LACIGF10 – 2-4 August 2017

Session 4. Cybersecurity: progress, setbacks, challenges and trends from a Human Rights perspective

Date: Wednesday, 2 August. 5 to 6.30 PM

Moderator: Diego Morales – IPANDETEC

Panelists:

- Martín Borgioli – Hiperderecho
- Shernon Osepa – Internet Society (ISOC)
- Maureen Hernandez – Internet Society (ISOC) Venezuela
- Ernesto Ibarra – Presidency/MX
- Maria Cristina Capelo – Facebook

Rapporteur: Alejandra Erramuspe – AGESIC Uruguay

Remote Moderator: Youth LACIGF

1. Introduction

The aim of this roundtable is to encourage dynamic, interactive dialogue to assess both the priorities and the implications of cybersecurity in our region, in its various dimensions: technology, Human Rights, governments and other stakeholders' roles.

There is still a long way to go with regard to building trust, managing cyber threats, sharing local experiences and offering capacity building models. The need to align cybersecurity policies and strategies within the international Human Rights framework remains one of the key issues and further multistakeholder discussion regarding the matter is needed.

Cybersecurity is still present in the LACIGF agenda, as well as in local and global discussions regarding internet governance. For the past few years, we have focused on surveillance and privacy issues when talking about cybersecurity. Recently, there has been a growing trend in our region of cases of limiting access or shutting down the Internet, limitations on anonymity, encryption and indiscriminate expansion of surveillance, often invoking reasons of national security.

2. Session Structure

- Roundtable
- 3 key questions, each with 2 minutes for each speaker, including questions and comments from the audience.

3. Key questions

- Which has been the most important cybersecurity progress, setback or challenge in the region?
- What is the current scenario with regard to Internet restrictions and shutdowns?
- How will users' trust in the Internet affect the future of the Internet?
- What examples of good practices in cybersecurity do we have in the region?
- Which areas should the region work on in order to ensure that cybersecurity policies and practices take into account the recommendations of UN and OAS rapporteurs as well as existing international frameworks?
- Which would be the most effective way of counteracting the tendency of governments to apply restrictions or shut down the Internet?
- How can we advance in building trust in the internet? What can LAC do to create an environment that will strengthen Internet trust?

4. Panel Discussion

The moderator began by presenting the main progress and greatest setbacks regarding cybersecurity in the region and how far it is possible to go.

It was pointed out that the main progress is that different voices are being increasingly included. Also, that participatory models have contributed to these issues being better addressed, not only with regard to technology, but also with regard to cultural and legal aspects.

The main setback observed in the region is the emergence of mass surveillance. It is hypocritical to demand a multistakeholder approach to solve this problem. We must acknowledge our responsibility and ask ourselves what we are doing to improve our cybersecurity.

Attention must be paid to Human Rights issues: privacy, freedom of expression, the right to search for and receive information. A crucial point in this regard is that we are seeing the blocking of Internet content, something that must be avoided.

One aspect to consider is the blocking of content. ISOC is working on this. Governments often want to put an end to certain things that can happen online. These web phenomena include gambling, the violation of intellectual property rights, the protection of children and adolescents, and national security. ISOC may help find solutions to these issues.

Five types of blocking currently observed by ISOC:

a. Blocking at IP address or protocol level: addresses can be included on a list and blocked.

b. Deep packet inspection with specific attack techniques.

c. URL: knowing the location of the information.

d. Platform biz: Search engines. Google for example. There's others.

e. DNS blocking

It was suggested that we must take as a reference the suggestions of independent rapporteurs, which need to be heard. There are differences between what governments believe and what Human Rights organizations say.

Governments often collect information about their citizens without asking for authorization and without informing them. There has to be a purpose to these actions, and they must be in line with Human Rights.

Civil society argues that it is difficult to speak of trust in a context of violation of rights. Participation of civil society needs to occur within a reliable framework. At present, such trust does not exist.

A good practice which can be exported to the region is to address cybersecurity with a strategic vision, as a tool for the development of innovation. To promote the adoption of these exercises in collaboration, not only in planning, but also in the implementation of cybersecurity strategies. Cybersecurity challenges are global, so we all need to work together.

We need to aim at building trust. In order to build trust, the paradigm that cybersecurity is “dark” must be abandoned, we need to demystify it, so that users can keep their mind open and become aware of these issues. Such awareness may stem from knowledge of the tools.

Cybersecurity requires government to commit to defending the population not only from external threats but also in the adoption of technology.

We are not aware of the lack of security of many of the applications we use on a daily basis.

How can we build trust? Building trust is not easy. An open data system would be useful. In countries which collect data, there should be laws to protect such data. If there were more information on these issues, users would have greater confidence. Also more interaction to strengthen legislation and institutional frameworks. Before implementing any policies, before passing any legislation, it would be necessary to hold a discussion with civil society on the matter.

Moderator: Which conditions are you observing in the region that might damage trust?

The three levels of the Internet were discussed: infrastructure, DNS and applications. The need for a holistic solution and concrete measures was stressed.

It was mentioned that often users do not know when they are placing their security at risk, which is why it is necessary to work with the education system, so that users will be cautious. The actions of civil society play a key role in this regard.

Some politicians or policymakers are not trained in technology issues, which is why it is important that these stakeholders have the ability to give citizens the confidence they need. In past decades, the appearance of digital policies has created division with regard to the responsible use of the Internet and ICTs. It is therefore necessary to have an alliance of different stakeholders in order to influence this process. Internet governance initiatives developed in each country are important.

Further open and transparent work on these issues would help, as cooperation and co-responsibility bring greater value.

Audience Participation

- How do governments adopt public policies and what process do they use? Sometimes there is a lack of commitment on the part of governments. There is genuine concern about what is secure, what is private and what is open. We need encryption to protect data. How can governments integrate these concepts?
- Citizen participation and the construction of evidence that will allow public agencies to create a more appropriate public policy. Empowerment of civil society and academia as well as their participation, all part of a cycle constantly serving as input for public policy. Need to strengthen jurisdictional work.
- LACRALO: In Latin America we have a network of 52 organizations in 21 countries conducting training sessions for Internet end users. Given that governments do not issue guidelines, we need to do that ourselves, from the bottom up.
- Technology will help improve security. At the same time, it is important to work on the cultural aspect.
- Cybersecurity is presented as something “dark,” but this is not so. Cybersecurity needs a specific approach, a closer perspective.
- There is a personal data policy in force in Peru. It includes a police department for dealing with specifically these issues, as well as a CERT. There is a need for close cooperation, as cybersecurity needs to be addressed keeping everyone in mind.
- Often disregarded, online security for women and activists must be addressed.
- Users are not familiar with encryption and how it works.