CYBERSECURITY IN THE MASS SURVEILLANCE AGE

Unveiling the Cybersecurity Agenda in Latin America: The Argentine Case

ADC
por los Derechos Civiles

Privacy Area

September 2016

https://adcdigital.org.ar

Index

Cybersecurity in the Mass Surveillance Age

Unveiling the Cybersecurity Agenda in Latin America:

The Argentine Case[*]

I The Project

Discussions on Cybersecurity are being held in international contexts such as the Organization of American States (OEA) and its programs, without civil society's participation and without considering the perspective of human rights protection. On the other hand, these discussions are also part of national agendas, addressing topics such as the security of the State, intelligence mechanisms and surveillance practices.

The research projects that have been conducted on the 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 due to the fact that there are Latin American countries with legal frameworks that allow them to massively obtain information on their citizens; and, even worse, the organisms in charge of collecting this

[*] This report was produced by Leandro Ucciferri, lawyer and researcher of the Privacy and Freedom of Expression Areas at ADC, with the collaboration of Valeria Milanes, Director of the Areas.

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.

Throughout this investigation, we published a series of briefing papers aimed at exploring various aspects of cybersecurity, with the ultimate goal of determining 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.[1]

In this document we will delve into the results obtained in various reports and provide information on the link between cybersecurity and the intelligence and surveillance system, which has expanded in Latin America in the last few years.

In the **second section** we will define the issue we encountered when we started to study and analyze the field of cybersecurity, establish the approach of the investigation and analyze two factors which influenced the development of cybersecurity policies at a global level. In the **third section**, we will explore what cybersecurity is through different concepts provided by different global players, their extent and implications. In the **fourth section**, we will analyze various documents that focus on the development of cybersecurity policies, as well as on the status of cybersecurity at a global level. In the **fifth section**, we will develop the legal evolution of cybersecurity in Argentina, analyzing the contexts in which the term is used, how said term is used and the extent of regulations. In the **sixth section** we will analyze the link between the intelligence system and cybersecurity. As a conclusion, we will include our comments, reflections and recommendations on the cybersecurity approach from a civil society and human rights perspective.

[1] The briefing papers can be consulted on the Privacy and Freedom of Expression Areas' website: https://adcdigital.org.ar/publicaciones/

II Cybersecurity: first approach

Before describing the current situation of cybersecurity in Argentina, it is crucial to understand what cybersecurity is.

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 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 contexts.

We were able to notice that, despite attempts to agree on Internet and technology related issues at an international level not being new, the cybersecurity debate seems to have deepened some issues, given that 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. The development of the concept of cybersecurity seems to be in full swing and a precise definition would mask the meaningful fact that the concept is in itself a matter of controversy among various views, perspectives and interests.

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

i Factors influencing its development

As will be analyzed throughout this report, the trends identified in international studies and the opinion of experts revolve around the treatment of cybersecurity as a necessarily interdisciplinary practice, which involves multiple aspects of society and the economy that are not related only to a military, defense or intelligence perspective. Yet, many countries have started their cybersecurity policy making processes with a strong link to cyberdefense, intelligence and surveillance.

In this respect, we identified two factors which we consider have become crucial to understand the context of cybersecurity policy making and the discourses adopted by certain countries in regards to this matter.

a 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, in late 2000, the average cost of 1 Gigabyte storage was USD 10; by 2005, the average cost had come down to USD 1. Ten years later, in late 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. Little by little, databases have turned into co-protagonists of the global economy, Internet development and state and business surveillance.

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"*, making a copy, as detailed as possible, of the digital life of the greatest amount of people in the world, just because some day it may be necessary to use it when people become a target or enemy.

b 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.[2]

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, which markets its products to NSA,[3] also present in Argentina;[4] Gamma International, an Anglo-German company known for its FinFisher software solution, also called FinSpy;

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

[3] Vaughan-Nichols, Steven J. "How the NSA, and your boss, can intercept and break SSL", June 2013. Available at: http://www.zdnet.com/article/how-the-nsa-and-your-boss-can-intercept-and-break-ssl/

[4] Blue Coat Argentina https://www.bluecoat.com/es/node/1316

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 as well as to *hacking* techniques and tools must be analyzed as a bidirectional issue. In this respect, government agencies and departments, as well as private corporations, are able to acquire this type of products without bureaucratic or legal barriers, even at prices that are far from being unreasonable. This situation also has an impact on relationships between "opposing" States (for example, USA – Russia or South Korea – North Korea) 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 faced by all the involved parties. In 2010, researchers discovered that the Iran nuclear-power plant had been the target of a malware[5] attack known as Stuxnet, which was later attributed to the United States and Israel.[6] Early in 2015, South Korea blamed North Korea for a nuclear-power plant hack in the country.[7] These are just two cases within a great number of reported attacks coming to light year after year, where we should also consider the private sector.[8]

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, whose potential violation or attack would directly affect the society and the economy.

[5] Malware is malicious software designed to secretly enter computers and cause damage to users or obtain an economic benefit from them.

[6] Zetter, Kim. "An Unprecedented Look at Stuxnet, The World's First Digital Weapon", Wired, November 2014. Available at: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[7] Kwaak, Jeyup S. "North Korea Blamed for Nuclear-Power Plant Hack", The Wall Street Journal, March 2015. Available at: http://www.wsj.com/articles/north-korea-blamed-for-nuclear-power-plant-hack-1426589324

[8] In this respect, please see report "Data Breach Investigations Reports" from Verizon, Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/

III Defining cybersecurity

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:

1. **Cybersecurity as the protection or defense of an organization's infrastructure (public or private), its networks, data and users;**
2. **The work performed by security forces on investigation, prevention and action against crimes in the digital field (cybercrime);**
3. **Surveillance activities conducted by intelligence agencies.**

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

Yet, international organizations have made progress on this matter 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,[9] later approved by Resolution 181,[10] 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

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

[10] ITU. Resolution 181. November 2010. Available at: https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

> 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" 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".[11] (emphasis is ours).

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 needs 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 under the Inter-American Committee against Terrorism (CICTE), designed –among other things- to help Member States to adopt national strategies of 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.

[11] OAS. IACHR. Freedom of Expression and Internet. December 31, 2013. Available at (PDF): https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

In the American continent, there are various countries that have already implemented national cybersecurity policies or they are working on them. Canada's[12] 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[13] 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 techniques of information security systems in order to fight cybercrime and maintain the cyberdefense of the country.

As can be seen, the term "cybersecurity" is used in a very flexible fashion. Without an international consensus, its definition will depend on whom is developing its policies. From the protection of information owned by the State and the private sector and the security services accessed by citizens online, to the investigation of cyber crimes and the development of cyberdefense and intelligence systems in the country, the extent of cybersecurity will depend on the context and the specific factors of whoever uses the term.

As mentioned in the previous section, the issues faced by certain countries call for measures that are often radically disputed among nations. In addition, in many countries, those who have control over the political agenda are a few officers currently in power, and many times the opportunity to discuss the best way to address cybersecurity in a truly democratic context is lost.

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

[13] UIT. National Strategies on Cybersecurity. France. Available at (PDF): http://goo.gl/ksfhou

i (De)militarizing ideas: cybersecurity alignment with human rights

Early in April 2016, a group of civil society organizations in Latin America jointly agreed to sign a declaration concerning ten fundamental topics which we understand must be promoted locally so that cybersecurity policies become aligned with a human rights perspective.[14]

Below we include some of the recommendations made in the declaration:

- Any cybersecurity strategy must be aligned with the human rights legislation of the country implementing them, of the inter-American system and international standards (in this respect, a sound example to be used as a guide is the International Principles on the Application of Human Rights to Communications Surveillance). It is essential to pay special attention to the protection of rights to freedom of expression, privacy and freedom of association, which –as we have been analyzing– may be easily violated if no consideration is given to the implications of the implementation and use of certain technologies or practices.

- Since the concept of cybersecurity stems from deep military roots, we recommend substituting it with the term digital security, which must have the protection of citizenship, individuals and communities at its core, while promoting economic and social development and respecting democratic institutions. This should limit the concept transcending a military, defense and intelligence scope.

- For the work done throughout the development and implementation of digital security policies to be effective, we must encourage governments to pay special attention to the use of products complying with recognized standards of digital security; otherwise, it could leave the door open to potential violations and risks that may jeopardize digital security policies and strategies.

[14] ADC Digital, "OAS: Civil Society Joint Declaration on Digital Security Issues in Latin America", April 2016. Available at: https://adcdigital.org.ar/2016/04/06/oea-declaracion-sociedad-civil-latinoamericana-seguridad-digital/

IV International trends in cybersecurity policy making and their adaptation to the Latin American context

When looking for references of international organizations studying cybersecurity within a context of public policies and their social impact, we found a scarce amount of cases we would be able to analyze and translate into the foregoing report.

On the one hand, we chose a study developed by the Organization for Economic Cooperation and Development (OECD) which analyzes various national cybersecurity strategies from the point of view of the Internet economy. The OECD is a forum where member countries can share experiences on policies and look for solutions to common issues. Even though Argentina is not part of the OCDE, this report is a good overview of the reality of different countries, especially from North America and Europe, and of how said countries face the cybersecurity matter, how it is included in public policies and what issues it must focus on. Another reason why we chose this report is the incorporation of the perspective, analysis and recommendations of non-governmental players who are members of the OECD.

On the other hand, moving onto the Latin American context, we explain some aspects of the situation Colombia is experiencing in its cybersecurity policy making, as it became the first country in Latin America to adopt a national strategy through the document Conpes 3701 dated July 2011, referred to as "Policy Guidelines for Cybersecurity and Cyberdefense", apart from the observations made by a group of experts summoned by OAS at the request of the Government of Colombia in order to analyze the case of the country and make recommendations based on it for the implementation and development of the strategy.

Finally, we conclude this chapter with two reports by OAS related to the situation Latin American countries are going through in the development of cybersecurity strategies and policies, where we will highlight the remarks made on the Argentine case.

i A new generation of national cybersecurity strategies for the Internet economy

In late 2012, the Organization for Economic Cooperation and Development (OCED) published the report "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy",[15] which analyzes cybersecurity policies in ten countries–Australia, Canada, France, Germany, Japan, the Netherlands, United Kingdom, United States, Finland and Spain– thereby identifying differences and commonalities, and comparing the characteristics of the various action plans implemented by governments, while making public certain trends in cybersecurity policy making, apart from underscoring recommendations from other non-governmental players, such as the Internet technical community, the private sector and civil society; in the following section we will develop some of the most relevant discoveries, trends and recommendations of this report.

Cybersecurity has been expanding within governments' priorities, which have determined that, on the one hand, the Internet and ICT are essential for the economic and social development and that they constitute a vital infrastructure for innovation, social well-being and individual expression, but, while the Internet economy develops, the economy and the entire society grow ever more dependent on this infrastructure for the development of their activities. On the other hand, threats on the Internet are evolving and increasing at a fast pace and fostered not only by individual criminals, but also by foreign states and political groups who engage in hacktivism, cyber spying, sabotage and even military operations.

For this reason, practically all the cybersecurity practices analyzed show an evolution in the approach of the matter, going from strategies which only protect individuals and private organizations, to those protecting society as a whole.

As the Internet has become essential for the full development of the economy and the society, the consequences of failures can directly impact society as a whole.

[15] Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OCDE, 2012. Available at: http://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm

Therefore, cybersecurity strategies focus on two main objectives: "strengthening cybersecurity for the Internet economy to further drive economic and social prosperity, and protecting cyberspace-reliant societies against cyberthreats."

The criticality of the Internet for the modern economy has several consequences on cybersecurity policy making, the main one being the adoption of strategies that approach cybersecurity in an integrated and comprehensive manner. Governments recognize the need to address all the facets of cybersecurity holistically, encompassing the social, educational, legal, economic, technical, diplomatic, military and intelligence aspects, as well as those related to security forces. According to the OECD, this type of approach must be supported by strong leadership, sometimes at head of State or head of government level.

Not all strategies use the terms "cybersecurity" and "cyberspace". Yet, the OECD states that some strategies which do use these terms also provide a definition which varies across countries as it changes based on the aspects of the policies they expect to adopt.

On the other hand, there are some concepts shared by the strategies of different countries, for example:

- Enhanced governmental co-ordination at policy and operational levels: No single agency can claim a comprehensive or global understanding and a sufficiently wide authority to manage all facets of cybersecurity. Thus, co-ordination among the relevant bodies becomes essential. Strategies clearly assign the responsibilities of each one of them to encourage proactiveness and avoid duplication.

- Reinforced public-private co-operation: All strategies recognize that the Internet is largely owned and operated by the private sector. In this respect, they acknowledge that policies must be based on inclusive or multidisciplinary public-private partnerships, which may include the participation of civil society, businesses, the technical community, and academia.

- Improved international co-operation: Most strategies share as key objectives the need for better international alliances with like-minded countries or allies, including organizations such as the Council of Europe, the European Union, the G8, the Internet Governance Forum, the OECD and the United Nations (including the Telecommunications International Union), but, overall, provide little detail on the role they expect such alliances to play. The OECD states that various countries mention the North Atlantic Treaty Organization (NATO) regarding cybersecurity in a military context.

- Respect for fundamental values: All strategies place a strong emphasis on the need for cybersecurity policy to respect fundamental values, which generally include privacy, freedom of speech, and the free flow of information. They also explicitly highlight the need to maintain the openness and freedom that characterize the Internet.

One of the most relevant trends found by the OECD is that *most cybersecurity strategies began to focus particularly on sovereignty considerations, including military, national security, intelligence and defense aspects* when developing their policies.

The OECD states that this evolution is a direct consequence of the consideration that cybersecurity addresses the protection of the society as a whole, which leads governments to put into practice an integrated approach.

Sovereignty considerations emerge at different levels of the national policy. In this respect, the OECD gives some examples based on the policies studied:

- At the strategic level: it entails the recognition of cyber attacks targeting the military and the infrastructure of the state, or the risk of cyberespionage from foreign states.

- At the organizational level: various departments and ministries in charge of intelligence and military activities were included in the governmental coordination for cybersecurity policy making.

- At the operational level: intelligence bodies begin to take on a key role as they become the source of information for situational awareness.

On the other hand, the OECD found that most strategies entail action plans aimed to strengthen certain areas identified by the government that need working on in order to develop a robust cybersecurity infrastructure. The OECD determined that, generally, these are the areas:

- Government security: regarding the infrastructure used at a state level.
- Protection of critical information infrastructures.
- Fight against cybercrime.
- Awareness raising: intended to develop initiatives targeted at society's vulnerable sectors, for example, children and adolescents.
- Education: action plans recognize the need for a stronger cybersecurity workforce. The development of cybersecurity skills is identified as a key priority.
- Response: strategies recognize the key role played by Computer Security Incident Response Teams (CSIRTs), and create a national CSIRT or strengthen it where it already exists through the action plan.

Finally, the OECD includes some recommendations in the report provided by non-governmental stakeholders (participants: Business and Industry Advisory Committee (BIAC), Civil Society Internet Society Advisory Council (CSISAC) and Internet Technical Advisory Committee (ITAC)). Generally, they agree that the collaboration of multiple interested parties (known as multistakeholder model) and cooperation are the best means to develop effective cybersecurity policies that respect the fundamentally global and open nature of the Internet; on the other hand, cybersecurity policies must be flexible enough to accommodate the dynamic nature of the Internet.

It is worth mentioning some of the suggestions made by the civil society when consulted by the OECD, mainly:

- To prevent certain measures adopted in the cybersecurity strategy from becoming illegal or threatening towards fundamental rights as technology and practices evolve, sunset clauses can be used to automatically stop them, acting as control mechanisms of citizens' rights.

- Governments should take on a more active role leading by example, by adopting best practices and technologies that respect not only digital security international standards, but mainly the fundamental rights of individuals. This role will allow governments to provide a clear direction to other actors who depend on the cybersecurity strategy.
- It is essential that those in charge of cybersecurity policy making seek advice from the Internet technical community as early as possible in the policy making process to avoid pursuing technologically and operationally flawed decisions that may jeopardize, for example, the very nature of the Internet.
- Cybersecurity policies could encourage the development of open standards enabling innovation for security solutions, relying on respected and open standardization groups and avoiding unilateral modification of Internet standards.

ii Colombia: pioneer in Latin America

Even though the report published by the OECD addresses the analysis of various countries in Europe and North America, at an institutional level, their reality does not necessarily coincide with the Latin American context, characterized by its vulnerability. For example, in the case of Argentina and especially in relation to cybersecurity, when analyzing how and when certain public policies were adopted, we may infer these were a response to a fashion trend rather than a real need previously analyzed, agreed upon and committed to developing a public policy regarding cybersecurity. When analyzing the background of cybersecurity policies and practices at a national level, we noticed their budget was not enough to reach the goals defined or to comply with the structure established by regulations and they were not conceived of as long-term State policies. We will go back to this topic.

On the other hand, a great number of Latin American countries have had military dictatorships with an authoritarian past, or even in democracy they have a military culture and presence rooted in their institutions, from the State's way of working to the training of officers and employees. This context cannot be overlooked when making an incursion in public policy making, whose approach has evolved towards respect for fundamental rights and democratic institutions.

A case in point is the one unfolding in Colombia, where in 2011 the document "Policy Guidelines for Cybersecurity and Defense"[16] issued by the National Council of Economic and Social Policy (CONPES, for its acronym in Spanish) created an Inter-Sectorial Commission in order to establish a cybersecurity policy. "Even though all its composition, except for the Ministry of Information Technology and Communications and National Planning, is connected to the defense sector, it is remarkable that the Director General of the Intelligence National Directorate is part of the commission. Nothing in the CONPES document explains the presence of this officer", states Juan Diego Castañeda, lawyer at Karisma Foundation.[17]

"Cybersecurity policies and institutions closely revolving around the Ministry of Defense seems to have been decided prior to the creation of CONPES, as the very same document, following the meetings of 2008 and 2009 with the OAS, especially its Inter-American Committee against Terrorism (CICTE), affirms that 'State institutions requested the Ministry of National Defense to adopt a national leadership that will allow promoting cybersecurity policies. (. . .) The final diagnosis showed that the Ministry of Defense had greater capacity for handling these matters in an efficient and coordinated way.' (CONPES 2011) There are no other explanations in this document", adds Castañeda.

In April 2014, the Organization of American States created a commission of experts to evaluate the status of cybersecurity in response to a request by the Government of Colombia. The Council of Europe, the World Economic Forum, INTERPOL, United Nations, the OECD and the University of Oxford participated

[16] CONPES 3701, National Council of Economic and Social Policy, Republic of Colombia, 2011. Available at: http://mintic.gov.co/portal/604/articles-3510_documento.pdf

[17] Interview with Juan Diego Castañeda, lawyer and researcher at Karisma Foundation (https://karisma.org.co). March 2016.

in this commission and they issued the document "Cybersecurity Technical Assistance Mission: Conclusions and Recommendations."[18] Said document focuses on the specific point of view of Colombia, but it helps to better understand the OAS' position regarding some of the topics we have mentioned; we include some of them below.

The OAS establishes that the cybersecurity strategy must have a "global vision", which must define broad goals that explain why the nation should pursue them and distinguish between economic and social prosperity goals; defense of the country (military, intelligence-related, etc); and the fight against cybercrime.

The cybersecurity institutional framework should establish a permanent coordination body with an overarching government-wide role; this body should report directly to the President. The coordination body must have the "statutory responsibility and authority to act", including budgetary resources to deliver the global vision of cybersecurity; "the responsibility for leading public policy making to ensure a coherent whole of government approach"; as well as the "capacity to develop a comprehensive national cybersecurity risk assessment." The coordinating body "should be a repository for best cyber security practices (. . .) including guidance and advice on standards, and frameworks for accreditation, and certification."

On the other hand, the OAS establishes the integrated link with all interested parties as a fundamental part for policy making, "it is essential to engage all stakeholders (public and private) in the development of the vision, policies and their implementation to maximize its commitment". In this respect, all parties must be consulted (civil society, technical community, private sector, academia, international entities) on how to organize the systematic dialogue among themselves, establish systematic consultation standards both in the initial phase as well as throughout policy making, and develop a short, middle and long-term plan to progressively reach all governmental and nongovernmental players.

The OAS recommends that issues pertaining to the prosecution of cybercrime

[18] Cybersecurity Technical Assistance Mission, Organization of American States, April 2014. Available at: http://www.oas.org/documents/spa/press/Recomendaciones_COLOMBIA_SPA.pdf

must be adequately removed from the issues of cyber defense and cyber war, "defining the police unit that will take care specifically of the prevention, investigation and prosecution of cyber crime."

The OAS establishes that special consideration needs to be given to the small and medium enterprises and sectors with few financial resources to develop cybersecurity capabilities, which can be helped through, for example, tax incentives or grants.

Finally, given that cybersecurity necessarily involves multiple stakeholders, effective work in this area "requires deep and sustained cooperation with the private sector (national and international) as well as foreign governments, international organizations, and academic experts."

"At least in these recommendations, the OAS does not seem to point out the need to separate cybersecurity from the Ministry of Defense. It only notes that an independent coordinating body is needed. In intelligence, it recommends separating economic and social objectives, as well as objectives related to defense and the fight against crime," comments Castañeda.

Castañeda adds "As for the changes we are worried about with respect to cybersecurity, we can mention:

- The expansion of military, intelligence and police powers, without the expansion and improvement of controls;
- The expansion of Internet data retention;
- The use of hacking tools to access devices, without any debate or control;
- The expansion of powers, techniques of communication interception and monitoring of spectrum;
- Encryption regulation;
- The use of large budgets whose priorities oppose the need to keep updated and resilient computer systems, and trainings not including views different than the military."

In the report "Freedom of Expression and the Internet", the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights 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 54). In this respect, "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 56).

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 56). "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 57).

iii Cybersecurity in the Latin American context according to the OAS

As we have been explaining, the OAS was a pioneer organization in addressing cybersecurity from a regional framework –due to its nature–; given the importance of this organization for the countries of the continent, we consider it is worth mentioning in this report two of its most recent works: "Report on Cybersecurity and Critical Infrastructure in the Americas" and "Cybersecurity: Are we Ready in Latin America and the Caribbean?"

The first report, "Report on Cybersecurity and Critical Infrastructure in the Americas", done jointly with Trend Micro, is a study that was conducted based on a survey made to governmental entities and key industries such as communications, banking and finance, manufacturing, energy and security, of over 20 OAS Member States, in order to provide a view into the actual state of cybersecurity around critical infrastructure in the region and the threat trends crucial organizations face, as well as organizations' cybersecurity measures and policies, collaboration with local governments; and their preparedness for cyber attacks

Some of the conclusions of the report showed that:

- Attacks against infrastructure are a clear and present danger. Only a small percentage of respondents said they had not seen this type of attacks. On the other hand, they claimed threats are becoming more severe, the frequency of attacks is growing and they are becoming more sophisticated. According to some respondents, the outlook is discouraging when it comes to the protection of critical infrastructure.

- There is a lack of a proactive partnership between governments and private organizations in the region. A stark majority of respondents reported either no dialogue or only informal dialogues between these key partners.

- Budgets managed by organizations constitute an impediment when needing resources to continually defend attacks against their infrastructures.

- The lack of funding and an unmet desire for government leadership focused on cybersecurity leave infrastructure defenders feeling increasingly left on their own. The OAS establishes that governments in the region need to take the outstretched hands of those in critical infrastructure looking for help and lead them to help better protect against increasing attacks against this crucial sector

The second report, "Cybersecurity: Are we Ready in Latin America and the Caribbean?" done by the Cybersecurity Observatory in Latin America and the Caribbean in partnership with the Inter-American Development Bank (IDB) and the OAS, seeks to provide a complete and up to date overview on the status of cybersecurity in the region through the collection of data from different actors such as: governmental agencies, critical infrastructure operators, military forces, the police, the private sector, the civil society and academia. The report comprises two sections: the first section consists of various essays contributed by experts specialized in trends in the region; the second part comprises the report of the various countries analyzed, providing an overview of the current state of cybersecurity in said countries.

The reflections the IDB arrived at show the trends that have started to emerge in the region:

- Even though governments recognize the importance of providing affordable access to information communications technology (ICT) and the Internet for business innovation, growth, and a greater development in the delivery of public services, Internet penetration is still quite low in around half of the region.
- Adopting a national cybersecurity strategy is arguably one of the most important elements of a country's commitment to securing the cyber infrastructure, services and ICT business environment upon which its digital future and economic wellbeing depend. The countries that have formally adopted cybersecurity strategies are Brazil, Colombia, Jamaica, Panama, Trinidad and Tobago, and Uruguay.
- Society is largely unaware of the risks and vulnerabilities associated with the use of ICT. The IDB highlights it is important for governments to describe the risks and opportunities associated with increasing connectivity and dependence on the Internet.
- Even though most national authorities maintain open and active lines of communication and collaboration with critical sectors and key enterprises, there is mistrust among stakeholders which has diminished collaboration.
- Crisis response or reporting mechanisms are in nascent stages across the region and there is limited capacity to proactively address cyber threats. About half of the countries in the region have established and operationalized Computer Security Incident Response Teams (also referred to as CERT).
- Efforts to develop comprehensive legal frameworks to fight cybercrime are underway across the region.

- Some governments are taking advantage of their increased Internet connectivity to explore technology development opportunities, expand their internal technology industry and launch cyber research and development programs.

In the last part of the following section, we will delve into the specific analysis carried out by Trend and IDB on Argentina's situation in order to compare it with what we have been able to observe based on the investigation for this document.

V Looking for a cybersecurity agenda in Argentina

The first steps made in this investigation showed that the term "cybersecurity" appears in some regulation, frequently used in the last years, but no type of definition or concept of cybersecurity is given.

In order to clearly understand Argentina's specific situation, it is necessary to describe the legal evolution under which the topic was brought to the public agenda.

i Emergency Response Team on Telecomputing Networks of the Argentine Public Administration (ArCERT, for its acronym in Spanish)

The Team was created in 1999 through Resolution No 81/99 within the former Secretariat of Public Administration, dependent on the Presidency of the Cabinet of Ministers, and was empowered to establish the policies for computing technologies, telecomputing or telematics, multimedia and telecommunications associated to computing for the National Public Sector.[19]

According to the Resolution, the National State had made considerable steps towards including computing and communications technologies in its organisms,

[19] Resolution No. 81/1999. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/55000-59999/58799/norma.htm

as well as their interconnection and network development, resulting in an increase of the information being transmitted through the National Public Administration networks, apart from an increase in the complexity of the interconnectivity among networks, which largely resulted from the use of the Internet. Hence, it was necessary to provide the National Public Administration with a technical service in order to address any issues occurring in its networks.

In this way, some of the ArCERT's objectives were: to promote coordination among administration units of computer networks for the prevention, detection, management and collection of information on safety incidents; propose regulations; provide technical assistance for safety incidents in computer systems; centralize reports on safety incidents; serve as repository for all information on safety incidents, tools, defense and protection techniques, etc.

The ArCERT then became part of the Critical Information Infrastructure and Cybersecurity program.

ii Program of Critical Information Infrastructures and Cybersecurity (ICIC, for its acronym in Spanish)

The ICIC[20] is created in 2011 through Resolution No 580/11 of the Presidency of Cabinet of Ministers.[21]

The reasons for creating this program are outlined in the Resolution's recitals, which, among others, highlight that the digital infrastructure virtual communications depend on for their use is a critical infrastructure and, thus, essential for the operation of information and communication systems, which in turn inexorably depend on the National Public Sector and the private sector.

The resolution also stresses that the safety of the digital infrastructure is exposed to constant threats whose materialization may cause serious incidents in information and communication systems; hence, it is essential to adopt the necessary

[20] Official website: http://www.icic.gob.ar

[21] Resolution No. 580/2011. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

measures in order to guarantee the effective operation of critical infrastructures. For that reason, it is important to create and adopt a specific regulatory framework that allows identifying and protecting strategic and critical infrastructures of the National Public Sector, interjurisdictional agencies and civil and private sector organizations that so require, and guaranteeing the collaboration of these sectors with a view to developing the adequate strategies and structures for a coordinated response towards the implementation of relevant technologies, among other actions.

This resulted in the creation of the ICIC, whose general purpose is to elaborate a specific regulatory framework that allows identifying and protecting strategic and critical infrastructures of all entities and jurisdictions of the national public sector, interjurisdictional agencies and civil and private sectors organizations that so require, as well as promoting the cooperation and collaboration of these sectors with a view to developing the adequate strategies and structures for a coordinated response towards the implementation of relevant technologies.

To that effect, the ICIC shall elaborate and propose regulations; collaborate with the private sector; manage information on safety incidents reporting in the National Public Sector and provide possible solutions in an organized and unified way; establish priorities and strategic plans in order to lead the cybersecurity approach; warn about identification cases of attempts to violate critical infrastructures; coordinate the implementation of response exercises; provide technical assistance for reported safety incidents; centralize reports; serve as repository; elaborate an annual report regarding the state of cybersecurity so that it can be published in an open and transparent way; monitor the services provided by the National Public Sector through the Internet and those identified as critical infrastructure for the prevention of potential cybersecurity failures; raise awareness about the risks posed by the use of digital media; disseminate useful information in order to increase the safety levels of networks, among others.

It is worth mentioning that, in order to participate in the Program, interested agencies, whether from the National Public Sector, interjurisdictional agencies or civil society and private sector organizations, must announce their intention to adhere to the program.

Likewise, the Resolution sets forth that the ICIC shall refrain from intercepting or inspecting private Internet or network connections under the provisions established by the Personal Data Protection Law and regulatory laws in force.

The ICIC has four group works:

1. ICIC CERT: designed to handle computing emergencies;
2. Preventive Action Group (GAP, for its acronym in Spanish), designed to research and analyze new technologies and computing tools;
3. Critical Information Infrastructure Group (GICI, for its acronym in Spanish), designed to identify and analyze the country's critical infrastructures, such as telecommunications, energy, oil, gas and financial services;
4. Healthy Internet, designed to raise awareness about the risks posed by the use of digital media in the National Public Sector.

Through the National Institute of the Public Administration (INAP, for its acronym in Spanish), the ICIC provides courses, workshops and conferences that are focused on the training strategy designed by the National Office of Information Technologies (ONTI, for its acronym in Spanish). In July 2014, for example, there was a training called "Introduction to Critical Information Infrastructures and Cybersecurity", conducted online and also via distance learning and targeted at agents responsible for administrative duties in entities and jurisdictions that are part of the National Public Sector, as well as personnel of interjurisdictional and civil organizations and of the private sector.

The training was divided into three modules which addressed the theoretical grounds on the subject (What are critical infrastructures? What is cybersecurity?) and analyzed specific cases of the European Union Agency for Network and Information Security (ENISA), as well as the national cybersecurity strategies of the United Kingdom, Canada, Spain, the United States and Germany.

When the ICIC was created, the enforcement authority of the ICIC program was the National Office for Information Technologies (ONTI),[22] which depends on the

[22] Official website: https://www.argentina.gob.ar/modernizacion/ONTI

Undersecretariat of Technology Management of the Cabinet Secretariat within the Presidency of Cabinet of Ministers.

ONTI is responsible for implementing innovative computing strategies for the Public Administration; developing systems that are used for management procedures; establishing the standards that must be used by public agencies when new technologies are incorporated; collaborating with other departments in order to create information and management portals; promoting the interoperability of information networks for state institutions. It also coordinates responses arising from attempted attacks and infringement of public agencies' computing networks; establishes security standards and ensures these are complied with by State systems; and implements and controls the use of the State's digital certification, which allows processing records electronically.

iii Undersecretariat of Critical Information Infrastructure and Cybersecurity Protection

The ICIC program led the National Executive Power to order in June 2015 the creation of the Undersecretariat of Critical Information Infrastructure and Cybersecurity Protection, which depends on the Cabinet Secretariat of the Presidency of the Cabinet of Ministers, whose main purpose is to implement the national strategy for the protection of critical information infrastructures and cybersecurity.

Decree 1067/2015 by the National Executive Power established the abovementioned, based on the improvement of the use of public resources with a view to substantially improving citizens' quality of life, focusing its actions on results which are collectively shared and socially valued.

To that effect, it decided to establish a new organizational structure of political levels, based on rationality and efficiency criteria which may allow a quicker response for society's demands, resulting in dynamic structures and adaptable to constant change.

This decree established that the ICIC Program should depend on the National

Department for Critical Information Infrastructures and Cybersecurity, which was created under the scope of the new Undersecretariat of Critical Information Infrastructures and Cybersecurity Protection.

It was then decided that the main responsibility of the Undersecretariat would be to handle all aspects regarding cybersecurity and the protection of critical infrastructures, including capacity building for detection, defense, response and recovery when faced with incidents of the National Public Sector.

To that effect, the Undersecretariat must undertake similar actions to those established for the ICIC Program, such as –and just to name a few:

- Handling, assisting with and supervising all aspects connected with the security and privacy of digitalized and electronic information;
- Establishing regulations and standards designed to increase efforts in order to raise the security thresholds in the resources and systems related to computing technologies;
- Defining the Sample Information Security Policy;
- Collaborating with the private sector in order to establish protection policies for digital security with regular updates;
- Establishing priorities and strategic plans in order to lead the cybersecurity approach, ensuring the latest technological advances are implemented for the protection of critical infrastructures.

In addition, Resolution 1046/2015 of the Presidency of the Cabinet of Ministers[23] created three departments and two divisions that depend on the National Department for Critical Information Infrastructures and Cybersecurity. Each one of them is responsible for the following actions:

1. Department of Regulatory Elaboration and Interpretation;

[23] Resolution No. 1046/2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/250000-254999/251022/norma.htm

2. Technical Department for Critical Information Infrastructures and Cybersecurity;
3. Department of Training, Awareness-Raising and Dissemination;
4. Process and Project Division; Development and Research Division.

iv The New National Intelligence Doctrine and the Cybersecurity Intelligence Operations Department

On July 6, 2015, after the Intelligence Law reform (Law 27.126), Decree 1311/15[24] came into effect, which created the New National Intelligence Doctrine as a doctrinaire body, the organic and functional structure of the new organism and a new professional regime for the personnel of the Federal Intelligence Agency (AFI in Spanish).

When developing the framework for the “Intelligence for the Democratic Defense and Security”, Chapter I in Annex I establishes that the national intelligence is an activity included within the scope of the social and democratic Constitutional State of law that is designed to produce knowledge of any issues –risks and conflicts– involving the national defense and homeland security. The deviation in the purposes of the Argentine intelligence system made it necessary to clarify that the national intelligence must guarantee the protection and good care of Argentine citizens instead of “spying on them”. Hence, the national intelligence system is organized as an “observatory” that focuses exclusively on the production and management of knowledge regarding the relevant issues on national defense and homeland security.

When defining the issues within the scope of Homeland Security, it establishes that these issues include criminal phenomena that violate citizens’ rights and liberties as well as the social and democratic Constitutional State of law and particularly those relevant criminal phenomena of federal nature.

Then it defines the complex criminal phenomena of federal nature:

[24] Decree No. 1311/2015. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

1. Terrorism and its various global and/or local, state and non-state manifestations;
2. Terrorist attacks against the constitutional order and democratic life, involving political and/or military groups or economic and/or financial groups;
3. Organized crime, particularly drug trafficking, human trafficking, economic and financial crime, arms trafficking, etc.;
4. *Any actions against cybersecurity*, crimes against confidentiality, integrity and availability of computing systems, networks or data, or a part of them, fraudulent use and illegal dissemination of contents. (emphasis is ours)

Chapter II in the New Doctrine, under "Extent and Activities of National Intelligence" (Annex I) establishes the extent of the national intelligence production, which includes:

- Strategic national intelligence
- Counterintelligence
- Criminal intelligence
- Strategic military intelligence

Among these four areas, cybersecurity is mentioned in the development of criminal intelligence. It establishes that criminal intelligence "includes production of intelligence regarding criminal issues and, particularly, those complex criminal issues of federal nature related to terrorism, terrorist attacks against the constitutional order and democratic life, organized crime and terrorist attacks against cybersecurity."

The Executive Power issued Decree 656/16 to repeal Annexes II to VII of Decree 1311/11, that is, those related to the Organic and Operating Structure of the Federal Intelligence Agency (AFI, in Spanish), its Organizational Structure, the Professional Regimes of Intelligence, Security and Support Hierarchies, and the Funds Administration Regime of the AFI.

Even though said annexes were eliminated, it is worth mentioning part of Annex II, where the term cybersecurity appears, as said annex shows how this topic would be approached within the intelligence system.

Annex II of Decree 1311/15 included a description of the "Organic and Functional Structure of the Federal Intelligence Agency". In Section II, Chapter 4 described the operational structure of AFI's intelligence, which included the detailed functions and composition of the Cybersecurity Intelligence Operations Department, located in AFI's headquarters, at 25 de Mayo street, No 11, in the City of Buenos Aires.

The Cybersecurity Intelligence Operations Department was "responsible for producing intelligence in order to gain awareness of the actions taken against cybersecurity within the framework of national defense or homeland security, and of the national or foreign groups that are responsible for performing them."

The Operations Department is composed of two additional departments:

Department of Computing Intelligence: which is responsible for producing intelligence in order to gain awareness of activities regarding risks and conflicts connected with or resulting from the use of information and communications technologies that may affect the national defense or homeland security, and of the national or foreign groups that are responsible for performing these activities.

Department of Cybercrime Intelligence: which is responsible for producing intelligence in order to gain awareness of the activities that may constitute a cyber crime in any form or kind, and of the national or foreign groups that are responsible for performing these activities.

Annex II established that the Cybersecurity Intelligence Operations Department "develops institutional activities of collection, management and information analysis and consists of intelligence officers and analysts who are experts in cybersecurity."

In addition, Decree 656/16 empowers the new AFI Director to approve its own organic structure and to establish complementary and explanatory rules. One of the main problems that could result from this is the creation of a new organic structure in a secret way, which would be a step backwards in the democratization process of the intelligence system, since not even the internal composition of the organism would be known.

v Undersecretariat of Technology and Cybersecurity

After the change of government and the arrival of new State authorities following the national elections in late 2015, the Executive Power took a series of measures designed to reorganize the structure of various ministries, based on the structure it had defined for the City of Buenos Aires.

One of these changes came into being under Decree 13/16, which came into effect on January 5, 2016. The Decree created the Ministry of Modernization within the sphere of the National Public Sector, which modified the organization chart we had been describing until then.[25]

The Ministry of Modernization has four secretaries: Secretariat of Public Employment, Digital Country Secretariat, Secretariat of Public Management and Innovation, and Secretariat of Administrative Modernization, each one having the corresponding undersecretariats. On the other hand, it has four undersecretariats which depend directly on the Minister: Undersecretariat of Administrative Coordination, Undersecretariat of Labor Relations and Civil Service Reinforcement, Undersecretariat of Technology and Cybersecurity, and Undersecretariat of Telecommunications and Public Networks.

For the purposes of this document, we will then focus on the Undersecretariat of Technology and Cybersecurity. This undersecretariat now encompasses a great part of the various divisions we have been describing in this section, and, hence, it is the central pillar of cybersecurity in Argentina.

The Undersecretariat of Technology and Cybersecurity is responsible for:[26]

[25] Decree No. 13/2016. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257556/texact.htm

[26] Administrative Decision 232/2016, Ministry of Modernization. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259845/norma.htm

1. **National Office for Information Technologies** (ONTI, in Spanish): whose main purpose is to handle policy making and the implementation of the development process and technology innovation for the transformation and modernization of the State, promoting the integration of new technologies, their compatibility and interoperability based on the objectives and strategies defined in the State's Modernization Plan.[27]

2. **National Department of Technological Infrastructure and Operations**: It is responsible for handling aspects related to the development and maintenance of the technological infrastructure, as well as to the administration and computer processing of critical systems and data under the National Public Administration.

3. **National Department for Critical Information Infrastructure and Cybersecurity**: It is responsible for handling all aspects related to cybersecurity and the protection of critical infrastructures, including capacity building for the detection, defense, response and recovery when faced with incidents of the National Public Sector.

In this way, the organization chart of divisions in charge of national cybersecurity under the Presidency of the Cabinet of Ministers is transferred to the Undersecretariat under the Ministry of Modernization.

Decree 13/16 assigns objectives to the Undersecretariat, which include, among others:

- Assist in the development of a national strategy for technological Infrastructure, protection of critical information infrastructures and cybersecurity at a national level.

- Lead and manage data and computer centers in order to provide key infrastructure services to other jurisdictions, maximizing the use of resources, improving security and the quality levels of the services provided.

[27] State's Modernization Plan, Ministry of Modernization. Decree 434/2016, March 2016. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259082/norma.htm

- Assist in establishing rules, policies, standards and procedures of Computing Technology and Security within its scope of competence.
- Assist the Ministry in designing a specific legal framework that provides for the identification and protection of critical infrastructures of the National Public Sector, civil organizations, private sector and the academic field that so require, and promoting cooperation and collaboration among said sectors.
- Assist the computing emergency response team at a national level (National CERT).
- Lead and supervise the National Office for Information Technologies (ONTI).

vi Cyberdefense Undersecretariat

On January 7, 2016, Decree 42/16 establishes the Cyberdefense Undersecretariat within the sphere of the Secretariat of Science, Technology and Production for the Defense, under the Ministry of Defense.[28] The Decree sets forth the following objectives for the Secretariat of Science, Technology and Production for the Defense:

- Assist in the development, approval and supervision of compliance policies and programs of investigation and development agencies from the Cyberdefense sector.
- Assist in the coordination and leadership of science and technology agencies from the field of Cyberdefense.
- Assist in the promotion of technical training exchanges related to Cyberdefense at an extra-jurisdictional level.

On the other hand, the Undersecretariat of Cyberdefense is mainly responsible for (emphasis is ours):

[28] Decree No. 42/2016. Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm

- Assisting the Secretary of Science, Technology and Production for the Defense in planning, designing and developing cyberdefense policies according to the provisions set forth in the National Defense Planning Cycle in coordination with the Undersecretariat of Strategic Planning and Military Policy.

- Assisting in the *coordination with organisms and authorities from the different State Powers to contribute from the Jurisdiction to the national cybersecurity policy and protection of critical infrastructure*.

- Exercising operations control over the Joint Command of Cyberdefense,[29] from the Joint Chiefs of Staff of the Armed Forces.

- Assisting in the development of policies, rules and procedures designed to guarantee information security and coordinate and integrate response centers when facing emergencies in teleinformatics.

vii From rules to practice: real situation status of cybersecurity in Argentina

So far we have analyzed what the main rules establish directly or indirectly in connection with cybersecurity in the country. Throughout this investigation and the different expert sources interviewed in the process, we were able to understand how these rules operated in real life, what was achieved and what not, how effective they were and what should have been planned differently.

“Although I consider the Missions and Functions of the [ICIC] program are appropriate, I think their execution has been deficient”, says the expert Mariano del Río,[30] “To date, we don’t have a catalogue for critical infrastructures, nor a cybersecurity national strategy. We have had numerous events though. Regarding

[29] Official website: http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx

[30] Interview with Mariano M. del Rio, April 2016. He is a specialist in Cybersecurity, Compliance and Privacy with more than 10 years’ experience in the implementation of Information Security Programs and compliance of the main rules and regulations on the subject in different industries. He funded SecureTech, an Argentine company of cybersecurity services and compliance.

the impact of the program on public policies, I think that, given the lack of an integrated vision on cybersecurity, which generally is achieved through a national cybersecurity strategy, I don't see other State divisions being influenced by said program."

With the available and verifiable public information that can be accessed, if we carefully read the objectives assigned to ICIC, the first conclusion we arrive at is that a great percentage of said objectives was partially or never achieved. Throughout the investigation work we tried many times, and to no avail, to contact officers in charge of different State divisions who are responsible for cybersecurity in the country in order to obtain more detailed information on the status of the situation.

As asserted by the expert Iván Arce,[31] one of the main problems was that "ICIC was given a number of responsibilities and functions which are immense, not only for its structure, but also for its institutional design. It remains unclear what they wanted to do, what their policies and objectives were. They did succeed in making a sample policy of computer safety, which is an adaptation of ISO 27001 for all State agencies to adopt. Its adoption is optional, as was the case with the ICIC program, which also was optional. [The rules] established a series of things that were interesting on paper, but whose execution has not been good in practice –as far as I know."

"The efforts made in the last few years are, from an institutional viewpoint, a step towards the right direction, but it remains to consolidate that in a national strategy, fill the conceptual gaps, determine and add what is missing. [Cybersecurity] does not only have to do with security, defense and intelligence; it's much more than that, such as the economic, social and commercial aspects. Regula-

[31] Interview with Iván Arce, May 2016. He is Director of ICT Security Program (STIC) of Dr. Manuel Sadosky Foundation, a nonprofit public-private organization dedicated to promoting and strengthening in all matters relating to Information Technology and Comunication Technologies (ICT) the link between the scientific and technological system and the productive sector of Argentina. Between 1996 and 2012 he held multiple roles in Core Security Technologies, a company he founded with 4 friends in Buenos Aires. He is a founding member of the Center for Secure Design of the IEEE Computer Society, editor of the journal IEEE Security and Privacy for the period 2002-2015 and frequent speaker at IT security conferences and events.

tory and technological development matters are also lacking, as well as having a sustainable cybersecurity environment. We need to think about it in a holistic way," concludes Arce.

For Dr. Hugo Scolnik,[32] "It is essential to have a unified center that coordinates all decentralized agencies responsible for the different State divisions. There must be an exchange of experiences among the officers and employees of the various departments; all ministries should be coordinated."

The experts surveyed agree that the Presidency of the Cabinet was the adequate place for the cybersecurity matter, mainly because it would allow reaching all State divisions more effectively and there is a direct link with the Presidency; this is fundamental given the holistic and transversal approach that cybersecurity policy making must have.

The transition to the Ministry of Modernization, made in late 2015, can be decisive for the effective implementation of national policies if special attention is not given to how said policies will be implemented and carried out in practice. In this respect, even though the scope of action may seem narrow –hierarchically speaking, given it is an undersecretariat within one of the many ministries–, it will all depend on how work is planned for the future, and fundamentally, on how they expect to ensure at a national level that the cybersecurity strategy is respected and complied with by all State divisions, as well as by the private sector.

The cybersecurity issue also poses problems that must be approached through the protection of personal data. The Argentine legal system establishes high standards of privacy protection and Law 25.326 –on personal data protection– is based on the European legal model. In this respect, the prohibition to process and transfer personal data without the data holder's consent is one of the pillars in our system. However, said rule does not apply when it comes to the databases

[32] Interview with Dr. Hugo Scolnik, May 2016. He holds a Bachelor's degree in Mathematics from the University of Buenos Aires and received a PhD in Mathematics from the University of Zurich. He is a consulting head professor at the Computer Science Department, FCEN-UBA and company CEO at Firmas Digitales SRL. From 2009 he holds the role of Adjunct Director in the Master's degree program in Information Security at University of Buenos Aires.

of state agencies. The broad interpretation of the rule allows for various state agencies to handle personal data beyond the strictly necessary and proportionate.

In this way, the authorities rely on a broad discretion margin, without an adequate control of independent bodies. Thus, citizens are deprived of numerous tools to protect themselves against potential privacy intrusions. Given its lack of functional independence and the budgetary issues resulting from the lack of financial self-sufficiency, the National Directorate for the Protection of Personal Data (DNPDP in Spanish) has not been able to efficiently perform its controlling functions, and has adopted since its creation a role that is more oriented towards education, participation and dissemination, rather than law enforcement.

viii An external viewpoint on cybersecurity in Argentina we do not necessarily agree with

a "Cybersecurity and Critical Infrastructures in the Americas"

At the beginning of 2015, the OAS in partnership with Trend Micro Inc. presented the report "Cybersecurity and Critical Infrastructures in the Americas". We will mention the findings they arrived at regarding the specific case of Argentina.

The Trend report states that as of 2014, ICIC has accomplished the following:

- Help pass the current cybercrime-related legislation, "which has allowed for the successful investigation and prosecution of several cyber-criminal cases", but it does not give more details regarding the specific cases that were benefited or statistics allowing to assess the success of the legislation, for example.
- Develop the initiative known as "Internet Sano" ("healthy" or "sound" internet), which promotes and provides educational material on responsible information and communications technologies and internet use.
- Carry out cyber incident response exercises –called ENRIC–, which had begun to take place since 2012.

On the other hand, it also established that "The ICIC has actively participated in events sponsored by the OAS, European Union Institute for Security Studies (EUISS), International Atomic Energy Agency (IAEA), Meridian Process, among others" (Page 42).

Finally, the report concludes the section on Argentina sharing three key aspects which were stated in the report "Cybersecurity Trends in Latin America and the Caribbean"[33] –made by the OAS and Symantec–; they were identified by Argentine governmental authorities as primary impediments to their on-going cybersecurity and cybercrime-related efforts, specifically:

- The persistent lack of awareness among stakeholders at all levels;
- Issues and concerns regarding privacy;
- Insufficient funding.

b "Cybersecurity: Are we Ready in Latin America and the Caribbean?"

In March 2016, the IDB and the OAS published the report "Cybersecurity 2016: Are we Ready in Latin America and the Caribbean?",[34] which examines the maturity level of various countries regarding four dimensions on cybersecurity: Policy and Strategy, Culture and Society, Education, Legal Framework and Technologies.

In the country profiles, for Argentina, the IDB establishes that "led by the National Program for Critical Information Infrastructure and Cybersecurity (ICIC) in coordination with various agencies, academic institutions and the private sector, the Government of Argentina has developed a draft National Cybersecurity Strategy that is currently awaiting adoption". Throughout the investigation conducted for this report, we have not found any clues leading to the existence of a

[33] Cybersecurity Trends in Latin America and the Caribbean, OAS, Symantec, page 38. June 2014. Available at: https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends

[34] Cibersecurity 2016, IDB. March 2016. Available at: http://observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5

project of a cybsersecurity national strategy, or the belief that such strategy is in the final implementation process. Different technical experts interviewed agreed that one of the flaws of the ICIC was the lack of publication of materials related to its objectives and work, which would allow society's actors to collaborate in the improvement of cybersecurity policies; for example, one of the ICIC's obligations was to publish yearly reports; but from its inception, the ICIC has published no report.

In this respect, if we assessed the work done by ICIC since its creation based on the publication of materials (that is: reports, policies, strategies, etc.) which obey the functions set forth by regulations, we could affirm that the yearly reports never existed, let alone a project of a national strategy. Throughout the investigation we insisted –to no avail– on getting an interview with the authorities responsible for the ICIC in 2015, in order to learn the official version about the work done by ICIC.

The lack of dissemination and transparency of the work done by ICIC coupled with the lack of participation of the various actors who should have been brought together by ICIC to assist in the process of cybersecurity policy making (technical community, academia, civil society, the private sector), accounts for two key errors in the work involving public policy making, which, as we have seen, is consistently highlighted in international studies.

The IDB also highlights the expansion of e-government and e-commerce services in the country, in respect of which it establishes that "government agencies have led awareness-raising campaigns to educate the public about cybersecurity", regarding initiatives such as "Healthy Internet", led by the ICIC, and "With You on the Web", an initiative from the National Department for the Protection of Personal Data (under the Ministry of Justice and Human Rights). Both initiatives were happily welcomed by various sectors of the society and complimented on for transitioning into the right path towards a greater capitation in technology and rights, especially in the most vulnerable demographics, such as boys, girls and adolescents. Projects have materials focused on parents and children, with guides on cyberbullying, grooming,[35] threats online and advice on how to protect

[35] *Grooming*: the predatory befriending of children on the web to lure them into sexual abuse

one's identity, reputation and image on the Internet. Currently, both initiatives are closed and none of the respective agencies have communicated plans for their continuation. Given this situation, we should mention the work done by the Fiscal Specialized Unit Cybercrime (UFECI, in Spanish) under the Public Prosecutor's Office in its contribution to raising awareness about Internet use through the elaboration of didactic material, such as the guide "How can we avoid being a victim in social networks?".[36]

To conclude this section, it is worth mentioning that the information included in reports such as those published by Trend and Symantec must be considered bearing in mind the role played by these companies in the global market of digital security, whose commercial purpose is to develop security software. For this reason, statistics may not represent an integrated view on the current state of a country's situation, but a biased view, given the type of information these private companies have access to or collect, and which is analyzed based on their own interests. If the research methodologies used in reports are not made public in detail, the cybersecurity policies of a country cannot be defined based on studies made by companies who have an interest in the market; hence, it is essential to develop investigations and studies by those who are part of the process of cybersecurity policy making, with the assistance of external consultants from society as well as from experts of the technical community and academia.

VI Intelligence and Cybersecurity

i The link between intelligence and cybersecurity

As analyzed earlier, at a global level, one of the trends in the discourse on cybersecurity focuses on facing this practice with the view to protect society as a whole, not just specific individuals. All State divisions and the private sector

or trafficking

[36] "How can we avoid being a victim in social networks?", UFECI, MPF. April 2016. Available at: http://www.fiscales.gob.ar/procuracion-general/como-evitar-ser-una-victima-en-las-redes-sociales/

must work in a holistic way. This results in national sovereignty being part of the cybersecurity policy, which allows those responsible for intelligence and national defense to be part of the discussion, development and implementation of said policies.

The New National Intelligence Doctrine treats cybersecurity as a new complex criminal phenomenon that the Federal Intelligence Agency will have to address through the production of national intelligence, specifically criminal intelligence. Even though the organic structure created for the AFI, which included the Cybersecurity Intelligence Operations Department, was repealed, we should mention the explanations given by the former Director of the Agency, Oscar Parrilli, in order to understand how cybersecurity had been conceived of within the national intelligence system.

During a press conference given in July 2015 to present the New National Intelligence Doctrine, Parrilli informed that the Operations Department would be responsible for "cyber and information crimes in the modern world, as well as the critical infrastructure in Argentina, which is part of its nuclear power plants, banks and the like and all the protection that has to be provided. In this context, there has been shocking news in the last few years: the German parliament has been threatened and hacked and institutions have been hacked in the United States and England. In turn, in Argentina we did not have a policy to anticipate, study, analyze or undertake intelligence activities on this issue. We have created it and will launch it in the coming days. In addition, we basically pride ourselves on the fact that a very prestigious Argentine computing engineer who comes from the private business sector and knows all these topics in depth will be in charge of this organism. He will provide us Argentine citizens with great support so as to avoid this type of threats and actions that may affect security and national defense."[37]

Given the short period of time the Cybersecurity Intelligence Operations Department had been running, we have not been able to obtain much information on

[37] Parrilli, Oscar. Press Conference. Casa de Gobierno. July 7, 2015. Available at: http://www.casarosada.gob.ar/informacion/conferencias/28837-conferencia-del-titular-de-la-afi-oscar-parrilli-en-casa-de-gobierno

it, except for some information obtained from informative notes. In an interview that was published on December 1, 2015, Parrilli informed that the Department had been working at full capacity for less than a month and that it was responsible for observing cyber attacks that occurred in the world, analyzing when the country could be said to be threatened and issuing the corresponding warnings if necessary; apart from participating in judicial investigations if the Federal Justice so required.[38]

Sources close to the former Director of the AFI mentioned that the choice of the term "cybersecurity" only refers to a simple catchy invention without really considering the implications of using this term in the field of national intelligence, despite warnings made by experts on the subject from their professional circles.

In this context a lack of a definition for cybersecurity at a national level causes problems. Failure to define precisely what cybersecurity is or what it is not allows for free interpretations of the term to be made.

The specialists and experts on cybersecurity consulted throughout this project agree that cybersecurity requires intelligence activity, linking it with the national defense and the protection of citizens. Mariano del Río states that "one just has to see the limitations security forces have to address the issue of cybersecurity. Unfortunately, the AFI has been used for purposes that have nothing to do with providing valuable information to fight against organized crime. Today, any information that may be found regarding cybersecurity matters is valuable for the investigation and battle against illegal activities."

The new organic structure to be adopted by the AFI will have to consider its scope of action regarding these matters. For example, with the former structure, one of the responsibilities of the Department of Cybercrime Intelligence –within the Cybersecurity Operations Department– was "producing intelligence in order to gain awareness of the activities that may constitute a cyber crime in any form or kind". Would this imply turning the AFI into a sort of cyber police, with the power to investigate citizens' virtual lives? ¿What added value could the AFI

[38] Bullentini, Ailín. "Predicting and Preventing Cyberattacks", Página/12, December 1, 2015. Available at: http://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html

offer which has not yet been offered by the Specialized Cybercrime Unit (UFECI, for its acronym in Spanish)[39] under the Public Prosecutor's Office?

ii Brief history on intelligence in democracy, a system unable to break bad habits

The intelligence services in Argentina emerged after the Second World War as a global trend with the view to defend the Nation and its interests. For many years the services were regulated by secret decrees issued by the Executive Power until 2001, when the National Intelligence Law (No 25.520) was passed in order to define the intelligence activities, narrow the scope of action and establish control mechanisms. It was a futile attempt that was unable to modify the operation of an agency maintaining practices, personnel and customs used since the military dictatorship. This is key to understanding why the main intelligence agency of Argentina kept apart from the democratization process that started in 1983. The intelligence agency remained closely connected with the dictatorships ruling Argentina during the 50's and 70's, as well as with the crimes against humanity committed during those years.

As previously mentioned in ADC's report "The democratic (un)control of intelligence agencies in Argentina",[40] with the return of democracy, president after president, the agency was kept under continuous reform that was more connected with political power than with an attempt to democratize an agency used as the carte blanche by the president in power, who would use the State's intelligence apparatus for the purposes of political espionage (involving officers, opponents, trade unions, journalists, among others), to finance bribes for judges and prosecutors with the agency's reserved funds, obstruct the investigation of one of

[39] Di Nicola, Gabriel. "A specialized prosecutor's office is created to fight against cybercrime" ["Crean una fiscalía especializada para la lucha contra el cibercrimen"], La Nación, November 18, 2005. Available at: http://www.lanacion.com.ar/1846626-crean-una-fiscalia-especializada-para-la-lucha-contra-el-cibercrimen

[40] El (des) control democrático de los organismos de inteligencia en Argentina, ADC, 2015. Available at: https://adcdigital.org.ar/portfolio/des-control-democratico-los-organismos-inteligencia-argentina/

the most controversial cases in Argentine history in connection with terrorism, disputes with the armed forces such as the Federal Argentine Police, and the repression of social movements with the economic crisis of 2001.

These are some of the events in which the intelligence agency had a key role in the history. As concluded in the abovementioned report, the lack of consequences on the scandals involving the intelligence system can be explained by the strong link between intelligence agencies and the executive power, which exerts part of its power over a secret agency with access to vast economic resources and which stays away from democratic control.

In the report "Who's watching the Watchers?" (ADC, 2014),[41] we made a comparative study on the various control systems of intelligence agencies, especially in Latin America. In the case of Argentina, this role is performed by the Bicameral Committee for the Control of Intelligence Agencies and Activities (of the National Congress), which was created in 2001 after the intelligence law was passed. In this study, it was mentioned that the Committee started to work 3 years after its creation, that it guards a strict secret regarding its activities, without even mentioning its meetings, reports or work agenda, and that even various members of the Committee had never received the yearly report the Committee had to make by law on a yearly basis for it to be sent to Congress and the Executive Power.

iii The Federal Intelligence Agency

In late 2014, the Federal Intelligence Agency began one of its most polemic reformation periods, which begun with several internal struggles[42] and the removal of one of the most controversial characters in the history of this agency, spy Antonio Jaime Stiusso, linked –among other things– with the investigations on

[41] "Who's watching the Watchers?", ADC, 2014. Available at: https://adcdigital.org.ar/portfolio/whos-watching-the-watchers/

[42] "An article by Revista Noticias brings down the leaders of the Secretariat of State Intelligence" [Tras una nota de Noticias, cae la cúpula de la SIDE], Perfil, December 16, 2014. Available at: http://www.perfil.com/politica/Tras-una-nota-de-Noticias-cae-la-cupula-de-la-SIDE-20141216-0039.html

the terrorist attack against the AMIA, in which the agency was involved from the very beginning. Stiusso's resignation was accepted by the former head of the then Secretariat of Intelligence –Oscar Parrilli– by order of former President Cristina Fernández de Kirchner. Stiusso had been the AFI's general director of operations, and had been working in the field for 43 years.[43] In January, 2015, a day before testifying to the Congress on a report involving the highest spheres of power (including former President Cristina Fernández de Kirchner), Alberto Nisman, federal prosecutor in charge of the AMIA case, was found dead from a shot to the head.[44]

This series of events, together with the prevailing political background, led to the enactment, in March, 2015, of Law No. 27126, amending Law 25.520 and introducing two major changes at the institutional level: the creation of the Federal Intelligence Agency (to replace the former Secretariat of Intelligence) and the Interception and Captation of Comunications Department (to replace the former Directorate of Judicial Surveillance).

Subsequently, Decree No. 1311/2015 (as amended by Decree No. 2415/2015) approved the New National Intelligence Doctrine for the purpose of establishing the AFI's organic and functional structure, as well as a professional regime for intelligence personnel. An analysis of the instruction and training of intelligence personnel can be found in the "Teaching to surveil" report (ADC, 2015).[45]

The creation of the Interception and Captation of Comunications Department (DICOM, for its acronym in Spanish), directed by prosecutor Cristina Caamaño, which was part of the General Directorate of Investigation and Technological Support for Criminal Investigations (DATIP, for its acronym in Spanish), within

[43] Obarrio, Mariano. "Stiusso was removed from the Secretariat Intelligence" [Desplazaron a Stiusso de la Secretaría de Inteligencia], La Nación, December 20, 2014. Available at: http://www.lanacion.com.ar/1754189-desplazaron-a-stiusso-de-la-secretaria-de-inteligencia

[44] "The internal struggles in the former Secretariat of State Intelligence are the main characters of the Nisman case" [La interna de la ex SIDE, protagonista en el caso Nisman], Diario Popular, January 22, 2015. Available at: http://www.diariopopular.com.ar/notas/214977-la-interna-la-ex-side-protagonista-el-caso-nisman

[45] Educar para vigilar, ADC, 2015. Available at: https://adcdigital.org.ar/portfolio/educar-para-vigilar/

the scope of the Public Prosecutor's Office,[46] was aimed at affording a greater independency to officers in charge of intercepting communications, by removing them from the scope of the intelligence agency, on which the full and exclusive power on telephone tapings in Argentina had been historically vested.

Thus, under section 17 of Law No. 27.126, the DICOM became "the only State agency in charge of intercepting or recording communications of any kind as authorized or ordered by a court of competent jurisdiction".[47] This means that, should they need to tap a telephone line or intercept any other kind of communication between users, the AFI, the federal forces (Federal Police, Border Patrol, Coastguard, Airport Police), the Metropolitan Police, and the provincial police agencies must submit a formal request before a court of law for it to be then processed by the DICOM, and any other means of interception are illegal. A more detailed explanation of the creation of the DICOM and the transition from the AFI can be found in the "Teaching to surveil" report (ADC, 2015).

The arrival of the new Federal administration, led by Mauricio Macri as head of the Executive, brought new changes into the intelligence agency and the interception of communications.

In early 2016, Gustavo Arribas and Silvia Majdalani were appointed as AFI's Director and Deputy Director, respectively.[48] This was criticized by the Citizen Initiative for the Control of the Intelligence System –of which ADC is a member–,[49] since these officers lack adequate training and knowledge on the workings of the intelligence system, which brings their professional aptitudes to hold such

[46] Public Prosecutor's Office. Resolution No. 2067/15. July 7, 2015. Available at (PDF): http://www.fiscales.gob.ar/procuracion-general/wp-content/uploads/sites/9/2015/07/PGN-2067-2015-001.pdf

[47] Section 17 of Law No. 27.126 Available at: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

[48] Savoia, Claudio. "The internal struggles in the former Secretariat of State Intelligence are worsened by controversial appointments" [La interna de la ex Side arde con las designaciones polémicas], Clarín, December 19, 2015. Available at: http://www.clarin.com/politica/Agencia_federal_de_Inteligencia_0_1489051101.html

[49] "Citizen Initiative for the Control of the Intelligence System: Problems with the appointment of officers to the AFI" [ICCSI: Problemas en la designación de autoridades de la AFI], March 30, 2016. Available at: https://adcdigital.org.ar/2016/03/30/iccsi-problemas-designacion-autoridades-afi/

delicate offices into question.

In turn, under Decree No. 256/2015, the Executive transferred the DICOM from the scope of the Attorney general's Office to that of the Supreme Court of Justice (CSJN, for its acronym in Spanish). For such purpose, by means of Decree No. 2/2016, the CSJN created the Captation of Communications Directorate (DCC, for its acronym in Spanish), which entirely replaced the DICOM; a situation that was duly analyzed by the ADC.[50]

The various events described in this section show the characteristics and defects developed by the Argentine intelligence system, and especially by its central agency –AFI–, throughout its gruesome history. Given the role this system seeks to play in the development of Cybersecurity policies, its participation cannot be regulated by the presumptions and ambiguities in the applicable laws. On the contrary, in order for its vices and defects not to impact Cybersecurity policies, it is essential to determine its scope of action and the way in which it is to operate.

VII Final comments

By the time this report was edited and published, several interview request were still awaiting a reply. Specifically, with the new authorities responsible for the Undersecretariat of Technology and Cybersecurity, Ministry of Modernization; Undersecretariat of Cyberdefense, Ministry of Defense; and the Joint Command of Cyberdefense, under the Joint Chiefs of Staff of the Armed Forces.

VIII Conclusions

Over the last years, initiatives in the field of cybersecurity took a step in the right direction by seeking to focus the work on the matter from the perspective of the

[50] "Thoughts on the creation of the Captation of Communications Directorate" [Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones], ADC, February 19, 2016. Available at: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/

State, setting goals and tasks adequate to start developing a true cybersecurity agenda which can be expanded nationwide. As described in the applicable section, this never actually took place, not only because of the lack of budgetary allowances for the agencies in charge of carrying out these tasks, but also because of the way in which those responsible chose to approach the matter, especially by failing to work, act and show their results in a transparent or open manner, encouraging the participation of experts who could input their vision, knowledge and experience to improve State practices.

Given the lack of international consensus regarding the definition and scope of cybersecurity, Latin America still has a chance to move towards a new concept of cybersecurity which is not a direct result of the military, defense and intelligence fields, but also adopts the upholding and respect of the basic rights of citizens and international human rights standards as the fundamentals of cybersecurity, avoiding to copy the practices of other regions and countries whose situation is not the same as ours.

Based on the work developed in this report, we believe it essential to highlight, from the civil society, some recommendations regarding the development of public cybersecurity policies.

Given that Latin America can still move towards a conception of cybersecurity respectful of human rights, States must promote dialogue and debate in forums allowing them to share their experiences and tools, for the purpose of consolidating standards which strengthen cybersecurity not only in each particular country, but throughout the entire region.

The scope of action of intelligence and cyberdefense agencies must be clearly limited, with a focus on the transparency and accountability of its main bodies, to prevent illegal practices and inefficiencies from being concealed through secrecy.

In view of the appointment of new authorities in charge of the various aspects of cybersecurity within the Ministry of Modernization, as well as in the National Directorate for the Protection of Personal Data (DNPDP, for its acronym in Spanish), it is essential to reformulate the dynamics of cybersecurity policies and the debate on the amendment of the Personal Data Protection Law (LPDP, for its acronym in Spanish), promoted by the authorities of the DNPDP.

At the same time, we must seize this opportunity to update, improve and deepen training programs introduced in subsequent years, such as “Internet Sano” and “Con Vos en la Web”, which play a major role by affording and improving citizens’ access to basic digital security levels.

In the past, State agencies in charge of promoting cybersecurity policies worked in a close and nontransparent manner, staying away not only from citizens, but also from experts. To ensure the full development of public cybersecurity policies which reach all social stratums with necessarily holistic outlook, we must engage all social players to contribute to the planning and implementation of such policies, both in the private sector and in the scientific, academic and civil societies.

These central ideas must be aimed at achieving a sustainable cybersecurity environment, allowing citizens to lead a safe virtual life while completing administrative proceedings, purchasing goods or performing other daily activities online; forcing public and private agencies to respect personal data and adequately safeguard and control databases in accordance with the LPDP; causing the different State bodies to maintain the same level of infrastructure protection and safeguarding of the information handled and stored by them; granting agencies such as the Office of the Prosecutor for Cybercrimes (UFECI, for its acronym in Spanish) the resources needed to face the challenges posed by these crimes and produce reliable statistics to help shape cybersecurity polices; allowing the cybernetic emergency response team to work in an efficient manner, receiving information and reports from all civil players, and advise and help those in need.

ADC

por los Derechos Civiles