courses of legal and technical content. To promote "training of trainers" in the different countries of the region and to promote a better use of the resources for international cooperation.

- Acknowledgement of the importance of the creation of special prosecution offices to deal with cybercrime and to promote joint activities and links among special prosecutors' units at a regional level.

- It was also acknowledged the need of new criminal procedure laws regarding digital evidence and the creation of procedural powers. It is recommended the use of the Budapest Convention as a guideline.

- It was accepted the urgent need to work on new rules (at the international and national level) regarding trans-border access to data and data in the cloud. Further, it was considered important the inclusion of an additional protocol to the Budapest convention regarding: data preservation, production search and seizure orders when data is in another jurisdiction.

- It was deemed important to promote rules regarding trans-border voluntary cooperation of ISP (asymmetric cooperation).

Participants expressed their appreciation of the way the conference was organised and of the quality of the interventions by speakers.