UNVEILING THE CYBERSECURITY AGENDA IN LATIN AMERICA
THE ARGENTINE CASE

FIRST PUBLICATION

1

What do we understand by cybersecurity?

APC
por los Derechos Civiles

Privacy Area

October 2015

https://adcdigital.org.ar

Índice

Unveiling the Cybersecurity Agenda in Latin America: The Argentine Case

First publication: What do we understand by cybersecurity?*

I The project

Discussions on Cybersecurity are taking place in international contexts, as is the case with the Organization of American States (OAS) and its programs, without the participation of civil society and without considering the perspective of human rights protection. On the other hand, these discussions are also being included in national agendas, which include topics such as the State's security, intelligence mechanisms and surveillance practices.

The research projects that have been conducted on the subject matter by ADC, Derechos Digitales and other civil organizations in the region allow us to describe the following scenario: surveillance practices in the Southern Cone, especially those related to intelligence activities, are not aligned with a broad perspective of human rights, lack an adequate control and they usually constitute grounds for illegal actions that end up affecting citizens' rights or weakening the democratic system and its institutions. This is the case as there are Latin American

*This document was produced by the Privacy Area of ADC.

countries that have legal frameworks allowing them to massively obtain information on their citizens; and, even worse, the organisms in charge of collecting this information, intercepting communications and performing surveillance and cybersecurity tasks are often inherited from military dictatorships. This inheritance generally means obscure methods, disproportionate data collection, excessive secrecy, lack of transparency and a large record of human rights violations that have gone unpunished.

This first publication is part of a series of three documents that we will publish on a bimonthly basis under the framework of a research project whose findings will be published during the second half of 2016, and whose main purpose is to determine the existence and content of a cybersecurity agenda in Latin America, focusing especially on the Argentine case in order to determine its alignment with human rights protection standards and, if necessary, make the corresponding suggestions or recommendations.

II Cybersecurity: the first approach

Before describing the current situation of cybersecurity in Argentina, we asked ourselves this very first question: What is cybersecurity?

Thus, we started looking for a definition, with the understanding that finding such definition would shed some light on the context in which this topic is being discussed, while helping us to interpret –in a restrictive or lax fashion- its extent and the different elements that must be taken into account when talking about cybersecurity.

However, it was not as easy as it may seem. So far, in our country, there is no (at least as far as we have been able to investigate before issuing this document) agreed upon or unanimously adopted definition by state organisms. Hence, we changed our approach and looked for a definition of cybersecurity in other national and international sources.

We were able to notice that, despite attempts to agree on Internet and technology related issues at an international level are not new, the cybersecurity debate seems

to have deepened some issues, given that the States have opposing interests, as far as how to regulate an activity, what its concept and extent should be, or what activities could amount to a crime. As a result, agreeing on a definition is a complex task where multiple factors should be considered.

For that reason, we started analyzing some of these factors; we compared concepts used by various countries and international organisms with the view to establishing rules for analysis that will allow us to approach and understand the Argentine cybersecurity agenda, so that it can conform to human rights protection standards.

III Factors influencing its development

i From low-cost storage to the "collect it all" motto

The data storage technology has made giant steps in the last few years towards reducing production costs and the byproduct. Hence, by the end of 2000, the average cost of 1 Gigabyte storage was USD 10; by 2005, the average cost had come down to USD 1 and, currently, by the end of 2015, the average cost per GB is lower than 5 dollar cents.

Companies and governments started to realize that it was unnecessary to get rid of all the information they collected from their users, claiming they could need it in the future and especially because they would not have to deal with high storage costs anymore.

State Governments were also part of this paradigm shift concerning information storage, even through the use of practices that may be considered clearly illegal.

The most emblematic case, shaping up as the most important of the decade, was the one reported by Edward Snowden (former NSA analyst) in 2013, who leaked thousands of documents that unveiled the programs conducted by the National Security Agency of the United States and the Government Communications Headquarters, whose main activity is to store information in a massive and

indiscriminate way, with different deadlines. For example, 3 days for calls' content and e-mails under the XKEYSCORE program; 1 year for the search history under the MARINA program; and 5 years for phone calls metadata. It should be noted that when an analyst uses stored data, its retention period becomes unlimited. This reflects the NSA's motto *"Collect it all, sniff it all"*.

ii Easy acquisition of massive surveillance tools

Besides the citizens' data storage factor, we also found out that massive surveillance tools are becoming easier to acquire, given that their development is no longer under exclusive military and state monopoly. The most recent case is that of the Italian company Hacking Team, which is well-known for selling spyware and applications for remote access to electronic devices. After hacking its internal databases and leaking more than 400GB of information, it was discovered that the company conducted business with governments of different regions in the world and even with authoritarian regimes that were penalized by the international community. Hacking Team has a strong presence in Latin America too, in countries such as Mexico, Chile, Colombia, Ecuador, Honduras and Panama, holding some conversations in Argentina as well.[1]

Hacking Team is just one of the participants within a bigger and multimillionaire business devoted to marketing surveillance and communication interception software. We may also mention the American company Blue Coat, the main NSA distributor, also present in Argentina; Gamma International, an Anglo-German company known for its FinFisher software solution, also called FinSpy; the French company Vupen Security; the Israeli NSO Group, a well-known competitor of Hacking Team, owner of Pegasus software; and the German company Utimaco.

The easy access to surveillance tools must be analyzed as a bidirectional issue. In this sense, government agencies and departments, as well as private corporations, are able to acquire this type of products without bureaucratic or legal barriers,

[1] "ADC Warning: Interception Software and Human Rights Violation". August 2015. Available on (PDF) http://www.adc.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf

even at prices that are far from being unreasonable. This situation also has an impact on relationships between "opposing" states (for example, USA – Russia) and private companies that compete for this "clientele".

One of the direct consequences of this interaction resulting from the easy access to and acquisition of these technologies is the high risk all involved parties run.

In this context, we may notice the key role played by cybersecurity regarding the protection of the infrastructure used to manage sensitive information and data, among others.

IV Analyzing the concept of Cybersecurity

Thus, when analyzing what cybersecurity is, we discovered that the definition may be approached from three different perspectives, which vary depending on who uses the term.

- Cybersecurity as the protection or defense of a State's infrastructure, its networks, data and users;
- The work performed by investigation security forces, prevention and actions against crimes in the digital field (cybercrime);
- Surveillance activities conducted by intelligence bodies.

We can make this triple distinction because there is still no defined concept of what cybersecurity is at a global level, let alone at a regional level in Latin America.

Yet, international organisms have made progress on this subject by coming up with their own definitions.

The International Telecommunication Union (ITU), a United Nations specialized agency in the field of communications and information technologies, established

a definition for cybersecurity in Recommendation UI-T X.1205,[2] later approved by Resolution 181,[3] which sets forth (bolding added for emphasis):

> Cybersecurity is the collection of **tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets**. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; confidentiality.

The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR), of the Organization of American States (OAS), established in its publication "Freedom of Expression and the Internet"[4] that "'Cybersecurity' is usually used as a broad term to refer to various issues, ranging from the security of the national infrastructure and networks through which Internet services are provided, to the security or safety of users. Nevertheless, subsequent developments suggest the need to limit the concept exclusively to the safeguarding of computer data and systems. (...) this narrow focus allows for a better understanding of the problem as well as a proper identification of the solutions needed to protect interdependent networks and the information infrastructure".

---

[2] UIT. UIT-T X.1205 Recommendation. April 2008. Available on: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

[3] UIT. Resolution 181. November 2010. Available on: https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

[4] OEA. CIDH. Freedom of Expression and the Internet. December 31, 2013. Available on (PDF): https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

As mentioned by the Rapporteur, this limited focus on the concept of cybersecurity intends to avoid the criminalization of the use of the Internet which is the reason why "(...) the response of States in regard to security in cyberspace need to be limited and proportionate, and designed to meet specific legal aims that do not jeopardize the democratic virtues that characterize the Web".

It is worth mentioning that, even though the OAS has a Cybersecurity Program, designed –among other things- to help Member States to adopt national strategies for cybersecurity, they do not provide their own concept of cybersecurity, despite the fact that their reports develop the topic in connection with best practices and regional reports on the status of cybersecurity.

In the American continent, there are various countries that have already implemented national cybersecurity policies or they are working on them. Canada's[5] main focus regarding its cybersecurity strategy is not only to secure government information systems and maintain alliances that will help them to guarantee systems outside the government, but also to help citizens to search and use the Internet in a safe manner, which involves fighting against cybercrime. This means providing security forces with modern resources and obliging Internet providers to maintain interception systems so that they may be requested, through court order, to intercept communications of a given target within the context of an investigation, and to provide their users with information.

When it comes to European countries, France's[6] efforts, for example, are also based on a broad concept of cybersecurity, as it focuses both on the protection against vulnerabilities of any systems storing, processing and transmitting data and on the use of those techniques of information security systems in order to fight cybercrime and maintain the cyberdefense of the country.

[5] Public Safety Canada. Cyber Security Strategy. Available on (PDF): http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

[6] UIT. Cybersecurity National Strategies. France. Available on (PDF): http://bit.ly/1Tj7gUH

V The concept of cybersecurity in Argentina

The first steps made in this investigation showed that the term cybersecurity appears in some regulation. For example:

In 2011, the Presidency of the Cabinet of Ministers issued Resolution No 580/11[7] in order to establish the National Program of Critical Information Infrastructure and Cybersecurity (ICIC, for its acronym in Spanish). This was the first legal document using the term cybersecurity, but it has not provided any type of definition. Four years after its creation, there are many State divisions that have been working on implementing the regulation's content. However, since this resolution only established general guidelines, each State's department has the power to adopt them as they see fit.

The department that is in charge of developing the ICIC program is the National Department of Critical Information Infrastructure and Cybersecurity,[8] which depends on the Undersecretary of Critical Information Infrastructure and Cybersecurity Protection, also dependent on the Cabinet Secretary of the Presidency of the Cabinet of Ministers.

However, neither the resolutions and decrees regulating ICIC, nor its official website,[9] explain the concept of cybersecurity that is used for the development of its activities, and, unlike the countries abovementioned, Argentina does have a documented national strategy on cybersecurity that can be publicly accessed.

On the other hand, on July 6, 2015, the New National Intelligence Doctrine was approved through Decree No 1311/2015,[10] which set forth the regulatory framework for the National Intelligence System and, most importantly, for the operation of the Federal Intelligence Agency (AFI, for its acronym in Spanish).

In the second chapter on "Extent and Activities of National Intelligence", the

[7] Resolution 580/2011. Available on: http://bit.ly/1Tj7gUH

[8] Decree 1067/2015. Available on: http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm

[9] http://www.icic.gob.ar/accessed on 10/28/2015

[10] Decree 1311/2015. Available on: http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

Doctrine established that criminal intelligence involves "producing intelligence in connection with criminal issues and, in particular, with those complex criminal issues of federal nature related to terrorism, attacks against the constitutional order and democratic life, organized crime and attacks against cybersecurity".

On the other hand, in the "Organic and Operating Structure of the Federal Intelligence Agency", within the same Doctrine, article 49 created the "Cybersecurity Intelligence Operations Department", which is "responsible for producing intelligence in order to gain awareness of the actions taken against cybersecurity in regards to the national defense or homeland security, and of the national or foreign groups that are responsible for performing them" and consists of the "Department of Computational Intelligence" and the "Cybercrime Intelligence Department".

Said article finally added that the Cybersecurity Intelligence Operations Department is designed to develop collection, management and information analysis activities and consists of officers and analysts who are experts in cybersecurity.

Once again, despite the repeated use of the term, the text does not have a definition or concept explaining what cybersecurity is for the National Intelligence System.

VI Corolary

We may summarize our first conclusions as follows:

- The difficulty and challenge involved in defining cybersecurity.
- The consequences on human rights that could result from the adoption of a broad or narrow definition of the term cybersecurity.
- The lack of a clear and enlightening terminology that allows establishing the extent and limitations of the actions taken by the Argentine state in regard to cybersecurity may result in undesirable effects such as the juxtaposition or even contradiction of implementation criteria among the

different departments, the adoption of discretionary measures by officers in power without any type of control or supervision, the use of obscure practices and a lack of transparency, and, all in all, the creation of a scenario promoting the violation of human rights.


APC
por los Derechos Civiles