Hackers and Coppers 2

Summary, analysis and perspectives from informal conversations with the infosec community

Beatriz Busaniche
Fundación Vía Libre[1]
www.vialibre.org.ar

Methodology

This document was elaborated from free conversations held during a working meeting organized in December 2018 under the premise of the informal talk on a semi-structured thematic agenda. The most approximate methodological approach is that of the focus group, however, the technique was not systematically applied.

Findings from our research with the *infosec* community

Throughout our first report[2] on the relationship bewteen the *Infosec* community and the current laws that affect its activity and law enforcement agencies, we found some guidelines that allow us to detect key areas of work in the future to strengthen the capabilities of the community and with it, significantly improve computer security strategies in Argentina and the region.

We understand that the strengthening of the community in Argentina implies a strengthening at the regional level due to the magnitude and influence that the *infosec* community of our country has in the region, especially due to the impact of various local initiatives that have gained enough visibility and magnitude to be the undisputed reference in the region. An example of this is the annual celebration of the largest *hackers* meeting in the region, **Ekoparty**, an event attended by practitioners from all over the continent and where the discussion on the practice and current affairs of the computer security field is broadened.

A fundamental finding of our research is that the *infosec* community considers that legislators and policy makers have little or no knowledge about the field they regulate when they address issues related to computer security and information technology in general. In the eyes of the community, legislators also lack good advice on the subject.

Within the framework of the informal conversations we had with the community, we also detected that there is a very critical view of the cybersecurity policies adopted by public bodies, and even a very distrustful view of the State's capacity in this area. Especially, the definition of cybersecurity appears as a controversial since it includes in that concept actions as diverse as a *fishing* attack, child pornography trafficking or grooming as well as a threat to a public official in any social network.

On the other hand, it clearly appears that not only there is no appropriate operational concept of work, but that the actions taken are purely punitive and absolutely ineffective in protecting the citizenry and defending the IT infrastructure in Argentina before an eventual attack.

An antecedent regularly mentioned in the meetings with the community has to do with the adoption of regulations that make a lean contribution to strengthen the *infosec* community in Argentina and in some cases contribute to the deterioration of their working conditions.

For example, the case of the computer crime law approved in Argentina in 2008 is cited regularly, That law modifies the criminal code in the following way:

2 See Hackers and Coppers 1.

> It will be punished with imprisonment from fifteen days to a year, ... that who alter, destroy or makes unusable data, documents, programs or computer systems; or sell, distribute, circulate or introduce into a computer system, any program designed to cause damage. [3]

Since the beginning of the debate on this legal reform in 2006 in which Fundación Vía Libre participated intensely, we have reiterated that the ban on circulation of software and any other system of this type due to its capacity to cause damage is contrary to the practice of security, since the same tools that are used to attack a system are appropriate to defend it. However, the capacity of incidence in the matter has been practically null.

Another issue that emerged from our informal conversations is the ratification by Argentina of the Budapest Cybercrime Convention. This agreement is hardly known by the *Infosec* Community, although it is a relatively old document for the field to which Argentina adhered with very few reservations.

Another issue emerging among the concerns of the *infosec* community has to do with intellectual property regulations and the various initiatives including the extension of the related criminal types, especially those related to reverse engineering. and with the possibility of conducting research on systems with digital rights management or DRM by its acronym in English.

Clearly, the other major concern besides the lack of proper advice for legislators is the tendency to replicate foreign models with their own weaknesses and problems. For example, the tendency to adopt measures related to surveillance in social networks, the incorporation of backdoors in certain programs, among other topics appear in the informal conversation with the *infosec* community.

Undoubtedly, one of the main causes of concern is the uncertainty at the time of vulnerability reporting. The local antecedents of prosecutions, imputations and even raids to the domicile of members of the local *infosec* community for having reported vulnerabilities to companies discourages the practice and generates a serious precedent in the country.[4]

To add a critical aspect, we could also mention that almost anything is considered cybercrime or cybercrime because it occurs on the Internet. For example, in the working documents of the Organization of American States (OAS), which has set the guidelines on Cybersecurity for the entire region, there is a ridiculous mixture of actions as disparate as hate speech or a threat on social networks. until the critical infrastructure vulnerability report. If all this is put in the same bag and public policies are not clear about it, then a country's cybersecurity strategy is doomed to fail.

Another relevant coincidence within the community is that over the years, despite the prestige it holds, the high level of local specialists, the capacity of the local members, *infosec* community was never called to make any contribution when regulating cybersecurity in Argentina. Added to this is the distorted image of a community of hackers rich in experience and knowledge but often viewed from the media as a band of criminals. The installed capacity of the *infosec* community does not deserve that disdain under any circumstances.

Everyone remembers and highlights as a fundamental milestone the contribution of this community to the discussion on electoral reform to introduce electronic voting in 2016 at the National

3 See Ley de Delitos Infomáticos. Modificación del Art. 183 del Código Penal http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

4 The case of Joaquín Sorianelo, accused of alleged cybercrime after having reported vulnerabilities in the system to the firm MSA SA, provider of electronic voting systems in the Autonomous City of Buenos Aires is the most prominent and cited, but not the only.

Congress. However, in that case, it was the community itself that was mobilized to influence that debate because of its crucial importance. In addition, many people observed that debate as a breaking point of the potential involvement of this community in public policy issues that are linked to their interests and competencies.

Finally, it is important to highlight the goodwill of the community when it comes to getting involved in the definition of public policies to strengthen information security. They know that without the participation of the community of practice in making strategic decisions, little can be done in an approach to information security as a system.

They do not know what the mechanism might be, but they also clearly understand that you can not look only at potential attackers, but that you need to establish strategies and public policies that commit companies and organizations that administer critical infrastructure to take serious precautions at the right time to protect the information they hold. This is especially clear when evaluating what is the responsibility of those who handle not only citizens' information (such as public bodies) but also all those members of the private sector that administer critical infrastructure by concession (such as public service concessionaires).

The lack of an information security policy in these sectors, the lack of appropriate response to vulnerabilities reports or the breach of data and information of citizens can not be minimized when distributing responsibilities regarding information security.

The cybersecurity agenda in the region

In the region, the main organization working on the Cybersecurity agenda is the Organization of American States (OAS), which for several years has been making recommendations to its member countries on information security strategies.

However, when reviewing the OAS reports we found that under the Cybersecurity agenda there are initiatives as diverse as the search for lost children and adolescents using the error 404[5] to studies and profiles of cybercrime.[6] The OAS publications for the period 2015-2018 are numerous and are available in the Cyber section of the agency's website.[7]

The OAS Cybersecurity Program (as it calls itself on the agency's website) has been working since the early 2000s with the goal of assisting member countries to strengthen their technical capacity and their IT security policies to guarantee a "safe and resilient cyberspace".[8]

Its objectives include the incorporation of multiple stakeholders, including civil society and end users of technologies as a key part of cybersecurity processes. As far as we can investigate, this incorporation has not only not happened, but the contributions from the infosec community have been hardly considered.

After many years of work in this agenda, the reality is that civil society, end users and the community of *infosec* are absent from the debates that have resulted, at least in a first

5 See https://www.sites.oas.org/cyber/Documents/2016%20-%20Presentacio%CC%81n%20No%20Encontrado-Daniel%20Monastersky.pdf (Visited on Dec. 27, 2018)
6 See https://www.sites.oas.org/cyber/Documents/2016%20-%20Tendencias%20y%20oportunidades%20en%20ciberseguridad-Alberto%20Bohorquez.pdf
7 See https://www.sites.oas.org/cyber/EN/Pages/Documents.aspx
8 See https://www.sites.oas.org/cyber/es/paginas/contacts.aspx

approximation, in mere legislative modifications of a punitive nature, in the creation of new criminal laws and, in many cases, the incorporation of aspects that have little or nothing to do with what we might understand as cybersecurity, such as bullying, online harassment, threats against politicians and grooming.

Argentina and cybersecurity. A pending issue

Until the end of 2015, the leading agency in charge of the so-called "cybersecurity" in Argentina was the National Program of Critical Infrastructures and Information and Cybersecurity (ICIC) under the purview of the National Office of Information Technology (ONTI) dependent on the Chief of Cabinet of Ministers. Within this scope, the first CERT (Computer Emergency Response Team) was created at the national level in 1994 and in 2011 it was designated as part of the ONTI. After the change of government and with President Mauricio Macri in house, all these functions were transferred to the Ministry of Modernization, which was later dissolved and reconverted into the Modernization Government Secretariat under the direction of the Cabinet Office.[9]

The area of investigation of computer crimes is the Technological Crimes Division within the Argentine Federal Police.

An important factor to be highlighted is that neither private sector companies nor public offices are obliged by law to provide information related to incidents suffered in relation to the security of their information to national authorities. In the Argentina section of the OAS regional report, the national authorities indicated that although the 2008 law has allowed the classification of certain practices as crimes, the main obstacles they face have to do with the nature of many of them that have no borders and are in "constant evolution", certainly a debatable position since crimes are undesirable behaviors in a society and their definition should not be tied to the use of a certain technology that can evolve or become more sophisticated. Without further comments, a scam is a scam, either committed in a corner of the city or through an email. This explanation of the Argentine government says more of the low legislative quality than of the problematic itself of the typified crimes.

In turn, the OAS report details government initiatives to raise awareness of the challenges of cybersecurity as well as the creation of an initiative called "healthy Internet" aimed at promoting the responsible use of ICTs and the Internet. Another program mentioned has to do with the "Con vos en la web" initiative, a data protection campaign for children and adolescents designed by the now restructured National Directorate for Personal Data Protection.

The OAS report also indicates that there is no detailed record or available figures of incidents and computer crimes or other malicious computer activities, but highlight an alleged increase in "identity theft", fraud through social networks, email or online banking through the use of social engineering or keyloggers. It is eloquent that under the figure of cybersecurity there are too many questions of a very diverse type, variety and impact. The government recognizes as limiting and impediments: "the constant lack of awareness among stakeholders at all levels, problems and issues related to privacy, and insufficient funding."[10] It is worth mentioning that issues related to privacy should never be considered a limitation to the investigation of crimes but should be part of the

9 See https://www.argentina.gob.ar/modernizacion/infraestructuras-criticas-de-informacion-y-ciberseguridad (Visited on Dec. 27, 2018)

10 See https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf pag. 35 y 36 (Visited on Dec. 27, 2018)

system of constitutional rights and guarantees that the State and public bodies have an obligation to respect and protect.

Since then and within the framework of the new admininstratio since December 2015, the cybersecurity strategy has not changed.

However, "cybercrimes" are always mentioned in legislative projects such as amendments to the intelligence law, in adherence to the Budapest Convention and in the design of the various regulations linked to the Ministry of Security and within the framework of the investigation of complex crimes.

To date, the strategy of "cybersecurity" in Argentina has not evolved and suffers from the same historical problems that characterized it over the past decades: security is not seen as a system, there is no clear distinction between issues such as speech crimes or a potential attack against critical infrastructure, companies are not required to develop nor maintain clear security policies and they are not required to report data breaches, the search and report of vulnerabilities is not promoted as a good practice and there is a clear lack of fluid cooperation with the rich and solid *infosec* community in the country.

Why is it necessary to develop an Infosec and Human Rights agenda in coordination with the local community?

The intersections between the *infosec* community, cybersecurity policies and Human Rights are many and are not always explored properly. In this brief report we want to highlight some key aspects of these intersections.

Electoral Rights

Within the framework of civil and political rights, the rights to secret, accurate, equal, auditable and transparent voting are part of the fundamental principles that the Constitutions of any democratic country must ensure. Since the end of the 90s of the last century, initiatives to "modernize" electoral systems have led various countries to engage in experiences of electronic voting and computerization of various areas of electoral processes. From that first uncritical utopianism that gave support to numerous legislative initiatives of adoption of electoral technologies to the present of criticisms and setbacks of those processes, we've seen numerous experiences in which the *infosec* community has been and is the key factor.

In Argentina, the *infosec* community has been key to call public attention to the vulnerabilities and problems associated with the incorporation of computers in the intermediation between the citizens and the expression of their political will, their vote. First, it was the key factor in the experience of the Autonomous City of Buenos Aires in 2015 in which the community had virtually its political baptism that concluded with raids and threats of all kinds to various members.

After that, with an active participation in the parliamentary debate in the National Congress in 2016 that ended up with the consequent suspension of the electoral reform that the executive power

impelled for the national elections of 2017. It was the academy, the Civil Society and the local *Infosec* community the main responsible of having detected and reported serious vulnerabilities that would have seriously risk the electoral rights of the Argentine citizenship.

Right to integrity and public safety

Contrary to the negative image that has been built of the figure of the hacker, nothing is further from the reality of the infosec community in Argentina and the region. The integrity of critical infrastructures is an issue of constant concern for the community and the possibility of contributing in these areas is fundamental.

With no clear delimitation of the scope of the problem, little can be done to protect the integrity of information and to take care of public safety. Cibersecurity cannot be a mixture of very diverse issues such as grooming, insults in a social network or online hacktivism. Instead, we have to think about the real and potencial threats that should be seriously considered, specialy to protect critical infrastructures as public services, government facilities and citizens sensitive data.

Right to privacy

The incorporation of more and more devices of the so-called “Internet of Things” into everyday life poses risks to the security and privacy of people in the domestic sphere. Without a solid security community capable of reporting vulnerabilities, more and more companies will integrate their applications to our phones with potencial backdoors to our homes from which personal data, conversatioins, life habits and our full life could be breached.

A strong infosec community could contribute to find and report those problems and raise the bar of demands to these companies that sell appliances and other devices that could have multiple vulnerabilities.

In turn, it is essential to have a critical perspective at the various applications that governments are using in their interaction with citizens to control the use and potential abuse of personal data.

We, the citizens, have the right to know how they work and what data is obtained in each of our interactions with the *apps* of public administrations at all levels, so they must be auditable and subject to deep investigation by the community. In this case, an open and transparent policy and promotion the reporting of vulnerabilities is also fundamental.

Access to information right

When a public office or a public services company has a security breach, it is essential to demand the publication of it and to inform appropriately the people who may be affected by this type of incidents. Access to information about this kind of situation should be promoted so that citizens can take the necessary precautions. The public offices in charge of the citizens' personal data should be required to report appropriately any security incident and the mitigation measures adopted. In addition, an appropriate vulnerability reporting policy should be promoted.

Freedom of expresion and hacktivism

Last but not least, the computer community has a long history of activism of all kinds and this field must be respected and protected with all the guarantees of freedom of expression and the right to social protest. We cannot confuse hacktivism with computer crime. Actions such as the intervention of a website with a political message should be analyzed within the fundamental right to expression and social protest. We also cannot confuse the political actions of a community with the actions of computer criminals.

Likewise, in order to protect the right to freedom of expression and hacktivism, the right to anonymity on the Internet, the use of pseudonyms and the anonymous report of vulnerabilities should be vindicated and protected to give the community a safe harbor. In relationships increasingly mediated by digital devices, infosec has a key role.

Nor should minor actions, that could be treated appropriately in a different fora, be incorporated into the punitive field. Issues of real concern, like hate speech, insults or other expressiones that may border the limits of freedom of expresion, should be approached with great care. We should tend to the reduction and not to an increase of the so-called expression offenses.

Furthermore, it is essential that the report of a detected vulnerability should never constitute an offense if the appropriate steps and good practices for the protection of public safety and fundamental rights have been followed, especially when the report of such information is protected by public interest.[11] A set of good practices as a public policy is also needed.

Next steps

As a result of this research developed by Fundación Vía Libre in cooperation with an important sector of the *infosec* community of Argentina, some actions can be outlined for the year 2019 onwards.

- To establish a permanent working committee between the *infosec* community and the Vía Libre Foundation to maintain the course of work opened in this research, review the state of the art in legislative and public policies fields and design public advocacy strategies.
- To promote permanent dialogue with advisors of decision makers, including national level legislators as well as officials from related areas to enhance the possibilities of establishing a common work agenda.
- To design and implement a vulnerability reporting system aiming to protect infosec researchers and comply with the public responsibility to report on real and potential incidents that may affect citizens and public infraestructure.
- To raise awareness of the need to promote and not combat the work of the computer security community by promoting a realistic view of their role and activities, differentiating and discarding the “bad hacker” narrative installed in the press and in the public opinion.
- To positively influence the cybersecurity agenda aiming to protect Human Rights.

11 The paradigmatic example is the dissemination of the notorious vulnerabilities of the electronic voting system of the firm MSA S.A. used in the Autonomous City of Buenos Aires in July 2015 in the election for Head of Government and legislators of the City. After an arduous judicial investigation that included the search of the home of one of the hackers who reported the vulnerabilities, the court ruled that reporting the vulnerability was not a crime and that the security of the electoral system was vague. See the case of Joaquín Sorianello, interviewed in the framework of this investigation.

Acknowledgments

This work would not have been possible without the contributions of a large number of individuals and organizations. We must thank the organizers and staff of the Ekoparty, and in particular Federico Kirschbaum, Francisco Amato and Paola Mastrángelo; the experts in information security who gave us their time and patience to discuss this research, including Iván Arce, Javier Blanco, Fabián Cuchietti, Martín Doyhenard, María José Erquiaga, Johanna Caterina Faliero, Roberto Fresca, Sebastián García, Alfredo Ortega, Alfredo Rezinovsky, Juliano Rizzo, Javier Smaldone, Alberto Soliño, Joaquín Sorianello, Nicolás Waisman and others who preferred to remain anonymous; Alexia Halvorsen, who did the field work at Ekoparty; Alejo Di Risio and Matías Blanco in charge of the capture and editing of audiovisual materials and AccessNow, for their generous support for this work.

Vía Libre Foundation Team

Beatriz Busaniche - General Project Management

Carolina Martinez Elebi – Logistics, coordination, reports.

Enrique A. Chaparro – Infosec Advisor – Data Design and analysis. Reports.

Alexia Halvorsen – Field Reasercher

Alejo Di Risio / Matías Blanco – Audiovisual production

Elena Maule – Financial administration