Participatory drafting of the

NATIONAL CIBERSECURITY POLICY:

TOWARDS A NEW REGULATORY FRAMEWORK FOR CHILE

Pablo Viollier

1.

INTRODUCTION

Cybersecurity is an increasingly relevant issue both for public and private institutions. Once pertaining almost exclusively to IT specialists, cybersecurity has now become the focal point for public policy debate among scholars, corporations, journalists, and civil society. The increased sophistication, scope, and frequency of cyberattacks has drawn public attention to the issue of cybersecurity, which is of strategic importance for government agencies and an aspect of utmost priority for the sustainability of many web-based corporation business models.

Chile is no exception in this regard. Our country has been subject to several international cyberattacks, with at least 270 detected cases of infected computers in Chile during a string of ransomware attacks in May of 2017.[1] The increasing number of cybercrimes has also been the subject of much debate: according to data from the Undersecretariat of Internal Affairs, during the first semester of 2017 a total of 23,928 cybercrimes were reported. Only 517 of these cases are actual computer-related offences; i.e. those specified under Law 19,223. The remaining 23,411 cases are related to the fraudulent use of debit and credit cards (La Tercera, 2017).

Additionally, revelations on mass government surveillance, like the one uncovered by Edward Snowden in June 2013, have motivated a growing consensus on the need for a more open, democratic, and safe internet, in order to adequately promote freedom of expression, stimulate the economy, benefit from cultural heritage, and encourage the exchange of ideas.

Thus, there is an evident need to establish national policies that may serve as a clear guiding point for the design and implementation of measures aimed at protecting the security and rights of internet users in cyberspace.

To achieve this, examining our country's own particular characteristics is essential, since this will point to the specific challenges we must face regarding cybersecurity. In this regard, one of the aspects to consider is geography: given Chile's long and narrow dimensions, it is less costly to map a single North-to-South optic fiber distribution, making it more difficult to ensure network redundancy, interconnection between providers, and availability of backup routing agreements (José Miguel Piquer, 2015). In order to face these challenges in a coordinated and systematic way, the Chilean Government decided to draft a National Cybersecurity Policy (PNCS form the Spanish acronym for Política Nacional de Ciberseguridad). After a discussion process between government agencies that included hearings and public consultations, the PNCS was officially adopted on April 27 this year (Undersecretariat of Defense, 2017).

This report aims to discuss the impact of the participation of the various parties involved in the policy-making process. Therefore, we will discuss the comments submitted by these contributors during the public consultation for the drafting of the PNCS. Differences between the draft and final version of the PNCS will also be discussed in order to identify any amendments that might have stemmed from recommendations made by participants.

---

1 El Mercurio, "Sigue creciendo el alcance del ciberataque: 270 detecciones en Chile y 75 mil a nivel mundial", May 12, 2017, http://www.emol.com/noticias/Tecnologia/2017/05/12/858167/Sigue-creciendo-el-alcance-del-ciberataque-270-detecciones-en-Chile-y-75-mil-a-nivel-mundial.html (Reviewed on October 10, 2017)

The first section of this report briefly provides details of the PNCS, the motivations behind its creation, the political objectives for 2022, the public policy measures designed for the 2017-2018 period, and the proposed institutional framework for its implementation.

The second section describes the participatory process for the PNCS' drafting and discusses its levels of inclusivity, transparency, and openness. This is complemented by an academic literary review of multi-participatory digital public policy design. This section also describes the participatory process both for the hearings and public consultation phases, as well as analyzes its level of inclusivity, transparency, and openness.

The third section classifies the participants for the PNCS's public consultation into categories: civil society, private sector, public institutions, academia, tech groups, and individuals. The comments are then analyzed by category in order to identify what topics participants placed most emphasis on when proposing amendments.

The fourth section provides details on the major modifications made to the draft document by comparing it to the final version of the PNCS. This section also provides examples of participant comments that match the amendments seen in the final version of the document.

The fifth section focuses on describing the participants' impressions regarding the level of openness and inclusivity of the PNCS's participatory process and to the extent to which participants felt their comments and contributions where included in the final document.

Finally, we present conclusions and recommendations regarding the PNCS's drafting and explain its instructive value for future drafting processes of digital public policies.

2.

METHODOLOGY

The purpose of this report is to discuss how the participation of various contributors impacted the PNCS's policy-making process. To perform such an analysis, certain methodological challenges must be addressed.

The participants are the first object of analysis and were classified into six participant categories.[2]

Then, there were certain methodological challenges when trying to select a method capable of measuring the impact of the participants' contributions and comments on the amendments made to the PNCS draft that later resulted in the final version of the PNCS. In order to determine causation between comment content and the consequent modification of the draft, it is not sufficient to compare between the draft PNCS, participants' comments and the final PNCS; in fact, whenever an amendment appears to have been taken literally from a specific participant comment, an external viewer cannot positively assure that such amendment was due only to that specific comment and not to another factor.

Due to this issue, we decided to divide the analysis of this participatory process into three phrases. The first analytical phase focuses its analysis on comment content per participant category. This allowed us to separate specific topics that were prioritized by participants of a specific category during their contributions. The second analytical phase provides details of anecdotal cases showing a strong correspondence between amendments made on the draft PNCS and some of the participants' comments. The selected amendments aim to represent at least one case per category.

Finally, in order to add a qualitative element to this analysis, we collected the participants' impressions about the process' openness, transparency, and inclusivity, as well as their impressions about the extent to which they believe their contributions were included. These impressions were collected during a meeting held on July 7, 2017 at the offices of Derechos Digitales, with a representative number of PNCS public consultation participants.

---

2 Some methodological precautions were taken in order to be able to classify certain participants that didn't belong in a specific category or participants with activities that fell within multiple categories.

3.

NATIONAL CYBERSECURITY POLICY

3.1 *Inter-Ministerial Cybersecurity Committee*

The need for a National Cybersecurity Policy was mentioned in President Michelle Bachelet's government program, which states "It is important [today] that we consider developing a digital security strategy for the protection of private and public users against possible data source violations, as well as for the protection of our citizens' privacy."[3]

In order to deliver on such a promise, the Inter-Ministerial Cybersecurity Committee [PV1] (CICS from the Spanish acronym for Comité Interministerial sobre Ciberseguridad) was created on April 27, 2015 by way of the Supreme Decree No. 533 of 2015.[4] According to Article 1 of this Decree, the purpose of this Presidential Advisory Committee is to propose a National Cybersecurity Policy and to advise in the coordination of actions, plans and programmes of the different institutional contributors in the matter. For the fulfillment of this task, the CICS had the following functions and attributions:

- Advise the President of the Republic on the analysis and definition of the National Cybersecurity Policy, which will contain the specific measures, plans, and programs to be applied for its implementation and compliance.
- Identify any current or potential threats in cyberspace and propose actions aimed at overcoming possible security breaches and monitoring their implementation.
- Analyze and propose organizational structure alternatives for Chile's cybersecurity.
- Analyze and study cyberspace-related legislation in force to propose appropriate constitutional, legal, and regulatory amendments.
- Propose ways of coordinating efforts between public and private sectors to the Government.

In order to fulfill its purpose, and in accordance with Article 3 of the Decree, the Committee is composed of permanent representatives and guests from the following institutions:

- Undersecretariat of Internal Affairs
- Undersecretariat of Defense
- Undersecretariat of Foreign Affairs
- General Undersecretariat of the Presidency
- Undersecretariat of Justice
- Undersecretariat of Economy

---

3 Michelle Bachelet "Programa de Gobierno Michelle Bachelet 2014-2018" (Chile, 2014), page 57, http://www.subdere.gov.cl/sites/default/files/programamb_1.pdf (Reviewed on October 10, 2017)

4 Available at: https://www.leychile.cl/Navegar?id-Norma=1079608&idParte= (Reviewed on October 10, 2017)

- Undersecretariat of Telecommunications
- National Intelligence Agency
- Undersecretariat of Finance, as an invited guest

The Ministries of Security, Defense, and Internal Affairs presented a joint publication on March 2015 entitled "Bases for a National Cybersecurity Policy", which is aimed at establishing the need for a PNCS, the main elements for the future PNCS, and a timeline.

3.2 *PNCS Objectives and Content*

Four objectives are established in the final version that justify the drafting of a National Cybersecurity Policy:

- Preserve people's safety in cyberspace
- Protect the country's security
- Promote collaboration and coordination between institutions
- Manage cyberspace risks

In order to achieve these objectives, the PNCS content is divided into three sections: policy objectives for 2022, functions and institutional framework, and public policy measures for 2017-2018.

3.2.1 *Policy Objectives for 2022*

This section establishes the general guidelines the PNCS intends to adhere to by 2022, as well as the secondary objectives required to achieve them.

The first objective is to have a robust and resilient data infrastructure that can withstand and recover from cybersecurity incidents from a risk management point of view.

For this objective to be achieved, the PNCS deemed the following as necessary: 1) establish technical measures to prevent, manage and overcome risks as soon as they are verified in order to protect data infrastructure, 2) identify and prioritize critical data infrastructures, 3) have cybersecurity incident response teams, 4) establish standardized mechanisms for reporting, management and incident recovery, and 5) establish distinct cybersecurity standards.

The second objective establishes that the State must protect people's rights in cyberspace. For this the following is deemed necessary: 1) preventing illicit acts and confidence-building in cyberspace, 2) establishing priorities in the implementation of punitive measures, 3) the existence of multi-sector prevention, and 4) the respect and promotion of fundamental rights. The third policy objective for the year 2022 is for Chile to develop a cybersecurity culture, in terms of education, good practices and a responsible use of digital technologies, by 1) creating a cybersecurity culture, 2) raising awareness and informing the community, and 3) educating people on the subject of cybersecurity.

The fourth objective establishes Chile's need to foster cooperative relationships with other concerned parties related to cybersecurity, as well as actively participate in international discussions, and forums by

1) establishing an international policy on the subject of cybersecurity, 2) cooperating and being of assistance on international grounds, 3) participate more actively in multilateral forums involving multiple stakeholders, and 4) developing international regulations to promote confidence and security in cyberspace.

Lastly, the fifth objective establishes that the country should promote the development of a cybersecurity industry that serves its strategic interests through 1) innovation and development in the field of cybersecurity, 2) develop a component of cybersecurity within the ICT sector, 3) perform studies in order to typify the industry and identify strategic domains, 4) creation of new services by the local industry, and 5) creation of a public sector demand based on the State's strategic interests.

3.2.2 *Functions and Institutional Framework*

The CICS, in its capacity, was tasked with proposing organizational structure alternatives for Chile's cybersecurity. To this end, the PNCS pointed out that the organizational structure in cybersecurity matters will be subject to law and it must be presented by the institutional actors responsible for cybersecurity, without explicitly stating which ones. The creation of an advisory council for multi-sector integration was also proposed.

While this cybersecurity bill is being discussed within the Government and Congress, the PNCS is proposing to temporarily extend CICS's mandate, as well as its communicational, coordination, and monitoring of measures outlined in the PNCS. As for managing incidents within the Government Connectivity Network, the proposal is that this function be temporarily assumed by the Government's Computer Security Incident Response Team (CSIRT).

The fact that the decision on which institution would be responsible for cybersecurity within the public sector was postponed may respond to a lack of consensus within the process. However, it should be noted that this element constitutes a shortcoming of the PNCS, especially given the fact that institutional definitions are key for defining clear political responsibilities at the moment of implementation, and that such definitions in cybersecurity strategies of other countries in Latin America.

3.2.3 *Public Policy Measures for 2017-2018*

This section of the PNCS establishes 41 "short-term" public policy measures to be implemented during 2017 and 2018. The proposed measures are presented in a table, which briefly outlines the content of the measure, the institutions responsible for its implementation, and the objective they relate to.

Short-term measures are limited to 2017 and 2018 so as to coincide with the current government's term period. There is, however, no prioritization of the proposed measures and no system of indicators to monitor compliance is proposed. Finally, no concrete monitoring or budgetary analysis mechanism was created, as it was for the 2020 Digital Agenda process.[5]

---

5 Available at: http://www.agendadigital.gob.cl/#/seguimiento/

4.

PARTICIPATORY PROCESS AND DEGREE OF INCLUSIVITY, TRANSPARENCY, AND OPENNESS

4.1 *The Importance of Multi-Sector Participation*

There is a growing trend in specialized literature to highlight the need for digital public policy development to be carried out through participatory and multi-stakeholder processes.

This is due, in part, to the importance of a holistic approach to cybersecurity strategies encompassing economic, social, educational, legal, technical, diplomatic, military, and intelligence-related aspects (OECD, 2012).

In this sense, the participation of various stakeholders makes it more likely that the draft and implementation of national cybersecurity policies are in line with fundamental rights, such as privacy, freedom of expression, and due process, as well as with the technical principles governing the Internet up to today, such as openness, universality, and interoperability (Maciel, Foditisch, Belli and Castellón, 2016).

Given that most Internet infrastructure is either privately owned or managed by non-governmental technical organizations, the implementation of a multi-stakeholder model is not only an alternative, but a necessity (Álvarez and Vera, 2016).[6]

4.2 *Hearings Phase*

Early in 2015, after the publication of the document entitled "Bases for a National Cybersecurity Policy,"[7] the CICS held a series of public hearings and invited several participants to comment on the document, to respond to various concerns the CICS had, and to propose topics that weren't included in the document. The public hearing sessions were attended by, among others:[8]

- Office of the Public Defender
- DuocUC (University)
- Public Prosecutor's Office of Chile
- País Digital Foundation
- NIC Chile (Entity in charge of administrating domain names)
- Derechos Digitales (Digital Rights)
- Judicial Branch
- Investigative Police
- Internal Revenue Service

---

6 It is worth mentioning that both authors were members of the Inter-Ministerial Committee on Cybersecurity.

7 Available at: http://ciberseguridad.interior.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADti-ca-Nacional-sobre-Ciberseguridad.pdf (accessed on October 10, 2017)

8 Information available at: http://ciberseguridad.interior.gob.cl/participacion/ (accessed on October 10, 2017)

4.3 *Public Consultation Process*

Based on the document entitled "Bases for a National Cybersecurity Policy" and the opinions and recommendations gathered in the public hearings phase, the CICS prepared the first draft of the PNCS, which was published in February 2016.[9]

This draft was submitted to public consultation between February 29 and March 18, 2016, pursuant to Law 20,500 on Associations and Citizen Participation in Public Administration. Comments were submitted through an online form where participants had to identify themselves and the institution they represented. The form consisted of two open-ended questions, a general one related to the document and another requesting the person to point out factual or assessment errors. Afterwards, there was a blank space for comments on each of the five strategic core areas, the institutional scheme, and the public policies measures for 2017-2018.

Once the public consultation process was completed, the comments made by the participants were made public on the website of the CICS.[10]

4.4 *Degree of Openness, Transparency, and Inclusiveness of the Process*

A previous publication (Lara and Viollier, 2017) noted, there are two main obstacles to the participation of several parties in collaborative processes of digital policy-making in Chile. On the one hand, the fact that many organizations do not have enough resources to participate in public consultation processes. On the other, the fact that many organizations feel that their participation in those processes is not justified, considering that their proposals were not dully considered in the past, or that the processes do not succeed.

In that regard, several elements that show a genuine interest from the CICS in generating a truly participatory process should be highlighted. Among them, the fact that the first draft was prepared taking into consideration elements provided by different participants in the public hearings, the efforts of the Committee to facilitate the participation of organizations located in certain regions (even though hearings were not held in those regions), the fact that the public consultation was open to all types of participants, and that the comments were fully published, pointing out the corresponding organization.

Among the aspects that can be improved, we believe that participation in the process was undertaken bilaterally between the Committee and the participants, without formal bodies of collective participation aimed at sharing and discussing different points of view.

---

9 Document available at: http://ciberseguridad.interior.gob.cl/media/2016/02/Borrador-Consulta-P%C3%BA-blica-PNCS.pdf (accessed on October 10, 2017)

10 Available at: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/ (accessed on October 10, 2017)

5.

PARTICIPANTS AND COMMENT CLASSIFICATION IN THE PUBLIC CONSULTATION PROCESS

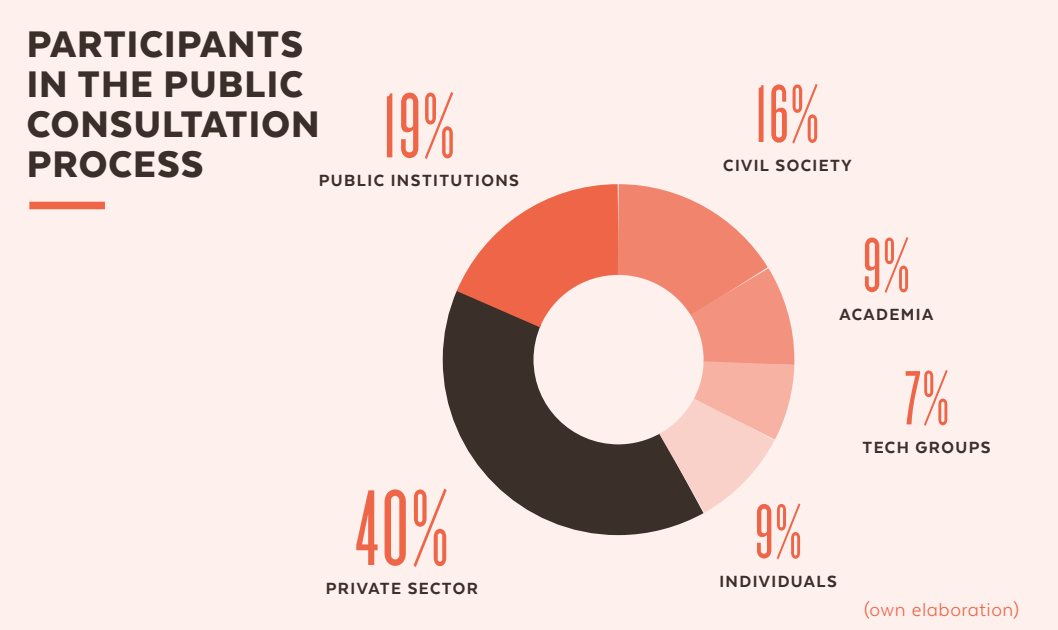
5.1 *Participants*

Forty-three organizations participated in the public consultation process; a significant number compared to previous public consultation processes on the matter of digital public policies. For this analysis, participants were divided into six categories: civil society, private sector, public institutions, academia, tech groups, and individuals.

Some of the participants were difficult to classify, because their nature could coincide with different categories. Such is the case of the University of Chile, which is an academic institution with the legal nature of a public institution, and within which various tech groups operate. Finally, it was categorized as an academic institution, while the bodies that operate within it, such as NIC Chile and the CLCERT, were classified as tech groups. Similarly, even though the legal nature of the País Digital Foundation is a non-profit organization, it was classified under the private sector category, as it advocates for the industry's interests. Finally, four people submitted comments personally, without representing any organization. These four participants were left uncategorized, even if it seems likely that they belong to some of the five categories mentioned above.

Thus, out of the 43 participants, four belong to the academia, three to tech groups, 17 to the private sector, eight to public institutions, seven to civil society organizations, and four are individuals.

TABLE 1:



As is noticeable, the participation of companies was prevalent in the public consultation process. This can be explained, on the one hand, by the strategic character of cybersecurity for companies that depend on the internet to maintain its business model and, on the other hand, by the fact that companies have greater human and economic resources which allow them to afford their participation in consultations of this type. The participation of public institutions is also important, which could also be the result of the resources they have available and their institutional interests.

Tech groups had the lowest percentage of participation. This may be due to the lack of resources and institutional strength of their organizations, as well as the fact that the PNCP was a legal document on public policy, with a language that may not be as familiar to members of those groups.

5.2 *Analysis by Comment Category*

As mentioned before, an external observer cannot identify a causal connection between a comment and a specific amendment made to the PNCS draft. Therefore, the comments must be made into the very object of the analysis in order to understand the priorities and emphasis participants had during the public consultation, and, thus, identify which topics were prioritized when trying to influence the final version of the PNCS for each category.

TABLE 2:

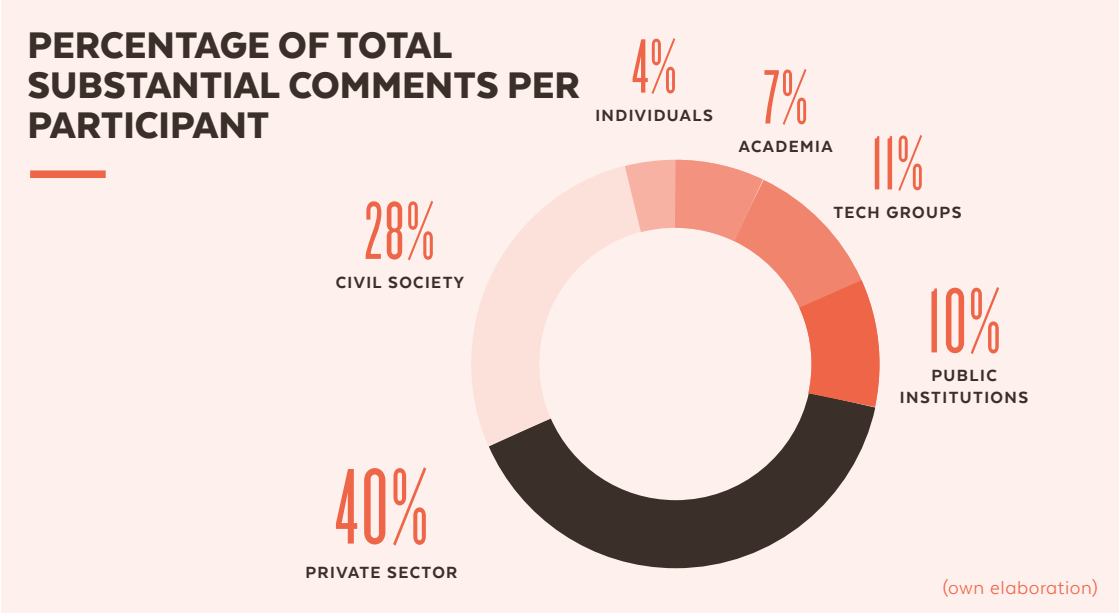
PARTICIPANT	# PER PARTICIPANT	INFRASTRUCTURE	CRIME PREVENTION	PROTECTION OF FUNDAMENTAL RIGHTS	EDUCATION	INTERNATIONAL COOPERATION	CYBERSECURITY INDUSTRY	INSTITUTIONAL FRAMEWORK	TOTAL COMMENTS PER PARTICIPANT
Academia	4	1	1	2	2	1	2	2	11
Tech Groups	3	3	2	3	3	1	2	3	17
Public Institutions	8	4	3	2	1	2	1	3	16
Private Sector	17	15	9	2	11	8	7	10	62
Civil Society	7	7	5	4	7	7	6	7	43
Individuals	4	0	1	1	1	1	0	2	6
Total Comments		30	21	14	25	20	18	27	155

For that purpose, over 400 comments that were submitted by the 43 participants during the public consultation process were analyzed, as well as the core topics that triggered most comments or that evidenced a clear interest in the topic.[11] The core topics considered were those established by the PNCS, which will be named, for simplicity as: infrastructure, cybercrimes, protection of fundamental rights, education, international cooperation, cybersecurity industry, and institutional framework. It is worth mentioning that core topic B of the PNCS was divided into two topics: cybercrime and protection of fundamental rights, since a great percentage of comments in that regard were addressed as individual topics.

As is noticeable, the private sector provided the highest number of substantial comments during the public consultation process. This might be due to the number of participants in that category (40%). In addition,

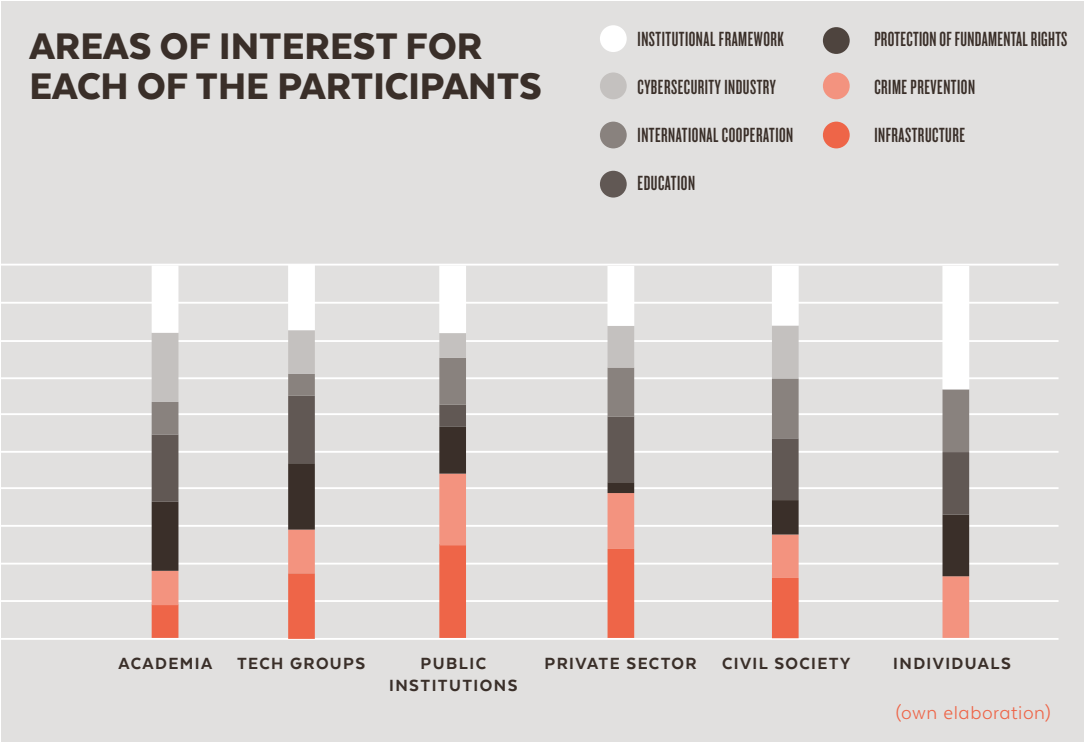
11 In this regard, it is important to point out that comments were only taken into account when the person showed an actual interest in elaborating on the topic. Comments that were simply formal or casual will be considered null in this analysis. As shown in Table 2, the number of comments considered "substantial" totals 155.

TABLE 3:



civil society, although showing a proportionally smaller participation in terms of the number of participant institutions (16%), submitted a significant amount of substantial comments (43). Conversely, the academia only provided 11 substantial comments overall.

TABLE 4:



The above statement can be observed more clearly by showing the number of substantial comments per participant expressed in percentages. Hence, the private sector maintains a percentage of participation that is proportional to the amount of participants in the consultation process. In addition, the number of substantial comments made by civil society is proportionally higher than its participation, in terms of the number of participant institutions. This means that, on average, civil society organizations made more substantial comments than the other participants. The same happens, although to a lesser extent, with the participation of the tech groups.

Finally, the academia and public institutions made on average less substantial comments compared to the amount of participants in the process.

Data in Table 2, shows what areas each category of participants expressed most interest in.

In the results, it is worth mentioning that, in the comments provided by public institutions and the private sector, a considerable emphasis was put on the core topic of infrastructure. Moreover, academia, tech groups, and public institutions were the participants that put most emphasis on the core topic of fundamental rights.

Something that stands out is the fact that civil society made more substantial comments on infrastructure, education, crime prevention, and international cooperation, than on the core topic of fundamental rights.

Finally, the lack of attention the private sector paid to the topic of fundamental rights is extremely worrying. Future qualitative research should delve into the possible causes for this apparent lack of interest.

6.

DIFERENCES BETWEEN THE DRAFT AND FINAL VERSION OF THE PNCS

This section describes the parts that were added to the final version of the PNCS, which parts were removed from the draft, and which parts were re-examined. While the comparison between the draft and the final version of the PNCS shows substantial amendments, it is difficult to assign a particular change to a specific comment.

Finally, the comments that seem to coincide with specific amendments are presented, which might suggest a certain impact of multi-sector participation in the final version of the PNCS.

6.1 *Major additions*

Regarding Objective A of the policy for the year 2022, a definition of cybersecurity was added and it established that the enhancement of surveillance capacity by the state or a private entity does not fall within the framework of cybersecurity. Moreover, a reference was added regarding the need to monitor the security of sensors and devices operating from within cyberspace. Related to cybersecurity incident response teams, the final version promotes the creation of sectorial CSIRTs. Finally, a remark on the need to promote reporting of cyber vulnerabilities by users and experts was added, avoiding unnecesary collection and processing of data that might violate the privacy of individuals.

The main amendment to Objective B was the change of title, from “The State shall ensure people’s rights in cyberspace through the prevention and effective punishment of crimes, thus ensuring full respect for human rights” to simply “The State shall ensure people’s rights in cyberspace” in the final version. This change is positive, since previous phrasing seemed to suggest that the only way the State ensures people’s rights in cyberspace (or at least the most relevant way) is through the effective punishment of crimes, even though this is only one among several ways to protect people’s rights in a digital environment.

Another crucial element that was added to this objective is an explicit reference to the importance of encryption technologies, by stating that the measures based on this policy shall promote point-to-point encryption. Similarly, it states that no person or organization shall be subject to the obligation of implementing “backdoor” mechanisms. However, no reference to the possibility of the State incurring in hacking activities or its possible regulatory framework was added.

Finally, a reference is added stating that, regarding fundamental rights, the rights of vulnerable groups shall be especially considered, and that this topic will be analyzed and implemented using a gender perspective. However, there are no clear parameters defining how this gender perspective is perceived other than just the inclusion of the term.

Objective C of the policy has no substantial additions.

Objective D of the policy has an additional reference stating that the adhesion to the Cybercrime Convention shall be made with reservations and precautions consistent with the PNCS.

Objective E of the policy for the year 2022 has no significant additions.

6.2 *Amended paragraphs*

The first paragraph of Objective A of the policy for the year 2022 is restated by pointing out the importance of establishing prevention and risk management models, in order to prevent, manage, and recover from cyberspace threats once these are verified.

Objective B of the policy for the year 2022 was also amended, particularly in its section concerning the respect and promotion of fundamental rights. Current wording establishes that all measures proposed by the public policy shall be designed and executed through a fundamental rights approach. Regarding this aspect, it is worth mentioning that no criteria was established to define a fundamental rights approach or at what point said standard would be breached. This weakens the ability to use the PNCS as a mechanism to measure whether future public policy is inconsistent with the fundamental rights approach that is sought to be established.

Finally, temporary governance in cybersecurity is reframed, by extending the existence and the mandate of the CICS with respect to its communication, coordination, and follow-up functions for the PNCS measures. However, functions identified as essential to the creation of the new public service in charge of cybersecurity are established in less precise terms.

6.3 *Incorporated comments*

Below are some examples of representative comments made by each category of participants, which appear to have been incorporated directly into the final version of the PNCS:

Tech Groups:

(1) The definition of the National CSIRT should include, among its objectives: promoting the creation of new sectorial CSIRTs [...] and also support/cooperation once they are operative.

(2) The policy should also mention the promotion of and regulatory support for responsible reporting and notification of software vulnerabilities by citizens to the organizations responsible for their development, through clear and public mechanisms that include the technical support from the National CSIRT [...].[12]

These comments appear to have been taken into account for the final version of the PNCS in the fifth paragraph of item 4 of Objective A (page 17) and in the fifth paragraph of item 5 of the same objective, respectively (page 18). However, despite having been depicted in the objectives of the policy for 2022, they were not included in the policies to be implemented during the 2017-2018 period.

Civil Society:

(1) "A reasonable objective for the year 2022 policy should be to ensure the rights of people in the digital environment and within that objective, one of the measures should be ensuring people's rights by fighting cybercrime. Based on the wording of the objective, it seems as if preventing and punishing crimes was the only way the PNCS plans to ensure people's rights in cyberspace."[13]

---

12 Comment by the CLCERT, University of Chile. Available at: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

13 Comment by Derechos Digitales. Available at: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

This comment seems to have been included in the amendment to the title of Objective B of the policy for the year 2022, as previously commented.

Academia:

(1) "I would include the specific topic of cryptography and electronic signatures. If we manage to spread its widespread use, we would achieve a great level of security for all of our data and documents."[14]

This comment seems to have been included in a new paragraph of item 1 of Objective B for the year 2022, which points out that the "widespread adoption of digital certificates (digital signature) will be promoted on websites and by individuals and organizations, as a way to ensure the communications and identity of users."[15]

Public Institutions:

(1) "A study of new institutionalism is recommended, without delving into specific design, both organic and functional, as that is a matter that must be defined in a corresponding bill."[16]

This comment seems to have been included in the paragraph on the institutional framework for cyber-security (page 25), which was reworded to establish the functions of the proposed new public service in charge of cybersecurity less specifically. However, nothing prevents the Committee from proposing clearer guidelines for the relevant bills.

Private Sector:

(1) "We believe that, due to the dynamic nature of cybersecurity, an addition should be made indicating that risk assessment initiatives must be updated regularly as an ongoing process."[17]

This comment appears to have been incorporated in a new paragraph in Objective A of the policy for 2022, which states that "Based on the policy, models for the prevention and management of risks in cy-berspace, or physical risks affecting it, will be created and updated regularly under a model of continuous improvement."[18]

---

14 Comment by José M. Piquer Gardner on behalf of the University of Chile. Available at: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

15 National Policy on Cybersecurity, page 19.

16 Comment by the Ministry of the General Secretariat of the Presidency. Available at: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

17 Comment by Microsoft Chile S.A. Available at: http://ciberseguridad.interior.gob.cl/con-sulta-ciudadana/

18 National Policy on Cybersecurity, page 16 (emphasis is ours).

7.

PARTICIPANTS' IMPRESSIONS ON THE PARTICIPATORY PROCESS

In order to add a qualitative analysis on the impact of multi-sector participation in the outcome of the National Cybersecurity Policy, a working meeting was held on July 7, 2017 at the offices of Derechos Digitales, to gather impressions on the process from a representative number of people who participated in it. Three civil society organizations (including Derechos Digitales), two public institutions (including a representative of the CICS), two members of tech groups, one academic, and no representative of the private sector participated in the meeting.[19]

With regard to the public consultation process, there was consensus on the participatory aspect of the process, particularly when compared to similar previous processes. Emphasis was placed on the fact that comments were published in a nominative form and, overall, most of the attendees felt that, to a certain extent, some of their comments were included in the final version of the PNCS. Many participants expressed their concern about that same spirit being maintained during the implementation stage, in particular due to the lack of a monitoring body for such measures.

In this regard, several participants pointed out that the way the public consultation process was conducted in the PNCS should be transformed into a new minimum standard of participation. However, members of civil society organizations stressed that these matters must be brought closer to institutions that are less specialized in cybersecurity matters, but that may still be affected, such as user and consumer organizations.

Finally, an interesting discussion came up about the need to allow input in a private and confidential manner, since advertising may refrain certain interested parts from sharing sensitive information.

---

19 Participants were invited to the meeting in a proportion that was representative of their participation in the process. Unfortunately, no representative of the private sector could participate.

8.

CONCLUSIONS AND RECOMMENDATIONS

Cybersecurity is a complex, multidisciplinary, and multi-sector phenomenon. This justifies, and to a certain extent makes it a requirement that public policy regarding cybersecurity should be carried out through processes including several concerned parties.

This modality allows different views and approaches to be considered, as well as to collect all the necessary background required to make evidence-based policies. Multi-stakeholder participation does not only make processes more open, transparent, and democratic, but also has the potential to improve their quality, especially on systemic issues involving various factors, such as cybersecurity.

In this regard, the process of designing Chile's National Cybersecurity Policy is a positive case study regarding the influence of multi-stakeholder participation on the outcome of public policies on cybersecurity.

The analysis of the participant's input and their nature shows that there is a predominance of private and government participation, which is probably explained by the greater resources that these institutions have, as well as a possible bias in the identification of relevant participants.

The study of the comments shows that while several public institutions participated, they only did so in a limited amount of topics, probably related to their fields of competence. Similarly, the lack of companies' participation in the fundamental rights topic is worrisome.

The comparison of comments between the draft and the final version of the PNCS suggests that several comments were included almost directly.

The overall impression about the process among the participants is positive, especially concerning its degree of openness, transparency, and inclusivity. However, there are still concerns that the implementation process might not turn out to be as positive.

REFERENCES

Álvarez, Daniel and Vera, Francisco. *"Ciberseguridad y derechos humanos en América Latina" ("Cybersecurity and Human Rights in Latin America"), in Hacia una Internet libre de censura II: Perspectivas en América Latina; compiled by Agustina Del Campo.* First edition. Ciudad Autónoma de Buenos Aires: Universidad de Palermo - UP, 2017.

Bachelet, Michelle. "*Programa de Gobierno Michelle Bachelet 2014-2018" ("Michelle Bachelet Government Program 2014-2018"), Chile, 2014*, http://www. subdere.gov.cl/sites/default/files/programamb_1.pdf (reviewed on October 10, 2017)

El Mercurio, *"Sigue creciendo el alcance del ciberataque: 270 detecciones en Chile y 75 mil a nivel mundial" ("Reach of cyberattacks on the rise: 270 detections in Chile, 75,000 worldwide")*, May 12, 2017, http://www.emol. com/noticias/Tecnologia/2017/05/12/858167/Sigue-creciendo-el-alcance-del-ciberataque-270-detecciones-en-Chile-y-75-mil-a-nivel-mundial.html (reviewed on October 10, 2017)

Global Partners Digital. *"Framework for multistakeholder cyber policy development",* October 7, 2017, https://www.gp-digital.org/publication/framework-for-multistakeholder-cyber-policy-de-velopment/ (reviewed on October 10, 2017)

La Tercera, *"Casi 24 mil ciberdelitos se reportaron el primer semestre" ("Almost 24,000 cybercrimes reported in the first half")*, August 16, 2017, http://www.latercera.com/noticia/casi-24-mil-ciberde-litos-se-reportaron-primer-semestre/ (reviewed on October 10, 2017)

Lara, Juan Carlos y Viollier, Pablo. *"Mapping the Cyber Policy Landscape: Chile"*, Global Partners Digital https://www.gp-digital.org/wp-content/uploads/2017/02/mappingthecyberlandscape_chile.pdf (reviewed on October 10, 2017)

Maciel, Foditisch, Belli y Castellón. *"Seguridad cibernética, privacidad y confianza: tendencias en América Latina y el Caribe. El camino a seguir", en Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? ("Online Security, Privacy, and Trust. The Way to Follow" Are We Prepared in Latin America and the Caribbean in Cybersecurity?),* 2016, https://publications.iadb.org/handle/11319/7449

OECD. *"Cyberpolicy security policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the internet economy"*, OCDE, 2012. P 12.

Piquer, José Miguel. *"Internet: Infraestructura Crítica" ("Internet: Critical Infrastructure")*, September 29, 2015, http://ingenieria.uchile.cl/noticias/115726/internet-infraestructura-critica (reviewed on October 10, 2017)

Judicial Branch, *"Noticiero Judicial: Correo falso recibido por usuarios" ("Judicial Newscast: False e-mail received by users"*), September 29, 2014, https://www.youtube.com/watch?v=uWHkaeBZ-MM0 (reviewed on October 10, 2017)

Undersecretariat of Defense "*Una Política Nacional de Ciberseguridad para Chile"*, April 27, 2017, http://www.ssdefensa.cl/n5427_27-04-2017.html (reviewed on October 10, 2017)


DERECHOS
DIGITALES
América Latina