Workshop 3: Capacity Building on Cybercrime and E-Evidence: What Impact?

Keynote on Public-Private Cooperation on Cybercrime Investigations In Latin America
By Dr. Cristos Velasco

Goof afternoon ladies and gentleman, first of all, I'd like to thank the Council of Europe and specially Mr. Manuel Pereira, manager of the GLACY + Project for the kind invitation to share some views and participate in the workshop discussions of this relevant topic that is key in facilitating and improving the global cooperation against cybercrime.
I will then proceed to give you a brief personal overview on how the public-private cooperation landscape in the fight against cybercrime looks like in Latin America and more in particular how that cooperation should be expected to evolve and develop in the next years with the different partners and international organizations working in this relevant field.

National Strategies on Cybersecurity

The implementation of national strategies on cybersecurity has considerably grown in the last two years in the Latin American region as a response to the global cyber attacks that are getting more sophisticated in terms of both, the technical capabilities used and exploited and the plurality of entities, actors and affected users targeted as a result of the attacks. Currently, ten countries of Latin America have implemented a National Strategy on Cybersecurity. More recently Guatemala and the Dominican Republic enacted their national strategies on cybersecurity on June 21, 2018.

The great majority of those Cybersecurity Strategies have commonalities and they identify and highlight the need to promote and address public-private cooperation for the development of policies related to improve the management of cybersecurity in general and they also address interoperability aspects so that they could work under a common regulatory framework. normally under the coordination an supervision of a national government entity.

Likewise, the great majority of those Cybersecurity strategies make specific mention to the need to coordinate policies in the fight against cybercrime and recommend enacting substantive and procedural legislation based on international standards like the Budapest Convention. Unfortunately none of those Cybersecurity Strategies specifically mention how the public-private cooperation for the investigation and the obtention of electronic evidence that might be relevant for cybercrime investigations and in particular how the use of information exchange should be conducted for purposes of investigating criminal conducts that might affect for instance the patrimony of internet users, the critical infrastructure of government entities or financial assets or intellectual property and resources of the private and banking sectors.

On this respect, the Council of Europe is many steps ahead and I firmly believe that it is going in the right direction since this organization has been promoting public-private cooperation since 2008 through instruments such the *Guidelines for the cooperation between law enforcement and*

internet service providers against cybercrime. The CoE has been working very closely in the last years promoting public-private sector alliances between global internet services providers and national investigative authorities of the criminal justice system to facilitate and improve the framework and current practices for the investigation of cybercrime and protect citizens against the sophisticated and complex attacks that we have seen in the last years.

The State of National Legislation and the Measurement of Level of Cooperation

In view that one of the objectives of this workshop is to measure the concrete outcomes, impact and results of capacity building on electronic evidence, and considering the different activities in this area where I have had the opportunity to participate in countries of the Latin American region under the GLACY+ Project. I would very much dare to acknowledge this audience that the cooperation is yet incipient but it is gradually evolving since the great majority of countries of the Latin American region that are now part of the Budapest Convention (Dominican Republic, Panama, Chile, Costa Rica and more recently Argentina) including some other countries that are not yet part of this instrument have become aware on the importance of taking the necessary steps to promote a national reform to their criminal procedural legislation in order to allow the authorities of the criminal justice system in charge of the investigation, prosecution and adjudication of crimes to establish effective procedural measures and mechanisms that allow for the use and recognition of electronic evidence in criminal investigations pursuant to the procedural provisions and safeguards contained in the Budapest Convention in combination with best practices of the private sector in this area..

Many countries in the region already contain provisions within their criminal legislation that regulate and mandate the cooperation of mobile telephone service operators and internet service providers with law enforcement authorities in the investigation of crimes that are committed through the use of technologies. In my opinion, this has been a good starting point, however when it comes to the facilitation of customer information in practice, national authorities and in particular the police and public prosecutors often highlight difficulties and barriers to gather and obtain information on a more flexible and expeditious basis in order to complete an investigation and this is due to various reasons. First, there are loopholes or gaps in the legislation that do not specifically underline the scope, duration and limits and how the information should be provided, a situation that occurs very often in practice. Second, the fact that the main Internet Service Providers are located in foreign jurisdictions and the fact that they have to go through formal mutual legal assistance channels to obtain that evidence, it is another major obstacle that delays and often prevents police and law enforcement authorities to finalize an investigation.

If we had to measure the *'state of the legislation'* that provides for cooperative measures between the public and private sector for the investigation of cybercrime in an scale from 1 to 10, I'd very much like to say that great majority of countries of the region are positioned between scale 5-6 while other are positioned even much lower based on the fact that the legislation is their countries is non-existent, and if there is, there are usually ambiguities and more importantly because there continues to be a lack of trust and credibility in investigative authorities of the national criminal justice system, a situation that is gradually changing but it is still conceived by the private sector as another barrier to facilitating cooperation.

Cooperation with Global Internet Service Providers and how that cooperation has evolved under the Budapest Convention

Without doubt, legislation plays a major role in strengthening cooperation between law enforcement authorities and the global Internet service providers for the investigation of cybercrime. This year, we have seen the enactment of legislation in the United States that facilitate law enforcement officials access to information and data from Internet Service Providers for purpose of investigation of crimes. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was passed on 23 March 2018 primarily as a response to the difficulties of the national law enforcement authorities in the US for obtaining remote data of foreign citizens and national residents stored in foreign servers of major global Internet Service Providers via warrants or subpoenas under the Stored Communications Act of 1986. The CLOUD Act, which is a comprehensive piece of legislation authorizes the U.S. government –interalia- to enter into executive agreements with *'Foreign Governments'* to facilitate law enforcement authorities access to data of citizens of other countries, pursuant to a broad list of procedural and substantive safeguards. Conversely, foreign governments must commit to ensuring that U.S. law enforcement can directly request communications content from the local providers of those countries, a situation that could have unforeseeable consequences like bypassing the existent mutual legal assistance treaties that the United States and Europe have with countries of the Latin American region.

Further, the European Commission's and EU Parliament recent proposals for a *Regulation on European Production and Preservation for E-Evidence in Criminal matters* and the *Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* will also have an impact on the regulatory framework and practice on mutual legal assistance for criminal matters in countries of Latin America. Unfortunately, the great majority of government actors and entities in Latin America are not yet fully aware on the arm's length and extraterritorial scope of the CLOUD Act and the European Commission's legislative proposals particularly with regards on how the mutual legal assistance framework and cooperation on criminal related matters in the field of cybercrime will work. Therefore, I believe its is important that the Council of Europe as well as other international organizations working in the fight against cybercrime incorporate in their capacity building initiatives a component or pillar with regards to the interoperability and function of the mutual legal assistance measures and mechanisms contained in major global laws like the American and European legal frameworks based on the current practice of major Internet Service Providers while at the same time address the major drawbacks, and point out the advantages and disadvantages based on the national legal framework of countries of Latin America.

The Way Forward for Latin America

Indeed, there is the need to improve the public-private cooperation in Latin America particularly with regards to the different levels of cooperation addressed by the Budapest Convention, some levels of which are regulated to a certain extent under the criminal legal framework of some countries of the Latin-American region.

Internet service providers and mobile service providers are key allies particularly with regard to the information they have that could possibly lead to the whereabouts of probable suspects and perpetrators of cybercrimes. The participation and commitment of both, Internet Service Providers and Mobile Service Operators with the national investigative authorities of the criminal justice system is fundamental and shall continue to be promoted in the capacity building initiatives of the Council of Europe and other international organization working in the fight against cybercrime taking into consideration the protection of safeguards and fundamental rights of citizens.

The transnational dimension of cybercrime has traditionally been problematic for the national investigative authorities specially because some of the conducts might have different effects or repercussions in different jurisdictions and most of the time, the perpetrators are not located within the same jurisdiction or territory of the victims or where the damage was done or felt, a situation that often hinders or prevents local law enforcement authorities from launching or initiating an investigation. This situation, -which is very common- requires an effective coordination and cooperation of national and international investigative authorities with major global internet service providers and mobile service operators, whose cooperation will often determine the course of a criminal investigation at both, the national and global level.

Legislation such as the CLOUD Act shall not be seen as barrier but particularly as an 'Opportunity' for the national investigative authorities and entities of the national criminal justice system in Latin-American to work more closely with their counterparts in the US government and with global service providers to address the main concerns and provide adequate responses that could make the mutual legal assistance mechanisms to work more dynamic and effectively while respecting due process measures, fundamental rights and the national framework on data protection of countries of Latin America. However, it is extremely relevant that the authorities of the national criminal justice system and local service providers bring this issue to the attention of their respective Foreign Affairs Ministries and National Congress so that said institutions could analyze and start working on a legislative reform that might help to improve and strengthen the current framework of MLA's treaties primarily with the US and Europe so that the public-private cooperation for the investigation of cybercrime -as established under the Budapest Convention and the Council of Europe capacity building initiatives- becomes less burdensome and fully operative in countries of Latin America in the near future.

Thanks a lot for you attention. I look forward to further contributions to the discussions in this workshop.

Dr. Cristos Velasco