Hackers and Coppers 1

Information security community perceptions about law and law enforcement issues in Argentina.

Enrique A. Chaparro

Assistance, logistics and field work by

Beatriz Busaniche
&
Carolina Martínez-Elebi

Fundación
Vía Libre

Hackers & Coppers 1

Information security community perceptions about law and law enforcement in Argentina

Enrique A. Chaparro

Assistance, logistics and field work
Beatriz Busaniche &
Carolina Martínez Elebi

Fundación Vía Libre
Buenos Aires, 2018

Introduction

This study

The purpose of this study is to carry out a quantitative analysis of the information security community perceptions about certain aspects of law and law enforcement directly related with the discipline. We prefer the term "information security" (*infosec* for short) because it has a broader meaning than that of "computer security", and also because it seems to be the term favoured by the involved community.

For a long time, frictions have existed between sectors of the infosec community and the law enforcement agencies. The lawmakers, often under the pressure of public opinion, tend to enact regulations to prevent or minimize actual or imagined "cyberthreats". The community, on their turn, finds that most of the regulations are seldom useful for anything but placing obstacles across completely legitimate research paths. The hacker stereotype often pictured in the mass media, covered with a hoodie and typing in the dark, has made a real disservice.[1]

How do the infosec practitioners perceive their interactions with criminal and intellectual property law? How frictional is the relationship? What level of knowledge do they have on the aspects of law affecting their work? Which fields of activity are the most harmed by sometimes inadequate regulations? What do hackers[2] think of policymakers? All these questions deserve an answer, but to our knowledge a systematic study on the infosec community perceptions about legal issues had never been done in Argentina.

Argentina has a vibrant infosec community and is home to a number of well known security experts and companies.[3] Therefore, it is an excellent field to measure the community perceptions vis-à-vis the law and the law enforcement agencies. *ekoparty*, the largest information security conference in Latin America and in the Spanish-speaking world, provides fertile ground to perform our field work: by the number and specific interests of the people attending the conference, it gives an excellent cross-sectional sample of the infosec community in all their diversity. The 2018 edition took place in Buenos Aires from 26 to 28 September, and 1933 persons attended it. About 1500 questionnaires were randomly distributed to the attendees, and 257 replies were received.[4]

1 On the other hand, the main author of this paper has worked more than thirty years in the infosec field and does not recall anyone working behind a computer in such a preposterous attire.

2 The very term *hacker* is contentious. It originally defines a person who enjoys exploring the details of programmable systems and how to stretch their capabilities (see e.g. G. Malkin & T. LaQuey Parker. *Internet Users' Glossary*. RFC 1392, January 1993, page 20; and G. Malkin. id-, RFC 1983, August 1996, page 22.) The pejorative use of the term in the mass media has caused that the general public use it with a different meaning.

3 See e.g. Penroth, Nicole. "Famed for Tango and Hackers". *The New York Times*, 1 December 2015, page B1.

4 From that number, 256 were processed and one discarded for technical reasons. The fact that the effective number of replies used in our work is 2^8, or `0xFF`, is purely coincidental.

Demographics

The first block of the questionnaire contains questions aimed to establishing the sample's demographics:

- Age groups: Respondents were asked to state their age segment by marking one of five uneven groupings: *<18, 19→25, 26→35, 36→45* and *>45*. The result shows a typical Gaussian distribution centered in the middle group: 10, 62, 112, 62, 10.

- Gender: It is a well known fact that a deep gender gap exists in general computing-related occupations[5]0], and that gap becomes deeper in the infosec field. Our survey reflects those inequalities. From the 254 respondents that answered the question about their gender, 217 (85.4 per cent of the sample) identified as male. Thirty three respondents identified as female, which represents a 13.0 percent of the sample. That figure is consistent with, and slightly higher than, global averages and higher than Latin American average shown by other surveys of women in infosec.[6] Four respondents (1.6 per cent) stated their gender as other/non-binary.[7][3]

- Relationship with infosec: the infosec community is not at all the "neckbeard computer geniuses in a basement" stereotype. People of many skills work in information security or have academic interest on it. And that group is augmented by individuals who, albeit not having full time dedication to infosec, have deep, hands-on interest on the field. All those profiles, according to the information provided by the respondents in the answers to Q4, define what is hereinafter called the "wide" or "extended" community. Two subsets were also defined:

    - The "core" subset, composed of all individuals in the sample that have infosec work as main source of income (n=110) plus individuals from the academic field whose replies showed practical involvement in infosec issues[8] (n=16); and

    - The "peripheral" subset, composed of all the remaining individuals in the sample (n=130). Five respondents that did not answer Q4 were included in this group.

5 Catherine Ashcraft, Brad McLain, and Elizabeth Eger. *Women in Tech: The Facts — 2016 Update*. Boulder, CO : National Center for Women & Information Technology, 2017.

6 Jason Reed, Yiru Zhong, Lynn Terwoerds, and Joyce Brocaglia. *The 2017 Global Information Security Workforce Study: Women in Cybersecurity*. White paper. Santa Clara, CA : Frost & Sullivan, 2017.

7 Surveying gender distribution in the infosec field lies beyond the goals of this paper. However, it is interesting to notice that three quarters of the respondents self-identified as *other/non binary* gender belong to the "core" subset.

8 For instance, by non-negative replies to Q8 and 11.

Methodological remarks

The survey was done using anonymous questionnaires. The questions were quite self-explanatory, but assistance to solve doubts was provided on request in *Vía Libre*'s booth at *ekoparty*. Providing demographic information was not mandatory but encouraged; no respondent refused to submit those data. Ninety-six respondents (37.5 % of the sample) accepted our invitation to inform a contact e-mail if the need of further communication to broaden the questions arose. After translating the textual values into numerical variables and processing, regular statistical tests for a sample of this size and a expected 90 % confidence level were conducted.

Unless otherwise stated in the text, the wide or extended community sample is statistically relevant: at 90 % confidence level, error margins are generally better than 5.4 % (they might be quite better for skewed population proportions, as in the case of Q14).

Knowledge of applicable law

Respondents were asked to perform a self-assessment of their knowledge on infosec-related aspects of criminal [Q5] and intellectual property [Q6] law on a five points scale ranging from "none" to "detailed". Valid responses were 255 for the question about criminal law and 251 for the intellectual property one.

Table 6 below shows the fraction of respondents for each class, and chart 6 the absolute numbers regarding the self-evaluated knowledge of criminal law. The median of the replies was 2 (*scarce knowledge*) and the mode 3 (*some knowledge*).

	Wide community	Core	Peripheral
None	25.9	7.1	44.2
Scarce	29.8	30.2	29.5
Some	30.6	36.5	24.8
Extensive	10.2	19.8	0.8
Detailed	3.5	6.3	0.8

TABLE 1: Knowledge of criminal law (percentages)

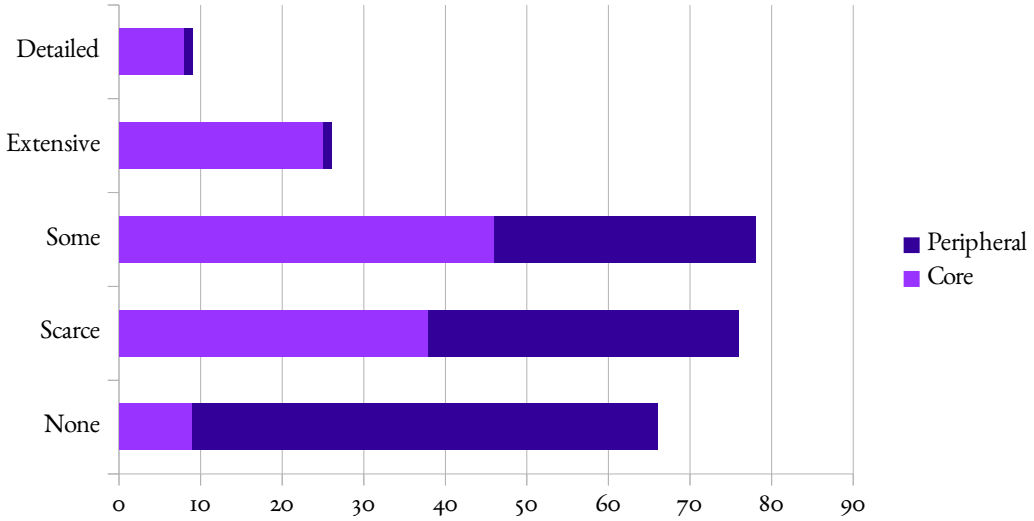

CHART 1: Criminal law knowledge (number of respondents)

In general terms, more than 55 per cent of the "wide" community members recognise a very limited knowledge of criminal law aspects related to information security. Those

assessing their knowledge as *extensive* or *detailed* are less than one-seventh of the sample. The level of familiarity with criminal law appears higher in the "core" group, where the largest subset belongs to the *some* category and the second larger to the *scarce* one, while the *none* and *scarce* categories, in that order, are the most populated for the "peripheral" subset. However, the figures obtained should be in any case a matter of concern.

A simple validation test was performed in [Q15]. We asked the respondents to answer a question about the legal framework that, in our opinion, should be correctly answered by any infosec practitioner with "some" or higher level of knowledge:

> *Is the following statement true or false: "Sending a malware sample for study may be a criminal offence under certain legislations or international agreements."*

Based on the self-assessments of [Q5], a level of correct replies around 44 per cent (for the full set), 62 per cent (for the "core" subset) and 26 per cent (for the "peripheral" subset) should be expected. The assumption showed right for the larger set: 45.9 per cent of the 246 respondents gave the correct answer. Correct replies were somewhat fewer than expected for the "core" subset at 55.3 per cent, while the "peripheral" subset performed better than anticipated at 36.6 per cent. It could be posited that the level of knowledge within the "core" subset may be lower than what the self-assessed values may suggest. This inference is also supported by other cross-matchings of data: it should be expected that a respondent with "extensive" or better knowledge of criminal law should also have an "approximate idea" or better about the Wassenaar Arrangement[9] [Q13b] due to the criminal offences involved in the violation of export controls. However, while 35 respondents fall into the first class, only 10 match both conditions.

Table 8 below shows the fraction of respondents for each class, and chart 6 the absolute numbers regarding the self-evaluated knowledge of intellectual property law. The median of the replies was 2.5 (midway between *scarce* and *some*) and the mode 3 (*some knowledge*).

9 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* is a multilateral export control regime with 42 participating states applicable to transfers of conventional arms and dual-use goods and technologies, established in 12 July 1996 in Wassenaar, The Netherlands. The amendments of December 2013 were widely criticized by security researchers, since the inclusion of a number of infosec tools into the "dual use" lists was seen as impairing the ability to identify and correct security vulnerabilities.

	Wide community	Core	Peripheral
None	18.7	7.2	30.2
Scarce	30.3	28.8	31.7
Something	34.7	36.8	32.5
Extensive	15.1	25.6	4.8
Detailed	1.2	1.6	0.8

TABLE 2: Knowledge of IP Law (percentage)

Intellectual property law includes — but is not limited to — copyright, patents, trademarks and integrated circuit layouts protection law (also known as "mask work"). The respondents assessed their knowledge of that legal framework slightly higher than the same for criminal law, but still low. Almost one-half of the full set reported a very limited knowledge (36 per cent of the "core" subset, 61.9 per cent of the "peripheral" subset). The results seem counter-intuitive, since IP law is by far more broad and complex.

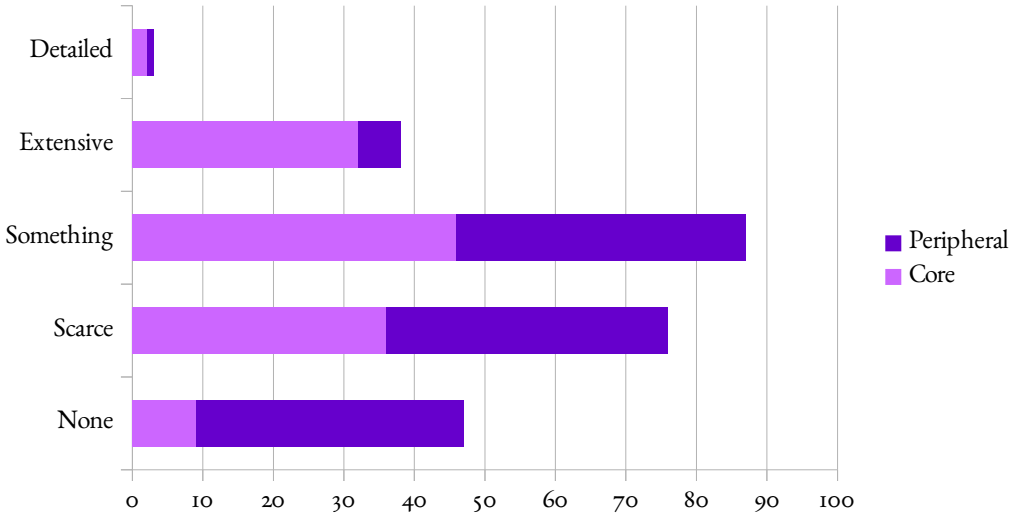

CHART 2: IP law knowledge (number of respondents)

Law as a hurdle

Respondents were asked if their infosec work had ever been affected as a consequence of criminal or intellectual property law [Q7]. Valid answers were *yes*, *no* and *do not know*, and 252 replies were received. Table 9 shows the number of answers and their percentages.

	Wide community	Core	Peripheral

Yes	41 (16.3)	30 (24.0)	11 (8.7)
No	169 (67.1)	76 (60.8)	93 (73.2)
Do not know	42 (16.7)	19 (15.2)	23 (18.1)

TABLE 3: Affected by criminal or IP law (absolute numbers and percentage — percentages may not add to 100 due to rounding)

Even if "affected" does not necessarily mean that the respondents or their employers were sued or prosecuted, a matter that was specifically asked elsewhere (see references to [Q8] below), the number of affirmative answers is highly significant. If the figures for the core group are extrapolated in order to exclude the *don't know* replies, we find that the work of 28.3 per cent of the practitioners that have infosec work as main source of income or other form of deep involvement into the discipline has been affected at least once due to legal issues. That means two of each seven respondents in the subset.[10]

As expected, the "peripheral" subset has experienced less friction with the legal system, a fact that is explained by the features defined for that subset as explained in section *Demographics* above.

The following question, [Q8] was more narrowly focused. Respondents were asked if they or their employers had ever been subject of legal actions due to the infosec activities. Possible answers were the same as in the previous question, and 255 replies were received. Table 9 shows the number of answers and their percentages.

	Wide community	Core	Peripheral
Yes	26 (10.2)	21 (16.7)	5 (3.9)
No	157 (69.4)	81 (64.3)	96 (74.4)
Do not know	52 (20.4)	24 (19.0)	28 (21.7)

TABLE 4: Subject of legal actions (absolute numbers and percentage — percentages may not add to 100 due to rounding)

Again, as expected, the percentage of those targeted by legal actions in the "peripheral" subset is very low — but not negligible. A strong indicator appears in the "core" subset: slightly more than two thirds of those whose work was affected at least once because of criminal or IP law became sued or prosecuted (See footnote 9 above.) That figure may indicate a lack of adequate resources, procedures or knowledge in order to prevent such type of escalation.

Respondents were requested their opinion on the following question [Q9]: *Do you judge that current law is detrimental for legitimate infosec activities?* Possible answers were *yes*, *no* and *do not know*, and 256 replies were received. Table 5 below shows the fraction of respondents for each class, and chart 3 the absolute numbers.

10 Please note, however, that due to the limitations in the sample size of this subset, there is a (reasonable) ± 5 % margin of error at 90 % confidence level.

	Wide community	Core	Peripheral
Yes	28.9	47.6	10.8
No	16.8	15.1	18.5
Do not know	54.3	37.3	70.8

TABLE 5: Current law detrimental to legitimate activities (percentages)

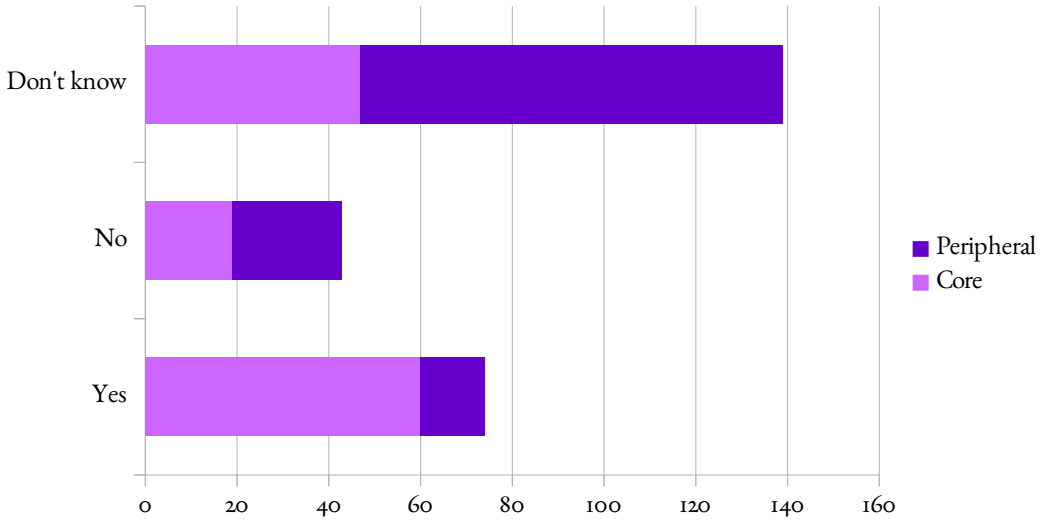

CHART 3: Current law detrimental to legitimate activities (number of respondents)

The figures for *don't know* reasonably correlate in all cases with the sum of those for the two lower levels of law knowledge in section *Knowledge of applicable law* above. A noticeable difference exists between the perceptions of the "core" and "peripheral" subsets. The members of the former consider current law as an obstacle for the development of legitimate infosec activities: when the figures are extrapolated to remove the indecisive replies, three-quarters of the group agree with the "yes" answer. The ample majority of the second subset was unable to give a decisive reply and almost two-thirds of the remainder believe that current law does not pose a significant threat for legitimate infosec activities.

Respondents that answered *yes* to the previous question were asked to rank [Q10a to Q10d] the level of harm created by inadequate laws in several areas of activity using a five-points scale ranging from "not at all" to "block". Questions 10a and 10c were replied by 73 individuals, while the full set of 74 answered the questions 10b and 10d. The areas were *Learning*, *Research*, *Product development* and *Deployment of measures and countermeasures*. Since very few respondents from the "peripheral" subset answered *yes* in Q9, table 6 and chart 4 below show the percentages and quantities for the full ("wide") set.

	Learning	Research	Development	Deployment

Not at all	12.3	3.9	11	13.5
Not much	19.2	15.6	28.8	23
Enough	27.4	29.9	27.4	28.4
Too much	32.9	37.7	26	25.7
Block	8.2	13	6.8	9.5

TABLE 6: Activities affected by current legal framework (percentages)

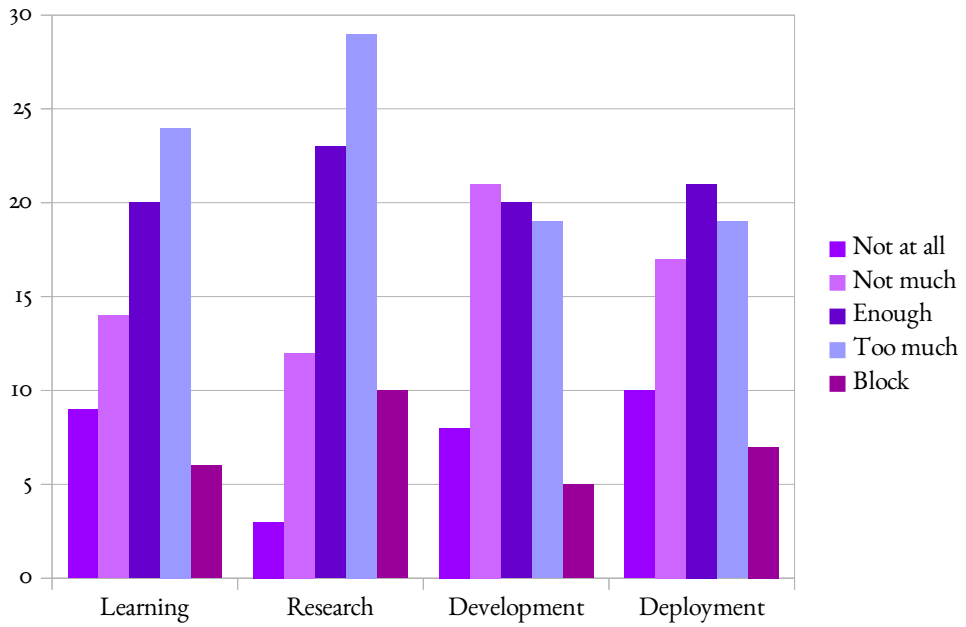

CHART 4: Activities affected by current legal framework (number of respondents)

Research appears as the most affected endeavour: more than 50 per cent of the respondents believe that current legal framework seriously obstructs or blocks the activities in this category. In addition, the number of participants considering this category as not affected at all is remarkably the lowest among all areas — less than 4 per cent. Respondents also show significant levels of concern by the obstacles posed by regulation in the *Learning*, *Product development* and *Deployment* areas, all ranked at approximately similar scales.

Legal counsel

Respondents were asked if they or their employers had resorted to retain legal counsel because of criminal or intellectual property law issues [Q11]. Valid answers were *yes*, *no* and *do not know* and 245 replies were received. Table 7 shows the number of answers and their percentages for each category.

	Wide community	Core	Peripheral
Yes	65 (26.5 pct)	50 (40.0)	15 (12.5)

No	132 (53.9 pct)	54 (43.2)	78 (62.5)
Do not know	48 (19.6 pct)	21 (16.8)	27 (25.0)

TABLE 7: Legal counsel retained (absolute numbers and percentage)

Comparing these replies with those to of question 7 (see table 3) may show that a number of infosec professionals and companies pre-emptively retain legal counsel in order to cut down risks associated to regulation breaches. If figures are adjusted in order to discard indecisive answers, the proportion of practitioners belonging to the "core" subset or their employers having retained counsel is approximately equal to the fraction not doing it.

Participants having answered *yes* to question 11 were asked some additional information about the interventions of legal counsel [Q12a to 12d]. Specifically,

a) If counsel is retained on a permanent or case-by-case basis. Valid answers were *permanent*, *case-by-case* and *do not know* and 88 replies were received.

b) If counsel was useful to solve the issue(s). Valid answers were *yes*, *no* and *do not know* and 100 replies were received.

c) If the performance of a scheduled task became impossible as a consequence of counsel's intervention. Valid answers were the same as in b) above and 98 replies were received.

d) If legal counselling implies a significant cost for the respondents (or their employers). Valid answers were the same as in b) above and 97 replies were received.

Over two thirds of the answers were provided by respondents in the "core" subset: 70 per cent for question 12a, 67 per cent for 12b, c and d. Also, most of the answers from the "peripheral" subset were indecisive. Table 8 shows the number of answers for each question and category. Chart 5 shows the percentages for each category and reply, once adjusted by removing the indecisive answers.

	Wide community	Core	Peripheral
12a. Counsel retaining basis			
Permanent	20	17	3
Temporary	41	32	9
Don't know	27	13	14
12b. Counsel was useful to solve issue			
Yes	49	42	7
No	16	11	5
Don't know	35	14	21
12c. Tasks prevented			
Yes	28	22	6
No	34	26	8
Don't know	36	18	18
12d. Significant cost			
Yes	29	27	2
No	30	20	10
Don't know	38	20	18

TABLE 8: Legal counsel details (number of replies)

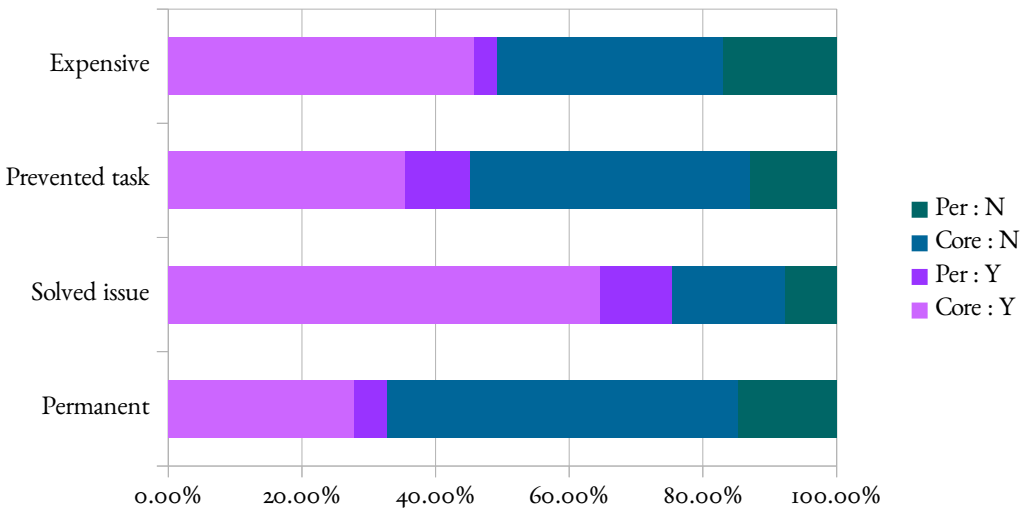

CHART 5: Legal counsel details, adjusted (percentages)

Thus, the adjusted answers point out that:

a) Legal counsel is preferentially retained on a case-by-case basis (67.2 ± 5.7 %).[11]

11 Error margins calculated at 90 % confidence level.

b) Intervention of legal counsel contributed to the satisfactory outcome of the issue in most cases (75.4 ± 6.4 %.)

c) In a significant number of cases (45.8 ± 3.9 %) the solution of the legal issue prevented the performance of a scheduled task.

d) Legal counsel might be considered a significant cost by close to one half of the infosec community.[12]

Multilateral regulations

Respondents were asked to perform a self -assessment on their knowledge of two relevant international treaties: the Budapest Convention[13] and the Wassenaar Arrangement[14] [Q13a and b]. The Convention is a regulatory framework for harmonization of legislative measures on the so called "cybercrime", i.e. criminal offences committed through the use of electronic digital devices, digital communication networks or computer programs as main means of execution. It is also a framework for cooperation among member states for investigation, prosecution and punishment of such offences. On each question respondents were asked "*Do you know the scope of this international agreement?*" on the basis of a 4-point scale: *no*, *by hearsay*, *have a rough idea* and *yes*. Replies were 247 for question 13a and 245 for 13b. Table 9 shows the number of replies for each category.

	Wide community	Core	Peripheral
Budapest Convention			
No	89	34	55
By hearsay	86	36	50
Rough idea	46	29	17
Yes	26	22	4
Wassenaar Arrangement			
No	162	72	90
By hearsay	46	22	24
Rough idea	27	17	10
Yes	10	9	1

TABLE 9: Knowledge of international agreements (number of replies)

In general terms, the figures show that both key multilateral frameworks are very poorly known. Relative percentages for each reply and subset of respondents are shown in chart 6. The "peripheral" subset is in average less knowledgeable in this field than the "core" subset, as seen in table 10.

12 The sample is too little to make an assertion with a reasonable level of confidence.
13 *Convention on Cybercrime* of the Council of Europe, ETS No. 185, Budapest, 23/11/2001. The Convention is open for accession by non-member states. The accession of Argentina to the treaty was enacted into law in November 2017.
14 See footnote [9].

	Core	Peripheral
Budapest	58.9 %	73.4 %
Wassenaar	78.3 %	91.2 %

TABLE 10: Sum of the two lowest categories (percentages)

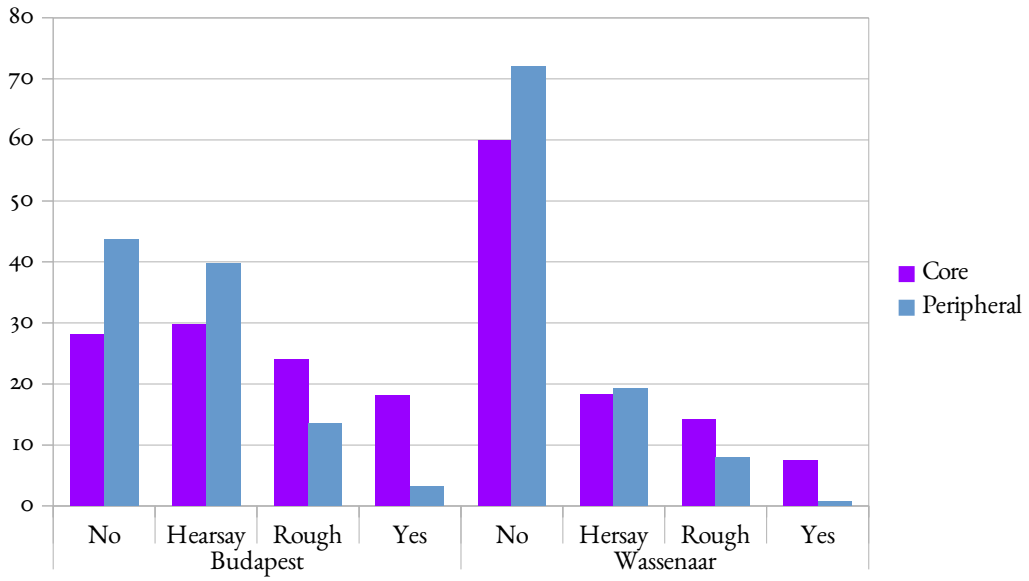

Chart 6: Knowledge of international agreements (percentage)

Lawmakers

Respondents were asked their opinion about the lawmakers' understanding of information security issues. The question was "*Do lawmakers understand or are adequately advised on information security issues?*" and the valid answers were *no*, *a little*, *enough* and *yes*. We received 238 replies; the median and the mode were both equal to 1. The consensus seems to be that lawmakers are not knowledgeable nor well advised on the matter, as table 11 and chart 7 show.

	Wide community	Core	Peripheral
No	73.9	72.7	75.2
A little	23.1	24	22.2
Enough	2.1	1.7	2.6
Yes	0.8	1.7	0

TABLE 11: Are lawmakers knowledgeable about infosec? (percentage of replies)

There are no relevant differences between the subsets, a fact that becomes no surprise considering that according to the information collected during qualitative surveys done in parallel with this one the formal contacts between the infosec community and the lawmakers tend to be very rare.

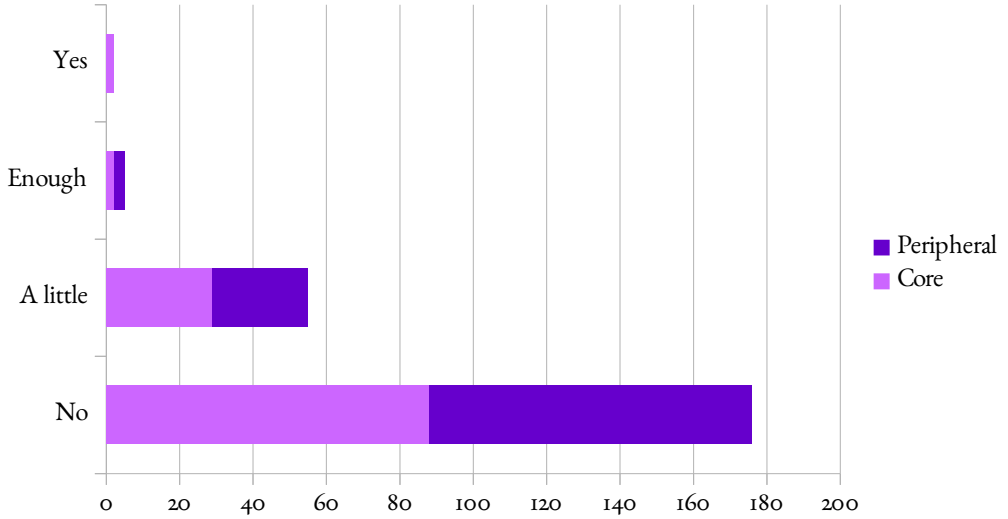

CHART 7: Are lawmakers knowledgeable about infosec? (number of respondents)

Conclusions

Based on the collected replies, it is possible to conclude with reasonable statistical confidence that:

1. The knowledge about fundamental laws and regulations that affect the field is poor in a relevant fraction of the infosec community. There are enough reasons to believe that the community self-perception about such knowledge is somewhat biased towards believing to have greater skills in that area than they really possess.
2. Full time information security practitioners
3. About one in five infosec practitioners or their employers has been subject to legal actions because of their trade. Correlation with the occurrence of less cumbersome legal issues may indicate inadequate preparedness.
4. The community tends to believe that the current regulatory framework is detrimental for the performance of legitimate infosec activities. Research is considered to be the most threatened field of activity.
5. About one in two infosec practitioners or their employers have retained legal counsel because of criminal or intellectual property law issues. Legal counsel is more often retained on a temporary, case-by-case basis. Such counsel has helped to satisfactorily solve the issue three-quarters of the time, but in some cases the practitioners or their employers were forced to stop planned tasks in order to achieve the satisfactory outcome. The cost of legal counsel may be considered as high by about one half of the community.
6. Key international agreements that affect infosec activity are very poorly understood by the community. The Wassenaar Arrangement is very rarely known.
7. There is a consensus in the community about the lawmakers' utter lack of understanding of, or proper advice on information security issues.

Future work

For us at *Vía Libre*, researching on the information security community largely exceeds the sociological or anthropological interest. The ours is fundamentally an advocacy organisation doing non-partisan politics in that barely explored area where digital technologies interact with fundamental rights and freedoms. This work should be considered just a first step towards better policymaking in the information security field, so that the actions of the states and the private sector in adopting policies and

regulations to protect their legitimate interests don't be at odds with the aims of protecting the human rights and fostering the research in the digital space. Consequently, there is a good lot of things to do:

- More useful information can be extracted from the trove of available data, which could study the behaviour of certain variables in correspondence with demographical data.
- An informal space for discussion of policy issues related to infosec seems to be a necessary step, encouraging the participation of relevant stakeholders in the field. That space could also be useful to devise strategies for a closer relationship with the policymakers.
- The research about the relationships between the infosec community and the lawmaking and law enforcement agencies will not be complete if the other side of the equations is not also investigated. A process for surveying "the other side" should be conceived and carried out.
- This type of survey should be adjusted on the basis of the lessons learned[15] during the study and repeated if feasible, polishing the current topics and possibly adding new ones.
- Supplementary tasks were conducted in parallel with this study, including a series of video-recorded interviews and a relaxed but idea-rich meeting with some of the most relevant infosec community stakeholders. The resulting materials should be processed and consolidated with an enhanced revision of this study.

Acknowledgements

This work would not have been possible without the contributions of a large number of individuals and organisations. We must thank the *ekoparty* organisers and staff, and in particular Federico Kirschbaum, Francisco Amato and Paola Mastrángelo; the anonymous respondents to our survey; the information security experts that 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, a lioness doing the field work for this survey; and AccessNow, for their generous support of this work.

15 For instance, adding more control structures into the questionnaires in order to check self-assessments will be useful. In this survey, we used Q15 as a correcting code for possible bias in the answers to Q5 (knowledge of criminal law).