UNVEILING THE CYBERSECURITY AGENDA IN LATIN AMERICA. THE ARGENTINE CASE

THIRD PUBLICATION

3

The voice of the experts

por los Derechos Civiles

Privacy Area

March 2016

https://adcdigital.org.ar

Índice

Unveiling the Cybersecurity Agenda in Latin America: The Argentine Case

Third publication: The voice of the experts*

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 countries that have legal

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

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 third 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.

In the first publication, referred to as “What do we understand by cybersecurity?”, we focused on the definition of the term at a global and national level, in order to highlight the lack of a definition, even though the term ‘cybersecurity’ appears in various regulations.

In the second publication, referred to as “Regulatory Framework”, we showed the regulations where the term is used as well as their extent, in order to determine the institutional framework of this concept.

In this third publication, we will inquire into the opinion of some professionals from the technology community with respect to the policies, practices and regulatory framework related to cybersecurity in Argentina.

Over the course of the work conducted by ADC, mainly through research, workshops and round-table meetings, we have noticed that the various professional communities that form part of the Internet ecosystem are not always working together, or at least fail to communicate fluently. The particular dynamics between the legal and the technology community serves as an example to illustrate the point.

For this reason, and considering interdisciplinary work is key to approaching these topics, the focus of this document will be to highlight the viewpoints presented by professionals who work, directly or indirectly, on the cybersecurity issue. It is not the intention of this report that the opinions described herein be understood as a reflection of the entire community, but on the contrary, as the voice of those experts who specialize in this subject. The professionals who helped draft this document are:

Mariano M. del Río: he is an expert in Cybersecurity, Compliance and Privacy, with more than 10 years of experience in the implementation of Information Security Programs and compliance with key laws and regulations related to the subject in various industries. He has founded SecureTech, an Argentine company on cybersecurity and compliance services. He collaborates with SecuringTheHuman (SANS Institute), INCIBE and ENISA, among other agencies. He is a Member of Thiber –the cybersecurity think-tank– and of the Industrial Cybersecurity Center (CCI, for its acronym if Spanish). He has created Security Guides for health services companies, social organizations and journalists.

Darío Piccirilli: He has been working as an expert in Computing Investigations since 1981 in the Civil, Labor, Commercial and Criminal jurisdictions. He holds a Magister's degree in Software Engineering from the Instituto Tecnológico de Buenos Aires (ITBA) and the Universidad Politécnica de Madrid, and is completing a PhD in Computing at the Universidad Nacional de La Plata (UNLP). He is the Director and Head Professor of Computing Investigations at the Universidad Tecnológica Nacional (UTN), Director of Postgraduate Courses on Computer Forensics at UNLP, and Postgraduate professor at the Magister's degree in Software Engineering at UTN. He has been a Consultant and Computing Auditor of the Supreme Court of Justice in the City of Buenos Aires.

Interviewee R: another professional who helped draft this document and

who has ample experience as a consultant in the field of information security. For professional reasons, he has decided to remain anonymous and he will be identified as 'Interviewee R' throughout the document.

Next, we will analyze the answers this group of professionals provided regarding certain cybersecurity aspects that we have been investigating in these series of reports.

II Going back to roots: cybersecurity as a practice

Reflections on what cybersecurity means

According to Mariano del Río, cybersecurity is "a practice whose purpose is to protect technology information assets, that is to say, those assets supported by ICT". He also adheres to the definition provided by the International Telecommunication Unit.[1]

On the other hand, Darío Piccirilli defines cybersecurity as the "security control related to the Cloud[2] (public and private data), with the security validation management of identities and accesses. It also comprises security in mobility, related to the risks that mobile devices represent today. It also comprises advanced protection against fraud (including data, infrastructure and applications)".

Finally, for Interviewee R, cybersecurity "is the security information area in charge of protecting information and resources used in cyberspace. It is connected with the information and assets used in computer networks, and especially on the Internet. In other words, it focuses on threats to

[1] Available on: https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

[2] Note: *'Cloud'* refers to information in the Cloud. https://es.wikipedia.org/wiki/Computacion_en_la_nube

processed, stored and transmitted information through interconnected information systems".

III Issues arising from the lack of definitions

For Mariano del Río, it is urgent to implement a National Strategy on Cybersecurity, "there are plenty of examples both in America and in the rest of the world, it is the most adequate way of handling such a vast subject. Cybersecurity risk management should be a State Policy, as it could affect both the public and private sphere, as well as society in general. It is necessary to develop a broad and new framework that will handle the topics that are currently part of people's daily lives".

Darío Piccirilli adds that "it is essential to have a definition and extent for the term [cybersecurity]. A lack of definition may bring about negative consequences when the boundaries of the term are unclear. We are dealing with an activity that must have clear limits in order to produce clear, complete and flexible regulations".

Interviewee R, who agrees with the abovementioned, considers that "it is important to have a definition, or, at least, to define its extent. However, there is no international consensus on this topic and it may be the case that the definition adopted in local regulations is not the one agreed upon among countries. I think we should closely monitor the progress of international agencies and adhere to the one adopted in the future. In regards to the consequences, I understand that not having an agreed upon definition in the regulations may cause the parties to lack consistent information on the field being regulated, and, as previously mentioned, the extent of the definition may not be established correctly or it may not be possible to convene those players who must participate".

The situation described by the interviewees coincides with the conclusions

included in the first report, which established that 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.

IV Good initiatives without a continuation

The role of the National Program of Critical, Information and Cybersecurity Infrastructures (ICIC, for its acronym in Spanish)

The specialist Del Río knows the ICIC Program in detail, as he collaborated with it on an ad honorem basis drafting documents for the 'Healthy Internet' initiative,[3] one of the four group works created by the Program, in order to raise awareness about the risks of digital media use through educational materials for a responsible Internet use.

"Even though I consider that the Missions and Functions of the program are appropriate, I believe its implementation has been deficient. Up to now, we do not have a catalogue of critical infrastructures, nor a national strategy on cybersecurity. On the other hand, various events have been held. In regards to the impact of the program on public policies, I think that due to the lack of an integral vision of cybersecurity, generally developed through a national strategy on cybersecurity, it has not been possible to influence other State's strata", said Del Río.

[3] Available on: http://internetsano.gob.ar

Over the course of the work conducted for these reports, people who work close to the areas of the State where cybersecurity efforts are or have been taken stated that the regulations introduced were utilized as a guideline so that each State division could adopt measures related to cybersecurity.

Like Del Río, Interviewee R considers that "it is essential to talk about the importance of the protection of critical information infrastructures in those countries where Internet services are provided with an ever growing frequency. In this sense, the ICIC Program has been a pioneer. However, there has been no meaningful progress made since its creation; nor has it had any influence on public policies and cybersecurity practices in our country. It is urgent to follow this path".

V Intelligence work as part of cybersecurity

In some Latin American countries, discussions on cybersecuruty have taken place in the same context in which topics such as massive surveillance and digital communication privacy occur, given that some consider state intelligence activities as part of cybersecurity practices, as is the case with Colombia.[4]

In Argentina, cybersecurity has already started to be a part of the intelligence system through the creation of the Cybersecurity Intelligence Operations Department, within the Federal Intelligence Agency (AFI, for its acronym in Spanish). In this respect, the specialists made the following observations.

Del Río holds the view that "Undoubtedly, [cybersecurity must have a permanent intelligence activity], reviewing the limitations security forces [Law

[4] Debate on Cybersecurity and Human Rights in the public sector. October 2014. Fundación Karisma. Available on: https://karisma.org.co/impactos-del-debate-sobre-ciberseguridad-y-ddhh-en-el-sector-publico

Enforcement Agencies] have when handling cybersecurity issues should suffice. Unfortunately, AFI has been used for other purposes that have nothing to do with providing valuable information in order to fight organized crime. Nowadays, any information regarding cybersecurity is valuable for the investigation and battle against every type of illegal activity".

In this sense, Piccirilli considers it is important to keep track of those aspects that "are related to national defense and the protection of citizens' privacy".

Interviewee R considers that "cybersecurity must be supported by intelligence activities, among others, but they must be used only in those cases where they are necessary and without affecting citizens' rights".

A first approach to the link between cybersecurity and intelligence would seem to show that they should not exclude each other, if we come to think of it, for example, with respect to the detection of attacks against State critical infrastructures. But, on the other hand, it is essential to circumscribe what type of intelligence activities can be carried out, definitely avoiding the indiscriminate surveillance of communications and the direct intervention of intelligence agencies, which must serve as a link when submitting information obtained through their own intelligence efforts to the entity that is in charge of the protection of critical infrastructures, so that they will not turn into a *'digital police'*.

VI So, does Argentina have a cybersecurity agenda?

Current situation and future challenges

According to Interviewee R, "Argentina does not yet have a cybersecurity agenda. A new government administration has taken power at a national level, which seems to have handled the topic through different agencies

with the structure decrees that have been recently published. It is essential to coordinate work among these areas as well as with the private and academic sector and civil society, within a framework of international cooperation and participation in specific forums. The extent of cybersecurity challenges resulting from the potential brought about by technologies for the country's welfare must be informed to the highest authorities so that they will create a cybersecurity agenda, provide resources and secure cooperation and collaboration instances".

The decrees the interviewee refers to –which were issued after the completion of our second report– are, on the one hand, Decree N°13/16,[5] which creates –in the sphere of the National Public Sector– the Modernization Ministry, within which the Undersecretary of Technology and Cybersecurity is created. The latter is responsible for developing a strategy for the national technological infrastructure within the scope of the National Public Sector as well as managing and supervising the actions taken by the National Office of Information Technologies (ONTI, in Spanish) and some of its objectives. On the other hand, Decree N°42/16,[6] created the Undersecretary of Cyberdefense within the scope of the Secretary of Science, Technology and Production for the Defense of the Ministry of Defense. The purpose of the Undersecretary is to "coordinate efforts with agencies and authorities from the different State Powers *in regards to Legislation and national policies on cybersecurity and protection of critical infrastructures*" (emphasis is ours).

On the other hand, Mariano del Río considers an agenda has existed, "but supporting private interests or society's control rather than the public interest. Several state projects have been discovered related to opinion control, spying and other practices that differ from what a cybersecurity agenda should be like in a democracy. I think that in order for an agenda to exist, there must be debates involving different sectors, current issues

[5] Decree 13/2016. Available on: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm

[6] Decree 42/2016. Available on: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm

and the risks citizens face. Of course, new teams need to be formed".

Darío Piccirilli adds that it is important to work with National Universities in order to deal with the topic of cybersecurity, "in order to promote contributions by adequate and updated experts".

VII Final comments

The report published by Trend Micro and the Organization of American States in 2015 on the state of cybersecurity in America,[7] which paid close attention to the Argentine case, emphasized that "although Argentina's capacity for handling cyber threats has shown great improvement since ICIC's founding", it highlighted three obstacles affecting the national cybersecurity practice: "the persistent lack of awareness among stakeholders at all levels, issues and concerns regarding privacy, and insufficient funding. Such challenges will need to be addressed going forward to ensure the success of Argentina's cybersecurity efforts".

Finally, we find it necessary to underscore some principles related to cybersecurity practice as established by the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights in its publication "Freedom of Expression and the Internet".[8]

On the one hand, the Rapporteur stated that "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" (Paragraph 120, page 59). In this sense, "the public policies on cybersecurity should be proportionate to the risk they address and, in any case, the security objective must be weighed against the protection of fundamental rights" (Paragraph 124, page 60).

[7] Report on Cybersecurity and Critical Infrastructure in the Americas. April 2015. OAS. Available on: https://bitly.com/1Fn3O0u

[8] OAS. 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

Additionally, “authorities need to report and be accountable for measures taken with regard to cybersecurity—both those directly implemented and those taken by private intermediaries hired by the State” (Paragraph 126, page 61). “Official programs and public policies on cybersecurity need to have oversight and control mechanisms where the final authority is a judge. There must also be follow-up procedures with some degree of participation by civil society” (Paragraph 128, page 61).

3

por los Derechos Civiles