LACIGF 12 Report

Title of the session: Session 10 – Cybersecurity and Cyber-Defense: Current Reality and How to Increase the Resilience of Our Societies for the Future

Session summary:

Session 10, moderated by **Ernesto Bojórquez (LACTLD, Mexico)**, was about cybersecurity and cyber defense. Ernesto began by proposing a brief reflection on how the world became a cyberworld and how security became cybersecurity, later he read 3 questions, which were answered by panelists:

1. What is the major / advance / setback or difficulty in terms of cybersecurity in Latin America?
2. What efforts are being made in the region to develop good cybersecurity practices?
3. What kind of cooperation is being carried out in the region or in your countries regarding cyber defense?

The first speaker to answer was **Maryleana Mendez (ASIET, Costa Rica**). She began by pointing out that cybersecurity is a very complex matter and that there is a shortage of cybersecurity specialists and the cost of cybercrime reaches $ 600 billion. She also said that the attacks have grown a lot and have become more sophisticated, adding that the user layer is the one which needs more investment since the lack of digital user education allows several failures, being the weakest link in this chain. It is necessary to teach the user not to become a victim or a possible source of attack.

Lía Solís (ISOC Bolivia, Bolivia) answered the second question, after giving a brief explanation about ISOC and its objectives. She showed the action plan for 2019, which is divided into four points, two of which were directly related to the session: to improve technical security and build trust by creating good practices and standards for routing tables, and also the creation and adoption of MANRS, a project that aims at defensive actions to reduce threats to routing.

Carlos Guerrero (Hiperderecho, Peru) began his presentation by quoting John Perry Barlow, in *A Declaration of the independence of Cyberspace*, in 1996, in the city of Davos. This quote was used to explain what the scenario was at this period of Internet and the position of governments. Then he said that today it would be impossible to say that the State should not regulate what happens on the Internet. After this preamble, he indicated that cybersecurity is a relatively recent concern in Latin America and the Caribbean; nevertheless, interesting projects have been developed, thanks to the support of entities such as the Organization of American States (OAS) and Inter-American Development Bank (IDB). After that, Carlos went further into explaining the difference between cyber defense and cybersecurity, noting that the latter is about cybersecurity of people's safety and the possible attacks they may suffer, and therefore it is necessary to determine safe practices that can be used or learnt by them in order to handle better with digital environments. He said that, currently, governments, private sector and civil society are having a discussion about what cybersecurity should involve and this is generating a correlate, in the way how cybersecurity plans are implemented, through technology purchase and capacity development.

Lorena Naranjo (DINARDAP, Ecuador) opened her presentation by quoting a global security index for the Americas, where there are five evaluation pillars: legal, technical, organizational, capacity building and cooperation fields. This index allows us to see where we stand in the region when it comes to cybersecurity issues. According to what Naranjo commented, Uruguay is the only country in the entire region that meets adequate cybersecurity standards. She mentioned the vulnerability of being part of the Budapest Agreement and the difficulty that it represents in generating qualified cooperation. The speaker stressed that there are not enough personnel trained in cybersecurity issues. However, there are important advances, such as the fact that cybersecurity plans or strategies already exist in 10 countries in the region. For example, in Ecuador they are working on a cybersecurity strategy called Digital Ecuador, which establishes connectivity, security and economic dynamics as its fundamental pillars. It represents an integral vision, where the human being is the center of cybersecurity and where the different visions are combined. This is important because the concept of security has changed, it is not only about state or territorial security anymore, but about people security, on which the central axis is Human Rights.

Outputs and other relevant links:
Full session: https://youtu.be/fIN3dDH7FzI

By: Carlos David Carrasco Muro (Observatorio del Gasto Fiscal, Chile), Matheus Figueiredo Lima (UNICURITIBA, Brazil)

Translation: Laura Gabrieli Pereira da Silva (UNESP, Brazil)

Revision: Verónica Arroyo (Access Now, Peru) and Luis Gustavo de Souza Azevedo (UFAC, Brazil)

Coordination and edition: Nathalia Sautchuk Patrício (NIC.br, Brazil) and Guilherme Alves (Youth Observatory, Brazil)