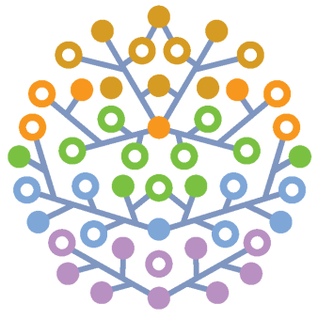
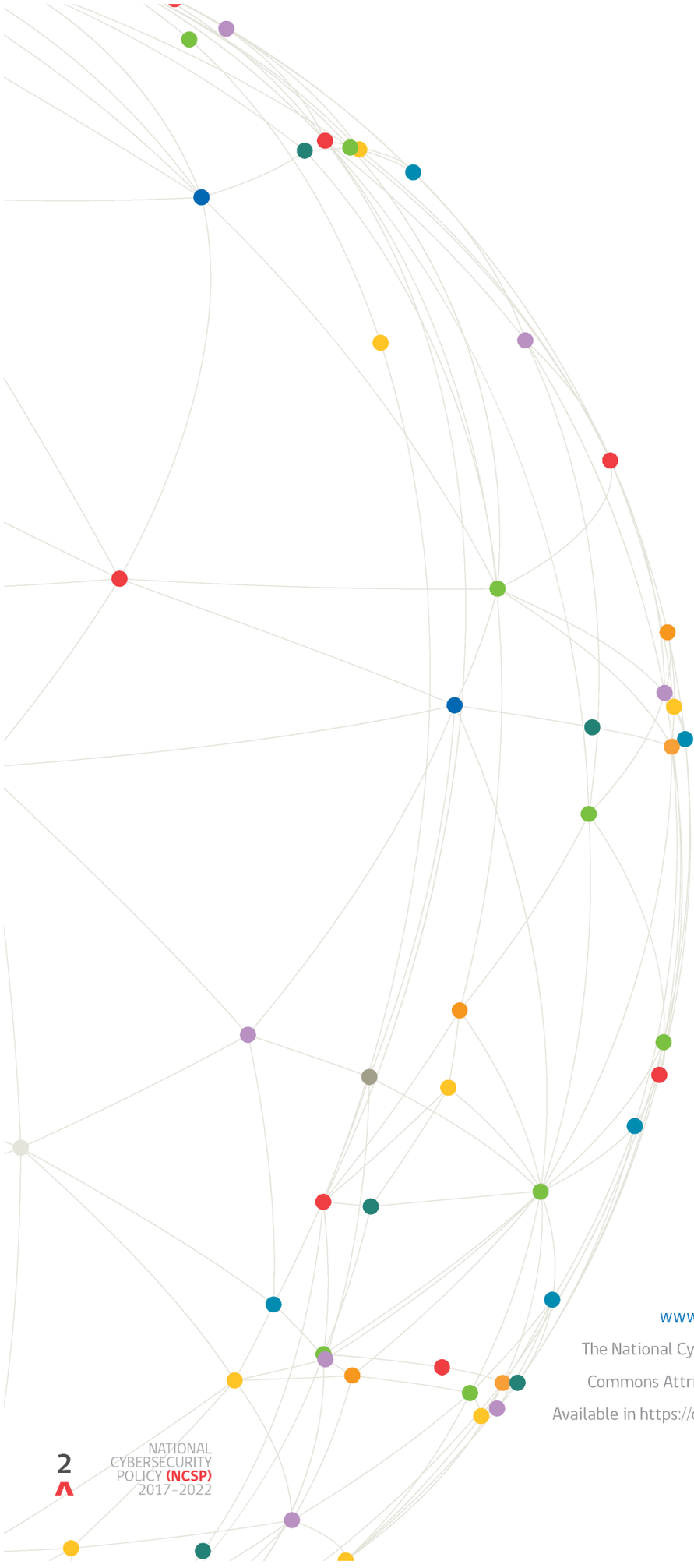


NATIONAL CYBERSECURITY POLICY

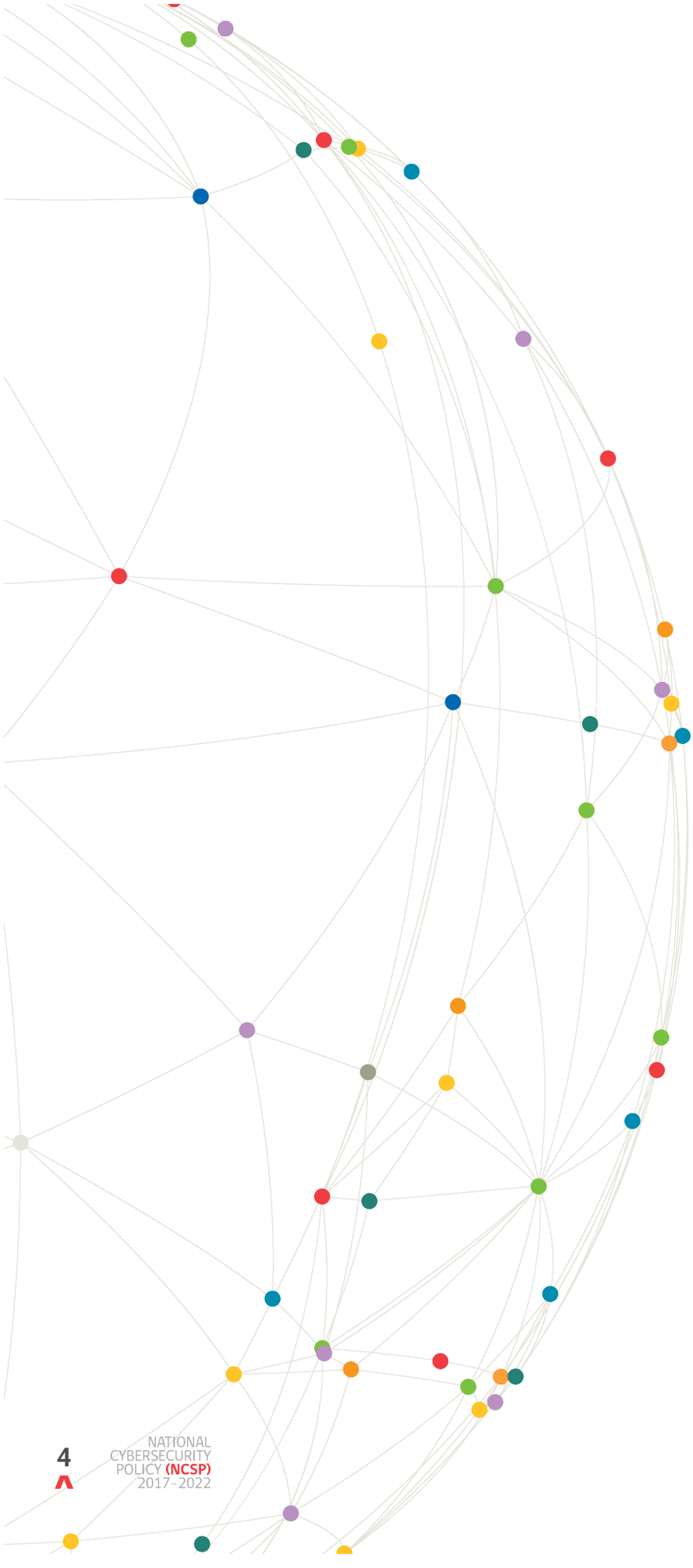
Gobierno de Chile

www.gob.cl



www.ciberseguridad.gob.cl

Table of contents



A Cyber-Security Policy for Chile

Information and communication technologies (ICTs) are a set of tools like no other in history, that has helped people, and has improved organizational interaction, economic operations and both private and public communications.

Their impact has been deep and broad in our society, and their reach extends day by day. People's access to the Internet has grown a 45.3% in the last two years, from a 52.2% by 2014 to 73.8% by March of 2016. Our national digital economy has grown around 11% in the same period, from 34 billion dollars in 2014 to 39 billion dollars in 2015.

This impact has transformed also the way our people use and understand technology.

The ICTs have had a social effect with no precedents in history, allowing our citizens to get informed, to organize themselves, and to participate from social life. Particularly, our children and adolescents make intensive use of social networks.

A transformation of this magnitude brings forth important challenges for our State, as it is imperative that all of this technology and its potential is used mainly to serve our people. We need to democratize the usage of the Internet, and to transform it into a tool for inclusion, efficiency and certainty, by ensuring the security and privacy of all those who use it everyday.

Chile must stay up-to-date in security matters, as any mistake, or any successful breach to our systems, may harm our people's welfare or our rights, it may negatively affect our interests, or it may hinder or even impede the operation of critical services for the country.

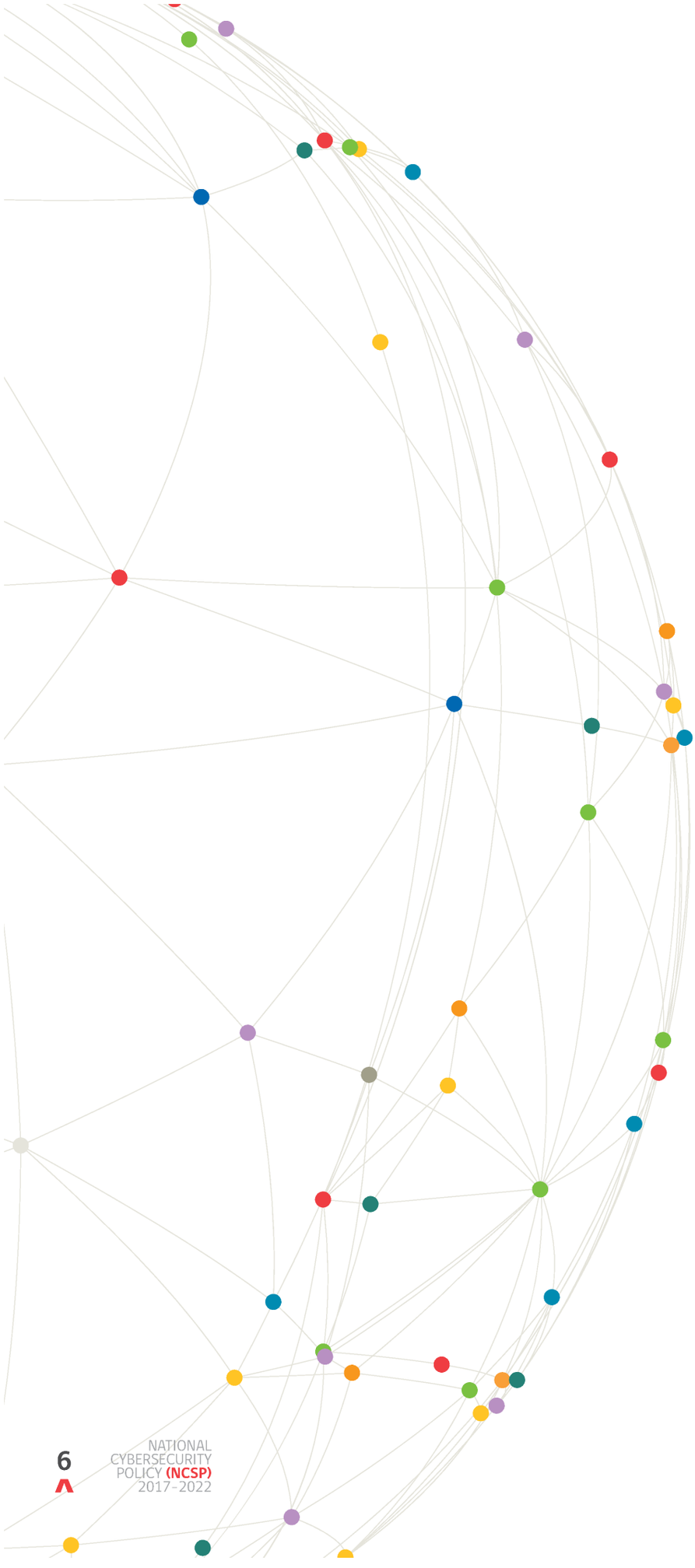
Listening to this demand, my government program included the development of a Digital Security Strategy, in order to protect both private and public interests in the digital realm.

This commitment was confirmed in November 2015, when we presented the Digital Agenda 2020, wherein it was announced the creation of a digital security strategy which, finally, is being released today through this document.

This first policy was designed from an intense dialog between private and public parties. For months we listened to public services representatives, professional and labor guilds, researchers and experts from within and abroad. When the Interministerial Committee wrote the first draft of this policy, it was subject to a public hearing as mandated by Law 20.500 about public participation. Numerous contributions were received which, no doubt about it, helped to improve it.

The national policy sets concrete goals and commitments for the overarching purpose of promoting and ensuring a free, open, safe and resilient cyberspace. A space that we expect it may allow our fellow citizens to reach their maximum potential. As it also happens with the
Digital Agenda, and the Productivity, Innovation and Growth Agenda, we expect this new policy to allow us to reduce the access gap, to increase awareness about safe use of ICTs, and to ensure the sustained technological leadership our country has in the region.

Michelle Bachelet Jeria
President of Chile



ICT penetration in every area in which we develop and interact has brought about a revolution that has left no one indifferent. Today we can hardly think of life without computer networks and that includes, of course, our social relations.

In the public sector, the State increasingly transmits information and interacts with citizens via the Internet, thus promoting the digital government and fulfilling its commitments of timely delivery of services and transparency. Along with the latter and in order to facilitate internet access to its citizens, the State has created programs that enable free internet access through the program WiFi ChileGob, a project that helps improve access in remote locations through Chile. In addition, the government is promoting the initiative "I choose my PC", which seeks to increase equality and to bridge the digital divide by favoring vulnerable seventh grade children. This program has benefited more than 350,000 students. Since it was launched seven years ago.

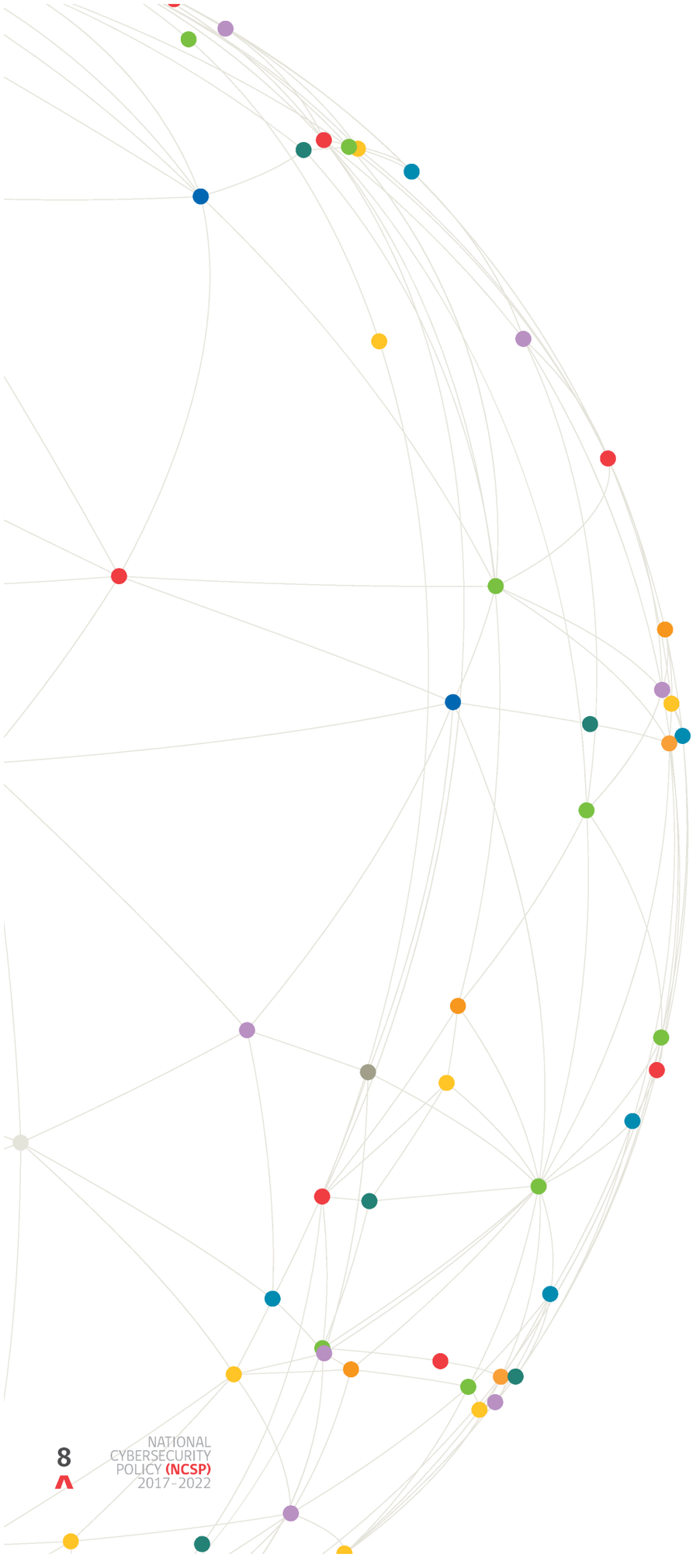
In this context, where Internet access and the use and dependence on ICT increases significantly, the criminological phenomenon associated with cyber crime and cyber attacks has worsened. For example, the State Information Network recorded an increase of more than one hundred million attacks, between 2014 and 2015, rising the 2016 to values exponentially higher by DDoS attacks.

In light of this reality, both the government of President Michelle Bachelet and the Digital Agenda 2020 in particular consider the development of a digital security strategy that promotes protection of private users. Therefore, the government has worked since April 2015 through an Inter-Ministerial Committee on Cybersecurity, on the development of Chile's first National Cybersecurity Policy, which has been fine tuned after a successful Citizen Consultation process carried out between February and March 2016.

While the National Cybersecurity Policy addresses with particular interest the prosecution and punishment of cybercrime, it goes far beyond the punitive area, for a fundamental variable to reduce the risks associated with cyberspace and take advantage of its potential is awareness, training in and dissemination of cybersecurity among society. Likewise, exploiting the competitive advantages of our country in terms of internet access, digital market maturity and quality professionals, the Policy seeks to promote industrial and productive development in cybersecurity.

Thus, I am convinced that the implementation of the measures contained in the cybersecurity policy as well as the State guidelines that it considers will contribute to further development of interagency cooperation and public-private partnership, which will enhance the value of free, open and safe cyberspace as a way to achieve greater economic development of our country and greater welfare for all Chilean people.

Mahmud Aleuy Peña y Lillo
Undersecretary of the Interior
Chairman of the Interministerial Committee on Cybersecurity



It has been a long time since cyberspace ceased to be part of science fiction to become one of the main areas of social interaction. Without going any further, Chile has the highest rate of Internet penetration in Latin America, with more than 70% of its population connected.

This has allowed its people to use digital technologies intensively to communicate with one other, express their ideas, share their causes or strengthen personal ties through social media, to carry out multiple transactions online and to take advantage of e-commerce facilities. However, this intensive use also increases our levels of dependence on the internet and the infrastructure that supports it, exposing us to new risks and threats.

Therefore, one of the challenges undertaken by the Government has been to improve the standards of digital security of our country, in order to protect people and the exercise of fundamental rights such as privacy, freedom of expression and access to information, among others.

This policy is the first concrete result of this challenge, a result that is the fruit of collective work that we assumed in the Interministerial Committee on Cybersecurity, made up by the Undersecretariats of Interior, Foreign Affairs, Defense, Finance, General Secretariat of the Presidency, Economy, Justice, Telecommunications and the National Intelligence Agency. The Committee met throughout 2015, holding multiple public hearings where it welcomed representatives from trade associations, companies, civil society, academics and national and international cybersecurity experts.

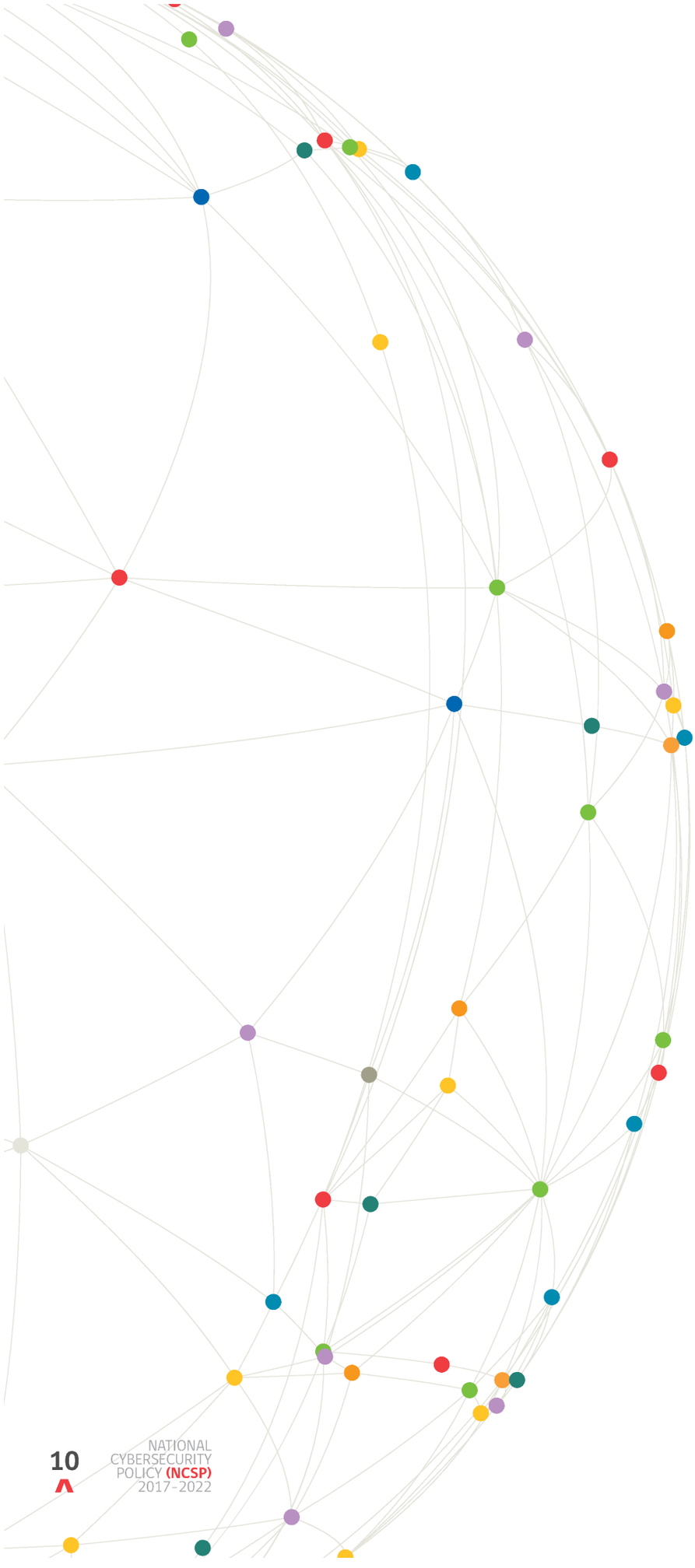
This policy was subject to an extensive public consultation process, through which fifty observations, comments and criticisms were received which certainly enriched the document that you have at hand.

The policy outlines five strategic long-term goals, aimed at addressing the challenges that our country faces in cyberspace, incorporating not only the scope of action of the State but also considering the role of the private sector, the civil society and the academia in this important task.

The policy reflects a central tenet: security and freedom are complementary. Combating cybercrime and other threats on the Internet cannot become an excuse to trample human rights such as privacy and freedom of expression on the contrary, they are means to fully guarantee these rights in cyberspace.

Now we face the great challenge of implementing the policy and monitoring its effectiveness, for which it is essential to have the cooperation of all stakeholders, so that our country can further progress in building an open, free and safe cyberspace for all.

Marcos Robledo Hoecker
Undersecretary of Defense
Executive Secretary Interministerial Committee on Cybersecurity



2 Introduction

The massive use of information and telecommunication technologies (ICT), while contributing to the country's development, also entails risks that may affect people's rights, public security, critical infrastructure, digital government, and Chile's essential interests and foreign policy.

These risks may arise from multiple sources and be translated into a series of activities including espionage, sabotage, fraud or cyber attacks carried out by, *inter alia*, other countries, organised groups or individuals.

There is important progress at an international level in the management of ICT-related risks. By 2015, over 40 countries had developed a cybersecurity[1] strategy or policy -some of which are already working on their second or third version. Note has also been taken of the important evolution in terms of doctrine, techniques and regulations within the most diverse organisations and international forums.

At a national level, the challenge lies on developing a policy driving the country's actions in cybersecurity matters, together with implementing and adopting the measures required to protect user security in the cyberspace, by taking into account educational strategies focused on self-care and prevention in the digital environment, and complying with President Michelle Bachelet's programme of government -which proposes **"to develop a digital security strategy protecting private and public users"**[2].

This document contains the political guidelines developed by the Chilean State in the field of cybersecurity, with a view to 20223, and aimed at having a **free, open, safe and resilient cyberspace.**

1 Further information in the following websites:
https://ccdcoe.org/strategies-policies.html
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

2 President Michelle Bachelet's Government Programme, Page 57.

3 As explained in section V, "Roadmap", this policy contains long-term guidelines aimed at this and the coming government, and a series of short-term measures to be planned and executed by each relevant administration.

3 Why there is need for a national cybersecurity policy?

A. To protect people's security in the cyberspace

People are to be ensured a security level allowing them to carry out their normal personal, social and community activities in the cyberspace, such as well as to exercise their fundamental rights as freedom of speech, access to information, protection of the private life and personal property.

B. To protect the country's security

There is need to promote the safety of information networks and systems belonging to the public and private sector, especially the ones that are essential for the proper running of the country, ensuring there is continuity of basic services.

C. To promote cooperation and coordination between institutions

There is need to improve communication, coordination and cooperation actions between institutions, organisations and companies, both in the public and private sectors, at a national and international level, with the purpose of strengthening trust and provide a single answer to cyberspace risks.

D. To manage risks in the cyberspace

There is need to take into account the development of analysis and management processes for the use, processing, storage and transmission of information, as well as the building of capacities to prevent and recover from cybersecurity incidents that may arise, in order to achieve a stable and resilient cyberspace.

4 Current status of cybersecurity: regulations, institutions, risk overview

A. Regulations and institutions

The current institutional structure in the field of cybersecurity is based on different bodies and entities. This requires the strategic coordination of different efforts, and their roles and duties, as well as the establishment of common practices and technical criteria, with the purpose of improving efficiency and effectiveness in the field of cybersecurity[4].

The country has in place a set of legal and statutory regulations that relate directly or indirectly with the challenges of cybersecurity -which should be reviewed and updated in accordance with the guidelines set out in this policy and with Chile's international commitments, for example, Law No. 19,223 about cybercrime or Law No. 19,628 about the protection of private life, among other rights.

B. Risk overview

Because of the global reach of cyberspace, risks and threats may come from Chile and abroad, due both to natural and criminal activities, such as, for example, espionage and to surveillance actions carried out with different purposes, thus affecting the confidentiality, integrity and availability of information assets in the cyberspace and, therefore, people's rights[5].

At a global level, there is plenty of evidence about cyber attacks and online espionage. The large-scale interference with telecommunication networks, the outage of Internet services and espionage carried out against governments and companies, as well as attacks against critical infrastructure such as basic services, financial institutions and government entities have been openly covered in the global news.

Regionally, the countries affected with the highest number of cyber attacks in 2013 in Latin America were Brazil, Argentina, Colombia, Mexico and Chile. Accessing or stealing information from infected computers or devices were a feature in the region[6].

Likewise, cybercrimes perpetrated in Chile are a confirmation of their cross-border nature, especially such crimes associated with the fraudulent use of credit and debit cards and cyber frauds among others.

The policy takes into consideration this type of threats, especially the ones affecting the country's critical infrastructure.

---

4 See Annex No.1 with a detail of the regulations and institutional structure currently existing in the field of cybersecurity.

5 See Annex No.2 containing information about the risks of cyberspace.

6 Prandini, P. & Maggiore, M. 2013. Ciberdelito en América Latina y El Caribe. Una visión desde la sociedad civil (Cybercrime in Latin America and the Caribbeann. A view from the civil society). Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y Caribe. pp. 3.

5 Policy roadmap

This cybersecurity policy is composed of two core elements: a State policy containing objectives by 2022, and an agenda with specific measures to be implemented between 2017 and 2018.

The objective of this structure is proposing a general overview as to the direction the country should take in the medium and long term, with the development of a set of measures that may be implemented and evaluated during this Government's administration, thus leaving to the following administration the task of reviewing the policy and proposing an agenda that may be executed by the next administration.

A. Policy objectives for 2022

This policy sets out high level long-term objectives that allow driving the country's efforts to pursue such goals, serving at the same time as a guide to prioritise and rationalise the measures contained in this document.

Additionally, the policy includes a series of minimum essential roles and the corresponding institutional design that shall govern the same both in the short term and in the medium and long term (2017-2022).

B. Timetable of measures 2017-2022 and evaluation

Upon development of the policy objectives, a timetable is proposed for implementation in the 2017-2018 two-year period that will enable a joint effort from the Government and the private sector in the field of cybersecurity –focused on the adoption of prioritised measures and the preparation of a series of feedback that review and extend the policy's scope by the end of 2017.

C. Integrated supplementary policies in the digital field

This cybersecurity policy is an integral part of a set of policies implemented by the Government or at a development stage in the digital field with the purpose of having clear and systematic definitions about cyberspace.

> The Digital Agenda for 2020

The Digital Agenda for 2020[7] is a roadmap designed to guide the country's digital development through the definition of medium term objectives, lines of action and concrete measures. Launched in the second semester of 2015, this Agenda proposes that the widespread use of technologies becomes a means to reduce existing inequalities, with the opening of more and better opportunities for development and contributes to the respect of the rights of all Chilean women and men.

The Agenda includes a specific measure (No. 25) focusing on the development of a cybersecurity strategy which will be executed through this policy. Likewise, this policy is enhanced and supplemented by a series of measures contained in the Agenda, such as the support introduced in the new Law

7 Available in: http://www.agendadigital.gob.cl/

for the Protection of Personal Data, the safeguarding of Internet consumers, the development of a National Telecommunications Infrastructure Plan, and the upgrading of regulations governing the electronic signature, among measures.

> National cyber defence policy

Because the National Defence's networks and information systems are a critical infrastructure for external security and the exercise of the country's sovereignty, and by virtue of the constitutional and legal rights vested on the National Defence, during 2017 the Ministry of Defence will prepare and publish a set of cyber defence specific policies containing specific political definitions about how these networks will be protected and how the National Defence's capabilities may cooperate in the development of a free, open, safe and resilient space for the country.

> International cyberspace policy

One of the high level objectives of this policy relates with the international relations and cooperation about cybersecurity in the global context. However, it is essential for the country to incorporate these and other objectives, such as the development of human rights, defence, and other related objectives in order to consolidate and integrate the same into Chile's foreign policy.

With that in mind, this policy includes a specific measure related with the creation of a strategy in this field by the Ministry of Foreign Affairs which, in turn, is consistent with and executes measure No.11 of the Digital Agenda 2020 aimed at generating a country's widespread view about Internet governance.

6 Policy objectives by 2022

A. The country will have in place a robust and resilient information infrastructure, prepared to face and recover from cybersecurity incidents, under a risk management approach

1. Concept. Risk identification and management

Cybersecurity is described as a condition presenting the least risk for cyberspace -understood as a set of physical and logical infrastructure, and the human interactions taking place in the same. Within this set, the main feature to be protected is information confidentiality, integrity and availability which, in turn, create a robust and resilient cyberspace.

This framework does not include the increased capability of state or private surveillance actions by using digital technologies, which relate with public order or national security objectives and are discussed in other instruments having a different focus. Surveillance actions proposed in this instrument will only be aimed at managing the risks of information in the cyberspace.

Prevention and management models for cyberspace will be created from the Policy, including physical risks that may affect the same, regularly updated by a continuous improvement model, which shall be the basis for technical measures to be adopted in order to prevent, manage and overcome actual risks, with an emphasis on service resilience and continuity within a set deadline and focus on maximising the country's cybersecurity levels.

2. Protection of the information infrastructure

Information infrastructure is composed of people, processes, procedures, tools, installations and technologies supporting the creation, use, transport, storage and destruction of information.

There is an especially relevant group, within information structure, for a country to keep moving forward, called critical information infrastructure (CII), which includes the installation, networks, services and physical and information technology equipment whose impairment, degradation, rejection, interruption or destruction may have an important impact on the security, health and wellbeing of people and on the effective operation of the State and the private sector.

Special emphasis will be placed on the impact that an information security incident may have on physical infrastructures controlled or monitored from the cyberspace, and on the security of industrial surveillance sensors and devices enabling such actions.

CIIs shall the designed with an architecture maximising their robustness and resilience against events that may render them non-operational, and enabling them to adapt to natural phenomena, human interventions and information interferences such as non-voluntary incidents or cyber attacks.

3. Identification and prioritisation of critical information infrastructure

Sectors included in the definition of CII are very similar and recurrent in various international classifications. In Chile, while consideration of a specific policy for critical infrastructure is under consideration, information infrastructure in the following sectors will be considered as critical:

energy, telecommunications, water, health, financial services, public security, transport, the civil service, civil protection and defence.

The policy contains a full set of areas, roles and responsible State entities used to identify and specify the critical level of each sector.

Technical bodies in charge of executing measures derived from this policy shall include special cybersecurity standards for CIIs depending on the different levels of development, especially with regard to special processes.

The medium term will see the implementation of measures ensuring service continuity through the redundancy of the physical infrastructure of some CII, especially in the fields of telecommunications, civil service, civil protection and defence.

> 4. Equipment available to respond to cybersecurity incidents

According to best practices worldwide, it is essential to have available prevention, monitoring, management and response structures to face computer-related security incidents at a national level.

The basic body in this structure is the Computer Security Incident Response Team (CSIRT) or teams in charge of responding to computer security incidents. Chile needs today the human and financial resources, a clear institutional framework and a mechanism to operate in coordination so as to promote the creation and operation of the same at different levels of the national life.

Chile will have a national CSIRT in place to collect and structure information received from other (national and international) CSIRTs, promoting action coordination between CSIRTs in each sector, with the required authority to coordinate the technical response in the case of incidents endangering the country's security.

The Government's current CSIRT will be strengthened, with a specific CSIRT to be created in the area of the National Defence. Likewise, the need is also in place to evaluate the relevance of creating a CSIRT for critical infrastructure.

The creation of CSIRTs by sector will be supported by different public, private, academic and civil society stakeholders.

> 5. Implementation of standardised mechanisms for reporting, managing and recovering from incidents

There will be centralised and standardised mechanisms for reporting cybersecurity incidents enabling the widespread and real time overview of incidents generated in the country.

These mechanisms will be compulsory for the central Government and certain regulated sectors, and voluntary, in principle, for any stakeholders that may want to join them. The amount of information required will be restrictedly limited to what is needed to describe and manage the type of threat, especially avoiding the collection and processing of data affecting people's private lives.

For such purpose, the National CSIRT will keep a secure and confidential platform able to cooperate in case of cybersecurity incidents and gather the relevant information, and will create a network in conjunction with public and private bodies.

At the same time, both public bodies and CII will have institutional bodies responsible for information security, together management and recovery plans in place for addressing incidents, with special emphasis on business continuity and on minimising any damages caused by actual incidents.

In addition to the foregoing, the preparation of computer vulnerability reports by users and experts will be promoted through the adoption of guidelines for responsible information delivery, models to reward the detection of security problems, and other mechanisms promoting responsible disclosure.

> 6. Differentiated standards are required in the field of cybersecurity

Any information infrastructure governed by or providing goods and services to the Chilean Government, or services to the people, shall comply with a basic set of standards covering confidentiality, integrity and availability of the information and the systems operating the same, according to the risks and threats faced by them and in consistency with their size, maturity, critical state and confidentiality level of information and/or processes supported by them.

With regard to critical information infrastructure, any risk shall be properly evaluated and addressed pursuant to standards including CII's confidentiality, integrity and availability, aimed at having an effective and comprehensive security system in place that allows the prevention, management and recovery from cyber attacks and other information security incidents, together with contingency plans for ensuring business continuity of their services.

Standards and best practices used shall be compatible with international efforts ensuring the confidentiality, integrity and availability of information, without setting out specific solutions – except for qualified cases.

B. The State will protect people's rights in cyberspace

> 1. Crime prevention and trust building in cyberspace

Crime prevention, dissuasion, control and punishment are critical to minimise risks and threats in cyberspace, thus contributing to trust building in connection with the activities carried out within the same.

There are multiple criminal activities carried out in cyberspace such as stealing strategic information, interrupting online service systems, information hijacking (ransomware), phishing, pharming and the fraudulent use of credit or debit cards, among other illicit activities.

At a global level, there is information about cyber attacks consisting in espionage activities and distributed denial of service (DDoS) attacks through the Internet, the large-scale intercepting of telecommunication networks against critical infrastructure such as, *inter alia*, banks, basic services and Government entities. This policy is aimed at minimising risks associated to these threats.

In addition to public policies developed to prevent and punish the above-mentioned crimes, it is also possible to build trust in cyberspace by employing the same technologies. The adoption of technical solutions allowing to increase user security in cyberspace, especially in the case of solutions cooperating with identity management in this environment, such as the mass adoption of digital certificates (digital signature) in websites, and by people and organisations will be promoted as a way to safeguard user communication and identity.

This policy also recognises the value placed on encryption technology, thus allowing the provision of the most unprecedented levels of information confidentiality and integrity levels in history.

Measures based on this policy shall promote encryption adoption for online users according to international standards, and under no circumstances the intentional use of unsafe technologies shall be promoted, or there will be and obligation by any person or organisation to provide digital services to implement 'back door' mechanisms compromising or increasing any risks associated with the security technologies used.

> 2. Priority setting in the implementation of punishing measures

Unlike crimes committed in the physical space, cyberspace presents some challenges to crime prosecution and punishment. Some of these challenges include, *inter alia*, the identification of authors, the time elapsed between the perpetration of a crime and the victim's reaction, the low rate of complaints submitted and the unlike possibility to prosecute the perpetrator(s) -because enforcement agencies operate within the State's territorial borders while the cyberspace is essentially a borderless place.

Measures in place to punish these actions should be implemented by bearing in mind this context, and as a complement to this policy.

The updating of Chile's legislation, promoted by the decision to adhere to the Convention on Cybercrime of the Council of Europe[8], together with the upgrading and strengthening of current regulations and the development of cross-cutting measures instead of the adoption of measures by sectors, are important objectives in this field.

> 3. Multi-sectoral prevention

Because cyber attacks and cybercrime may be perpetrated by State bodies, organised groups or individuals, and threats may come from inside and outside the country, any response must come from multi-sectoral actors involving the private sector, the academia, the civil society and, indeed, criminal prosecution and defence bodies, as well as victim advocacy organisations.

It is therefore essential to generate the proper spaces for coordination, meeting and cooperation, and strengthen significantly the existing technical skills and access to training by prosecutors and judges, the investigation and forensic capacities of the police bodies, and the development of guidelines aimed at providing a minimum safeguard to the entire population.

Definitions must be designed to gather, standardise and integrate data and information related with cybercrime, increase investigation capacity and generate evidence regarding such crimes.

> 4. Respect for and promotion of fundamental rights

All measures proposed by the policy should be designed and executed with a focus on fundamental rights -because of their fundamental nature and indivisibility, and on the basis that cyberspace is an environment where people have the same rights as in the physical world[9]. Therefore, the policy includes and promotes the following:

8 Available in: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

9 In this regard, Resolution A/HRC/20/L.13 from the UN Human Rights Council declared that "people's rights should be also protected in the Internet".

- The Internet is a global public asset; therefore, users may not be deprived from accessing the network but for reasons of *force majeure* duly based, with access never being denied by vague reasons such as public order, national security, or for the honour of any individual despite their capacity or title.
- Regarding the foregoing, and taking into account that information availability is an essential characteristic of cybersecurity, this policy will support public and private efforts made for the access to information and culture by the population through digital channels.
- Related with the above, the principle of respecting Internet neutrality is also included, so that Internet service providers may not discriminate or arbitrarily restrict the access to any content whatsoever, unless there is a legal justification to do that.
- This policy also respects and promotes the respect for freedom of speech, by taking into consideration not only communication media but also the population as a whole, the intermediaries making possible to communicate these messages and social networks[10]. Any interference with this right shall be carried out in accordance with national and international standards in the field of human rights.
- The protection of private life and the inviolability of user communication in the cyberspace, including the protection against the unauthorised gathering, process and publication of personal data; transparency in the management of such data by private and public stakeholders, and as mentioned above, the protection of essential technologies to ensure that users may safely and confidently use the cyberspace.
- The protection of due process with regard to the measures affecting information security, seeking that surveillance and criminal prosecution measures in cyberspace comply with international standards with regard to protection such as the principles of suitability, need and proportionality[11]. These measures will not only be applicable to criminal prosecution by the State, but also to the actions of all its bodies, thus safeguarding the application of this right among the users of cyberspace. Massive and indiscriminate surveillance of cyberspace is a serious attempt against fundamental rights.

Efforts in the field of fundamental rights will especially take into account the rights of vulnerable groups, such as, *inter alia*, boys, girls and young people, the elderly, disabled persons and ethnic minorities. There will be also a gender focus making possible to visualise and address the inequalities faced by different users in cyberspace.

The policy will seek that all people may enjoy a safe cyberspace free from abuses such as online bullying, the theft of personal information, large-scale surveillance and other practices affecting especially the most underprivileged members of society. Particularly, efforts will be carried out at all levels so that cybersecurity is not considered luxurious for people or the country's organisations.

10 The role of Internet intermediaries has increasingly attracted attention because of the critical role they plan in ensuring rights such as freedom of speech. In this regard, reference frameworks such as the Manila principles may be consulted, [online] Available in https://www.manilaprinciples.org/es

11 A useful analysis tool is the document "*Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*" (International Principles about the Application of Human Rights to the Surveillance of Communications). [online] Available in: https://es.necessaryandproportionate.org/text

C. Chile will develop a cybersecurity culture based on education, good practices and accountability in the management of digital technologies

> 1. Cybersecurity culture

ICTs promote the development of an equitable and inclusive cultural, technological and economic heritage of the country and comprehensive people's development.

Therefore, a cybersecurity culture will be promoted at all levels with the purpose of making the tools and knowledge available for society to understand this field of human relations including its advantages and risks, and may manage them properly.

> 2. Community awareness and information

People will be made aware of the risks and threats involved in cyberspace with the purpose of achieving a safe use of platforms providing services to the community, both from public institutions and private agents.

The community will be made aware of the good use, measures or personal care and security in cyberspace.

> 3. Cybersecurity education

This field will present many challenges to Chile's educational system. Early and advanced education of the Chilean population should be a part of these challenges; therefore, digital gaps generated by, *inter alia*, inequitable access to resources, skills, infrastructure and connectivity should be addressed.

To achieve the above goal, it is critical to implement initiatives promoting and developing a **conscious, competent, informed** and **responsible** digital culture including all relevant stakeholders and understanding that this is a joint effort to achieve a common, long-term benefit.

D. The country will carry out cooperation actions with other stakeholders in the field of cybersecurity and will actively participate in international forums and discussions

> 1. Chilean foreign policy principles

Chile's foreign policy is based on a series of principles driving its diplomatic work and actions, such as: the respect for international law; the promotion of democracy; the respect for human rights; conflict prevention; the pacific resolution of disputes and the commitment to cooperate in the international arena. In turn, these principles drive the interest of Chile's foreign policy, namely: contribute to the strengthening of multilateralism and promote international peace and security[12].

The emergence of cyberspace, especially the Internet, as a public asset urges us to face the challenges of managing all types of risks, where interacting at an international level is particularly important in the light of the global and cross-border nature of the same.

Cybersecurity is a cross-cutting and multi-factorial concept which, at an international level, conveys the possibility to build common capacities, approaches and measures with the cooperation and

12 Further information in: http://www.minrel.gov.cl/minrel/site/artic/20080802/pags/20080802194424.html

assistance of other countries, such as the conviction that sustained multilateral diplomatic work involving multiple stakeholders allows decreasing the risk of conflict in cyberspace.

To achieve the above, the Ministry of Foreign Affairs will be responsible for coordinating with other ministries and Government agencies the international cybersecurity policy.

> 2. Cooperation and assistance

Bilateral cooperation work will promote different types of relations with other countries in the field of cybersecurity, including assistance to and from Chile, exchange of information and experiences, the implementation and furtherance of mechanisms for facilitating political dialogue in this field, and the promotion of transparency and trust building in cyberspace, with an emphasis on multi-agency work.

> 3. Reinforce the participation in multilateral and multi-stakeholder work

Efforts must be focused on promoting digital as a free, open and safe environment for all users in the cyberspace.

The country needs to strengthen its work in this field, taking into consideration the special challenges faced in terms not only of the technical conditions, and the global nature and decentralised character of the network, but also regarding its political scope, and with a system of Internet governance including multiple stakeholders where the private sector and civil society have a special role.

Within this framework, the country's involvement will be increased in the multilateral and global arena, supporting regional, sub-regional and multilateral consultations in this field, especially in Latin America, and actively involving stakeholders in this debate.

> 4. Promote international regulations encouraging trust and security in the cyberspace

Although there are practically no specific regulation instruments, the cyberspace is actually regulated both by the existing national laws and by the general applicable international regulations; therefore, the challenge lies particularly on being able to identify and interpret the relevant regulations of the applicable international law.

However, there are some challenges that must be faced through specific international agreements and regulations, such as the Convention on Cybercrime, which the country will adhere to, with reservations and safeguards consistent with this policy.

Additionally, the debate and adoption of multilateral and bilateral agreements should be promoted in order to encourage cooperation and mutual assistance in the field of cybersecurity, both in terms of formal instruments and as informal agreements and arrangements focused on international transparency and the trust building in this field.

E. The country will promote the development of a cybersecurity industry serving its strategic objectives

> 1. The importance of innovation and development in cybersecurity

Activities aimed at protecting domestic security and foreign defence generally require a strong innovation and development element promoting an increased development of the industry at a

national level. Within this framework, the field of cybersecurity requires a special effort because of its original nature and strategic importance for the country as a whole.

2. Cybersecurity as a means to contribute to Chile's digital development

While the size of the ICT sector represents 3~4, 12% share of the Chilean economy, in OECD countries this industry reports an average 6% share in the country's economies[13], generating a gap between both realities that Chile will partly resolve through the development of the cybersecurity component within this industry.

This will generate both an increased demand on the information technology industry and a higher industrial development in this field, helping the country to advance towards OECD's indicators, as well as strengthening policy objectives.

3. Development of the cybersecurity industry in Chile

There are no specific figures regarding the level of development of the national industry apart from some studies exploring this alternative[14]. The country's effort to develop a cybersecurity industry will be supported by studies describing the industry and identifying strategic fields for development in the short, medium and long time.

Particularly, a field which is regularly developed in compared experiences is the domestic industry related with the development and use of encryption standards by reason of its strategic importance for the country's security abroad.

4. Contribute to the generation of an offer by the local industry

Measures will be adopted in order to help creating and strengthening a domestic industry for cybersecurity services, technologies and management through a programme and initiatives aimed at the production of new goods and services in this area. A development pole will be created in this area which is in line with the Productivity, Innovation and Growth Agenda[15] and the Digital Agenda for 2020.

5. Generation of demand by the public sector based on the State's strategic interests

The generation of demand by the public sector based on their strategic and security needs and interests will support the strengthening of a national industry focused on cybersecurity services, technologies and management which is in line with international technical standards.

---

13 There are studies giving an approximate value to the GDP contributed by the ICT sector such as the "Índice País Digital" carried out by the País Digital Foundation and UDD, submitted in January 2015. This study estimated that the ICT sector represents 3% of the total Chilean economy (source from 2012). Likewise, in March 2015 the Under-Secretariat of Economy commissioned to F&K Consultores the study "Status of the Digital Development in Chile", which reported that the aggregate value of the ICT sector reaches 4.12% as compared with the total aggregated value (source from 2011).

14 Report "*Tecnologías de la Información y Comunicación en Chile: Áreas de investigación y capacidades, informe de estado del arte*" (Information and Communication Technology in Chile: Research Areas and Capabilities, State-of-the-art Report), Conicyt, 2010. "Índice País Digital", País Digital Foundation in conjunctions with UDD, January 2015. "Status of the Digital Development in Chile", F&K Consultores, March 2015.

15 Available in: http://www.agendaproductividad.cl/

7 Roles and required institutional structure to develop a national cybersecurity policy

A. Institutional structure for cybersecurity

It is essential for Chile, in order to fulfil this ambitious national cybersecurity policy and following the example of several other countries that have started this process some years ago, to have available a cybersecurity governance model responsible, at least, for carrying out such roles identified as essential -which are not being addressed, or are executed with no coordination within the country; therefore, the creation of an institutional framework to take up that role is hereby proposed.

A modern governance model and institutional framework which is in line with the needs of cyberspace and the country's digital development, will be a matter of law to be prepared and submitted by responsible institutional actors. Additionally, the creation of an advisory consulting council composed of different sectors will be assessed.

The roles identified as essential are: management of inter-institutional relationships, incident management, national and international point of contact, communications role, technical regulation and advisory role in general regulations, follow-up and evaluation of measures.

To carry out the above, correspondence of the cybersecurity framework with supplementary measures being developed in the area of digital governance within the State administration will be especially taken into account.

B. Transitional governance in cybersecurity

While the cybersecurity bill containing the final proposal for its institutional structure is discussed in the National Congress, certain essential roles identified up until now shall be temporarily performed by some of the institutions that are currently a part of the Government's structure.

An example of this is the role played by CSIRT Gob, which will be technically responsible for managing incidents arisen within the State's Connectivity Network, while, at a political level, it has been proposed to extend the term and scope of the Inter-Ministerial Cybersecurity Committee with regard to the communication, coordination and follow up roles of the different measures set out in the NCSP.

8 Public policy measures for 2017–2018

The measures below are an integral part of the public policy agenda to be implemented based on the strategic objectives described above[16].

	MEASURE	RESPONSIBLE – ASSISTING	OBJECTIVES NCSP
1	Prepare and forward to the National Congress a cybersecurity bill aimed at consolidating the institutional framework and incident management related with information security throughout the country.	MISP - MINDEF - MINHACIENDA - CICS (monitoring this measure)	A
2	Update Decree Law 83 about the State's information security aimed at the adoption of new standards and the creation of a model to control effective compliance.	MINSEGPRES	A
3	Add a cybersecurity dimension to the preparation and management of contracts for public concession tenders.	MOP (Concessions Department)	A
4	Create a working group responsible for developing a regulation and obligation framework for critical infrastructures in Chile, from a risk management focus.	MISP	A
5	Create a technical regulation for the development or contracting of software within the State, pursuant to standards for safe development.	MINSEGPRES	A
6	Create a platform to add information about cybersecurity incidents.	CSIRT	A
7	Coordinate the creation of updated requirements for regulated economic sectors	MTT - Super-intendence - CSIRT	A
8	Identify a minimum set of risks for Critical Information Infrastructure	CSIRT	A
9	Implement a standardised template for cybersecurity incident reports.	CSIRT, MINSEGPRES	A

16 The first body is the main responsible entity to carry out the task, and the other bodies support execution of the same. CSIRT means the current security equipment of the State's Connectivity Network, which will gradually take on operational duties identified in this policy.
Public institutions are identified with the following acronyms: CICS, *Comité Interministerial sobre Ciberseguridad* (Interministerial Committee on Cyber Securiry; MISP, *Ministerio del Interior y Seguridad Pública* (Interior and Public Security Ministry); MTT, *Ministerio de Transportes y Telecomunicaciones* (Transport and Telecommunications Ministry); MINDEF, *Ministerio de Defensa Nacional* (National Defence Ministry); MINHACIENDA, *Ministerio de Hacienda* (Finance Ministry); ANI, *Agencia Nacional de Inteligencia* (National Intelligence Bureau); MINJUSTICIA, *Ministerio de Justicia y Derechos Humanos* (Ministry of Justice and Human Rights); MINSEGPRES, *Ministerio Secretaría General de la Presidencia* (Ministry of the President's Office); MOP, *Ministerio de Obras Públicas* (Ministry of Public Works); MINEDUC. *Ministerio de Educación* (Ministry of Education); MINREL, *Ministerio de Relaciones Exteriores* (Ministry of Foreign Affairs); MSGG, *Ministerio Secretaría General de Gobierno* (Ministry of the Government's Office); MINECON, *Ministerio de Economía, Fomento y Turismo*, (Ministry the Economy, Development and Tourism).
When a ministry is mentioned without identifying a specific public service or under-secretariat, the reference relates with the under-secretariat participating in the Inter-Ministerial Committee on Cybersecurity or, should the corresponding ministry not be a part of the Committee, the corresponding ministry shall be responsible in general.

	MEASURE	RESPONSIBLE – ASSISTING	OBJECTIVES NCSP
10	Incorporate a cybersecurity dimension in the national emergency system.	MISP (CICS - monitoring this measure)	A
11	Prepare the regulation setting out safe mechanisms for exchanging information within the Government, between high level officers and other officials handling confidential or secret information.	MISP - MINDEF - ANI- MINREL- MINSEGPRES	A
12	Prepare a study about the resilience of telecommunication networks in Chile, proposing measures to improve it in the public and private fields.	MTT	A
13	Update the regulation on computer-related crimes.	MISP - MINJUSTICIA	B
14	Design and implement a standardised template to report cybercrimes.	MISP (with the police forces and ANI)	B
15	Promote the strengthening of investigation and forensic analysis skills related with cybercrime.	MISP (with ANI and the police forces)	B
16	Generate a first point for the dissemination of information to citizens based on the different digital channels and social networks enabled by the Internet.	MISP - MSGG (CICS - monitoring this measure)	C
17	Mark the Cybersecurity Month in October each year, promoting and developing activities to raise awareness at all levels. Additionally, participate in the Safe Internet Day in February.	MISP - MSGG (CICS - monitoring this measure)	C
18	Design and implement a large-scale cybersecurity campaign and promote the implementation of dissemination programmes in partnership with the private sector in awareness campaigns, with an emphasis on vulnerable sectors and a gender perspective.	MSGG (CICS - monitoring this measure)	C
19	Generate best practice guidelines both for citizens and the public sector.	CICS	C
20	Establish a cross-sectoral committee to promote cybersecurity at all levels and areas of the educational field.	MINEDUC- MINECON (Human Capital Committee) (CICS - monitoring this measure)	C
21	Design and implement a cybersecurity campaign aimed at the elderly population, including training and dissemination.	MDS (Senama) - MINECON (Human Capital Committee) (CICS - monitoring this measure)	C
22	Include Internet security issues in MINEDUC's specific programmes, promoting the ENLACES initiative.	MINEDUC (Enlaces) - MINECON (Human Capital Committee) (CICS - monitoring this measure)	C

	MEASURE	RESPONSIBLE – ASSISTING	OBJECTIVES NCSP
23	Strongly support the establishment, at an international level, of regional, sub-regional and multilateral political consultation processes, with special emphasis on the region.	MINREL	C
24	Advance the creation of bilateral work mechanisms, developing agendas and implementing cross-cutting political consultation instances with partner countries.	MINREL	D
25	Prepare a document containing Chile's international policy about cyberspace and cybersecurity.	MINREL - (CICS - monitoring this measure)	D
26	Establish an inter-agency working group to address international issued related with cyberspace.	MINREL - OTHER	D
27	Encourage the exchange of experiences with other countries in the field of cyber-security, with emphasis on the implementation and evaluation of strategies and policies.	MINREL	D
28	Analyse the regulation and application of the current system of public procurement supporting production and strategic domestic interests.	MINHACIENDA (Chilecompra Division) - MISP - MINDEF	D
29	Carry out studies both describing the cybersecurity industry (offer) and the use of cybersecurity in the country (demand), with the purpose of creating special programmes to promote the cybersecurity industry in specific sectors.	CORFO - MINDEF - MINECON	E
30	Analyse tax incentives, subsidies or R+D+I schemes in order to develop and adopt cybersecurity standards.	MINHACIENDA - MINECON - CORFO	E
31	Process the new law on personal data, conferring powers to a specific body that may impose security and notification requirements in connection with data leakage.	MINHACIENDA- MINECON	A, B
32	Develop one or more multi-sectoral cooperation opportunities with a series of social stakeholders (NGOs, companies, unions, and academia, *inter alia*).	CICS (committee coordinator)	A, B, C
33	Update Decree No. 5, 996 and Supreme Decree No. 1,299 in line with the amendments to Supreme Decree No. 83, setting out the requirements to access the network (self-assessment, online courses) and the obligation to report incidents by public bodies.	MISP	A, C
34	Carry out cyber exercises about cybersecurity incidents with different stakeholders in order to encourage the proper knowledge, research and dissemination of gaps, vulnerabilities and ways of mitigation in the national systems.	CSIRT	A, C

	MEASURE	RESPONSIBLE – ASSISTING	OBJECTIVES NCSP
35	Incorporate cybersecurity standards in the State's suppliers, requesting specific requirements for ICT suppliers, and analysing other requirements for other suppliers.	MINHACIENDA (Chilecompra Division)	A, E
36	Include a set of questions linked to cybercrime in the National Urban Survey on Citizen Security (ENUSC).	MISP (Under-Secretariat of Crime Prevention)	B, C
37	Prepare and regularly update a record of training offers for public servants about cybersecurity available in international organisations and national institutions.	MISP - MINREL	B, C, D
38	Adhere to and implement the Convention on Cybercrime of the Council of Europe.	MISP - MINREL - MINJUSTICIA- OFFICE OF THE PROSECUTOR	B, D
39	Encourage State support of R+D+I projects with public or private financing, whether national or international, in the field of cybersecurity.	CICS	C, E
40	Promote the development of advanced human capital regarding cybersecurity in the different technical-professional or vocational areas.	CORFO - MINECON (Human Capital Committee)	C, E
41	Support the export of national products and services in the field of cybersecurity, identifying international exhibitions and evaluating support actions.	MINREL (Prochile) - MINECON	D, E

9 Annexes

Annex No 1: Standards and institutions involved in cybersecurity in Chile

1. RELEVANT STANDARDS AT A NATIONAL LEVEL

a. Political Constitution of the Republic of Chile

- **Article 8,** about public transparency
- **Article 19**, including a catalogue of fundamental rights, with the most relevant ones being: **No. 2**, equality before the law; **Nos. 3 and 7**, due process and individual safety; **Nos. 4 and 5**; protection of life and inviolability of communications; **No. 12**, freedom of speech and freedom of information, and **Nos. 24 and 25**, property and freedom of creation.
- **Article 24**, vesting upon the person who acts as President of the Republic the authority to safeguard the public order in and the external security of the Republic, apart from the regulations that govern the authorities vested upon other State powers and bodies.
- **Articles 39 and following** regulating specific **situations** that affect the normal operation of the State.

b. Laws

- **Criminal Procedure Code:** This piece of legislation regulates criminal investigation and prosecution in Chile, and, within this framework, any investigation related with cybercrime that may be carried out in the country. Additionally, it regulates a set of intrusive measures that may affect the recipient's private life or inviolability of communications and, therefore, the inviolability of their communication –for which purpose the Law demands certain legal requirements and a court order authorising the practice of such measures.
- **Law No. 19,913, which creates the financial analysis unit and modifies a series of provisions in the field of money laundering and bleaching:** This law regulates some investigation and surveillance measures that, as in the case of the Criminal Procedure Code, may affect the recipient's private life or inviolability of communication and, therefore, the confidentiality of their information –for which reason the Law in this case also requires a court order in conjunction with the fulfilment of the legal requirements of the case.
- **Decree Law No. 211, Free Competition Law:** As in the previous case, this law authorises the carrying out of intrusive in specific cases and in the same terms described above.
- **Law No. 19,974, about the System of the State's Intelligence and creating the National Intelligence Bureau:** Within the framework of intelligence information gathering, this Law regulates the practice of special procedures to gather information, which has to be done under a court order and taking into account a series of legal safeguards restricting the gathering and use of this information.

- **Criminal Code:** This legal piece is the country's main criminal catalogue containing the description of a set of specific conducts together, with the associated sentences. Regarding cybersecurity, this code describes a series of conducts that may be carried out through cyberspace or affects the elements thereof, having a key relevance in the development of policies and the combat against cybercrime.
- **Code of Military Justice:** A legal piece containing specific provisions regarding crimes mostly perpetrated by members of the armed forces or at times of war. The provisions of this legal piece cover crimes related with espionage and disclosure of certified information to third parties, with the purpose of protecting the national security.
- **Law No. 19,223** There is a sub-category in the field of cybercrime related with the disturbance of the logical components of cyberspace (computer programmes, information systems, databases) called computer-related crimes. This Law sets out specific criminal definitions describing the non-authorised access, theft and destruction of information systems.
- **Law No. 20,009 covering the Loss, Theft or Robbery of Credit and Debit Cards.**
- **Law No. 18,168, General Telecommunications Law:** This piece of legislation regulates the legal framework of the country's telecommunication industry which provides key physical and logical infrastructure for the national cyber space. One of its provisions set out the protection, confidentiality and integrity of the information through the criminalisation of offences related with the non-authorised interception (art. No. 36B, letters b and c). Two recent modifications are especially relevant for the country's cybersecurity, namely: **Law No. 20,453 that ensures the principle of network's neutrality for Internet consumers and users,** regulating network management measures that may be adopted by Internet service providers and ensuring the duty of confidentiality, and **Law No. 20,478, about business recovery and continuity when the public telecommunications system is affected by critical and emergency situations,** enacted after the earthquake that affected the country in 2010. As described by its name, this Law sets out a set of measures allowing maintaining the continuity of the country's telecommunications and, therefore, the availability of information contained in the cyberspace.
- **Law No. 19,799 regarding electronic documents, electronic signature and signature certification services:** This Law regulates the use of electronic documents in the country, with the corresponding mechanisms to ensure information integrity and confidentiality by the use of digital signature, together with a system guaranteeing the proper operations of the bodies providing this service.
- **Law No. 20,285 about the access to public information:** This piece of legislation creates a transparency scheme for the State's activities, with active transparency obligations, which must be carried out through the website of each relevant public body; and passive obligations, which consist in providing the data that any person may require from these bodies, provided that this does not affect other rights and interests set out in the law -such as the State's security and third party's privacy, so that the confidentiality of the relevant is not affected.
- **Law No. 19,628 regarding the protection of private life:** This law sets out a series of principles and rights relative to the management of personal data in the country that may be requested by the owner of the personal data to whom is in possession of or manages a record containing such data, together with the general application rules for the management of personal data by the public and private sectors in connection with the safeguarding of the data contained in such information.

c. Decrees

- **Supreme Decree No. 83/2005 approving the technical regulations for the State administration bodies about the security and confidentiality of electronic documents:** This decree, which evolves from the provisions contained in Law No. 19,799, sets out a regulation for the public administration of the State about the security and confidentiality of electronic documents, together with the information infrastructure based on ISO standard 27,000, with the setting out of administrative measures such as the creation of information security committees in each public service. This decree is supplemented with **Supreme Decree No. 93/2006 that approves the technical regulation for adopting measures aimed at minimising the detrimental effects of unwanted spam messages received in the mailboxes of the State administration bodies and their officers.** As described, this decree sets out the measured aimed at preventing spam from being received by the State's administration bodies.
- **Supreme Decree No. 1,299/2004 setting out new regulations for the State's Connectivity Network managed by the Ministry of the Interior and describing the technological procedures, requirements and standards for the incorporation to such network by public bodies:** This decree, based on the provisions of the 2005 budget law, and Supreme Decree No. 5,996/1999, consolidates an intranet, named the State's Connectivity Network, where a number of ministries and public bodies should be interconnected. Centralising Internet access, this network has to comply with security technical standards in line with IEEE and ISO standards.
- **Supreme Decree No. 1/2015 approving the technical standards for the systems and websites of the State administration bodies:** This Decree updates the technical standards for the websites of the State administration bodies regulating certain conditions about confidentiality, availability and accessibility of information contained in those websites, all of them being key elements of cybersecurity.
- **Supreme Decree No. 533/2015 that creates a Cybersecurity Inter-Ministerial Committee:** This decree creates an Inter-Ministerial Committee responsible for developing a proposal for the National Cybersecurity Policy, of which this Annex is an integral part.

2. INSTITUTIONS INVOLVED IN THE FIELD OF CYBERSECURITY

a. Ministry of the Interior and Public Security

Body	Role	Mission
Undersecretary of the Interior	Preventive Public policy design	The mission of the Ministry of the Interior and Public Security is to safeguard public security, coordinating, evaluating and monitoring the execution of inter-sectoral plans in the field of crime prevention and control (Art.1, Law No. 20,502), including cybercrime, and to design public policies in order to prevent, challenge and punish the same. In particular, the Organised Crime Department is responsible for developing strategies for combating cybercrime (Exempt Resolution No. 10,168, 3/12/2013).
Undersecretary of the Interior	Preventive Reactive Public policy design	By virtue of Decree No. 5,996 of 1999, the MISP is responsible for implementing and operating, at a national level through the Computer Division, the State's Connectivity Network (RCE). Supplementing the decree mentioned above, Supreme Decree No. 1,299 of 2004, grants this State body the power to publish or disseminate the country's official regulations in the field of information security and to set out logic security regulations, standards and policies that public bodies included in the RCE shall be obliged to fulfil. This division was also granted the power to submit technical consultations to any State body. It is worth mentioning the RCE's role as a tool to support Government cybersecurity.
Investigations Policy (PDI), Cybercrime Investigation Brigade	Preventive and investigative	This Brigade is responsible for investigating crime under the direction of the Office of the Prosecutor, including cybercrime.
***Carabineros* Police, OS9 Department**	Preventive and investigative	According to Law No. 19,974 regulating this Department's responsibilities, one of its duties is to: "propose regulations and procedures to protect the State's critical information systems", Art. 8, letter c).

b. Ministry of National Defence

Body	Role	Mission
Defence Under-Secretariat	Policy design	The Defence Under-Secretariat is responsible for developing and updating the relevant primary planning and policies to face the challenges of cybersecurity for the National Defence, and ensuring that it is in line with the secondary planning thereof.
Joint Staff of the Armed Forces	Preventive and reactive	The Armed Forces are responsible for protecting their own information infrastructure. Additionally, they cooperate in tasks related with the national cybersecurity and national intelligence systems. The Joint Staff is the Ministry of Defence's permanent working and advisory body in matters having a connection with the joint preparation and use of the Armed Forces, thus being responsible for preparing and updating the Defence's secondary planning, together with other tasks relevant for the country's cybersecurity. The Armed Forces, pursuant to the planning carried out, are responsible for executing the relevant institutional and operational plans.

c. Ministry of Transport and Telecommunications

In charge of designing public policy and monitoring compliance in the area of telecommunications, the Telecommunications Under-Secretariat is also responsible for the implementation of Law No. 20,478 about "Business Recovery and Continuity under Critical and Emergency Situation of the System of Public Telecommunications", which task is executed through Decree No. 60/2012 setting out the Regulations for the inter-operation and dissemination or alert messages, the declaration and safeguarding of the telecommunications' critical infrastructure, and the information regarding serious failures of the telecommunications systems. Likewise, this Under-Secretariat is responsible for monitoring the respect for the principle of the network's neutrality set out in Law No. 20,453.

d. Ministry of Economy, Development and Tourism

This Ministry is responsible for designing public policies for encouraging productivity. The Ministry of Economy's mission is promoting the modernisation and competitiveness of the country's productive structure, the private initiative, and the market's efficient action, as well as the advance of innovation and the consolidation of the country's economy at an international level; therefore, cybersecurity as a focus for national development is included in the Productivity, Innovation and Growth Agenda.

e. Ministry of Justice and Human Rights

Pursuant to its role in the modernisation of the justice system, as well as in the development of regulations and policies aimed at facilitating the access to and protection of people's fundamental rights and citizen security, the Ministry of Justice and Human Rights is responsible for seeing to the ongoing updating and technical adequacy of legislation to the challenges posed by technological development.

f. Ministry of Foreign Affairs

Performing an articulation role within the international community and responsible for the international coordination of the national cybersecurity policy, the Ministry's *Dirección de Seguridad Internacional y Humana* (Department for International and Human Security), (DISIN), is responsible for identifying, coordinating and promoting Chile's cybersecurity position and interests within the international community, in all its dimensions. Likewise, the Ministry coordinates and promotes Chile's involvement in specialised international bodies and forums (Meridian, Octopus, OAS, UNASUR, ITU, IGF, UN expert groups, *inter alia*). It is also responsible for promoting bilateral relations in this field.

g. Ministry of the President's Office

With regard to the design of public policy in the area of digital government and digital development, the purpose of the Ministry of the President's Office, through the State Modernisation Unit, is to make the State accessible for people, with the relevant modernisation of the State and digital Government.

h. University of Chile

Body	Role	Mission
NIC Chile	Technical body, administrator	NIC Chile is the organisation responsible for the names containing the .CL domain, and for operating the technology allowing the efficient and safe operation of these names, so that people, companies and institutions may be identified in the Internet.
CLCert	Academic body, contact point with international CERTs and FIRST	CLCert's main objectives are: -Provide, in a timely and systematic fashion, information about security vulnerabilities and threats. -Disseminate, and make available to the community, information allowing the prevention and solution of this type of security incidents. -Educate the general public about security matters, promoting policies allowing implementation thereof

i. National Standards Institute (*Instituto Nacional de Normalización*)

A technical body responsible for setting out standards and accreditations, the National Standards Institute (INN) is a private law, non-for-profit foundation created by CORFO in 1973 as a technical body in charge of overseeing quality infrastructure which, in the cybersecurity fields, relates with a series of ISO/IEC 27000 standards.

j. Office of the Prosecutor

Exercising its role to lead the criminal prosecution process and carry out the public criminal action, the Office of the Prosecutor is an autonomous body responsible for investigating criminal offences, taking the accused before the courts and, if relevant, providing protection to victims and witnesses leading.

k. Judicial Branch

The Judiciary, which has the exclusive power of hearing, resolving and executing sentences in civil and criminal lawsuits, is composed of courts having different competences, namely, civil, criminal, labour and family courts. With regard to cybersecurity, judges have the power to order some intrusive actions, control the legality of criminal investigations, and decide upon criminal cases, including cybercrime.

Annex No 2: Risk and threat overview

1. SOURCES AND TYPES OF RISKS AND THREATS

Due to the global nature of cyberspace, risks come from threats both from Chile and abroad and have different origins relevant for the country, namely:

- **Internal incidents:** Involuntary information leakages, accidental interruption of information systems, or other involuntary incidents that may affect the confidentiality, integrity, availability and traceability of the information.
- **Natural disasters or *force majeure:*** Earthquakes, floods and other disasters that may affect cyberspace caused by the destruction of physical infrastructures essential for information availability.
- **Espionage and surveillance activities carried out by State actors:** Conducts that affect information confidentiality due to theft of the same for political or strategic purposes. Particularly important is the use of sophisticated tools known as APT (Advanced Persistent Threat) that, in turn, may benefit from non-published computer vulnerabilities of technologies in use.
- **Denial of Service and Distributed Denial of Service (DOS and DDOS) attacks:** These attacks relate with the intentional overcharge of services provided in a computer system which, in turn, can be conducted from one point of the network, or distributed to coordinate the attack from various points, many times by using infected devices with malicious programmes in order to achieve their objective.
- **Cybercrime:** Criminal activities perpetrated against components in the cyberspace (non-authorised access, information sabotage, information theft, information hijacking or ransomware) or employing tools in cyberspace as a means for such crimes (phishing, pharming, virtual fraud, and other related crimes).
- **Attacks against critical infrastructures through the cyberspace:** An alteration in the operation of critical infrastructures (both physical and information infrastructure) carried out by electronic means, e.g. the large-scale disruption of financial systems, interference of basis services, physical damage to physical structures and other related attacks.

All the above risks and threats affect the confidentiality, integrity, availability and traceability of information assets in the cyberspace and, in the medium-term this may affect the country's development in cyberspace, thus depriving us from the benefits associated with the digital government, ways of social organisation facilitated by cyberspace and threats to the security of people and institutions in this field. Some cases may fit in more categories than the ones described herein.

2. RISKS AND THREATS IN THE GLOBAL CONTEXT

At a global scale, there are many examples of cyber attacks consisting in espionage activities and distributed denial of service (DDoS) attacks in the Internet. Likewise, the large-scale interception of telecommunication networks, the failure of Internet services, espionage activities against governments and companies, as well as attacks against critical infrastructures such as banks and Government services, have been regularly in the news. There is also plenty of evidence with regard to legal abuses in the request for data to diverse providers of digital goods and services by countries where such providers are based.

Some cases worth mentioning are: Iran (2010), whose nuclear centrifuges were disabled by a computer virus especially designed for such purpose; Estonia (2007), where part of its critical infrastructure was disabled for weeks; disclosures by Edward Snowden (2013) about widespread espionage activities by the United State's intelligence agencies -which scope is still undetermined due to the number and regularity of such disclosures; and espionage activities against companies in the defence field (Lockheed, 2011) and entertainment (Sony, 2014),also in the US, which scope seriously compromises the economic interests and fundamental rights of people around the world.

3. RISKS AND THREATS IN A REGIONAL CONTEXT

Regionally, the countries that have reported the highest number of cyber attacks in Latin America were Brazil, Argentina, Colombia, Mexico and Chile. Accesses and information theft from infected computers - called *botnets* - were widespread in the region. There was even a specific type of malicious code called *dorkbot* that generated over 80K actions against the virtual system, with higher concentrations in Chile (44%), Peru (15%) and Argentina (11%)[17].

4. MALICIOUS ACTIVITIES DETECTED IN THE STATE'S CONNECTIVITY NETWORK

In Chile, the State's Connectivity Network (RCE) is affected by many malicious or suspicious activities. There is an incident record related with distributed denial of service (DDoS) attacks or alterations in Government website's operations, with an increasing number of these incidents starting in 2010. Likewise, in 2015, at a general level, administrators of the Government network spotted the following patters:

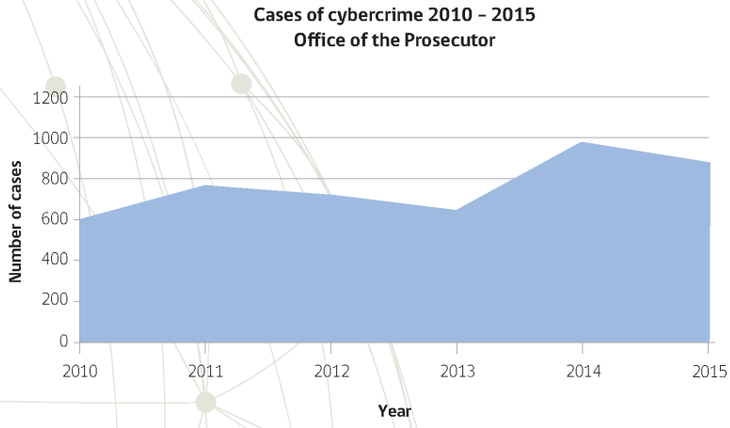
17 Prandini, P. & Maggiore, M. 2013. Op. Cit.

Number of Records	Description
58375435	Attempts to access information in network devices through SNMP protocol.
45903511	Scanning of device administration ports in switch, router or security platforms.
19745086	Web flow with password transfer in clear text (no encryption).
7805544	Detection of DNS dynamic updates.
5570661	Detection of TFTP flow (file transfer) by using tftp protocol.
4463394	Detection of portmap flows.
3359194	Detection of anomalous traffic in DNS ports.
2479277	Detection of remote desktop flows.
2077435	Detection of DNS queries by domains recognised as using malware.
2023403	Detection of recognition by PING.
1451708	Scanning of device administration ports in switch, router or security platforms.
1428461	Detection of wordpress access (key components).
1400697	Detection of MORTO malware.
1120311	Detection of NON encrypted traffic through a port usually used to transmit encrypted traffic (443).
1106303	Detection of access to forbidden areas in websites.
1025252	Flow of credentials in clear text of wordpress login (used in Government websites).

Patterns detected in the State's Connectivity Network (RCE) in 2015.
(Source: IT Division of the Ministry of the Interior, 2016).

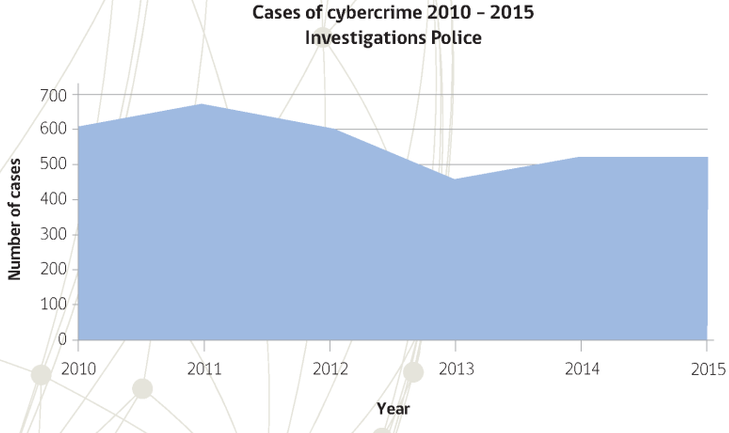
5. CYBERCRIME IN CHILE

According to figures provided by the Office of the Prosecutor, regarding cybercrime between 2010 and 2015, the number of cases submitted with the name "computer-related crime" was 4,648 cases, distributed as described below:



Cases submitted as cybercrime in 2010-2015 by the Office of the Prosecutor, related only with the types of offences set out in Law No. 19,233 (Source: ULDDECO, Office of the Prosecutor, 2016[18]).

Likewise, according to the data provided by the Investigations Police (PDI), during 2010-2015, a total number of 3,370 investigations distributed as described below:



Number of cybercrime investigations carried out in 2010-2015 by the PDI (Source: Cybercrime Brigade, PDI, 2016).

The *Carabineros* Police, on their part, have identified different types of illicit behaviour in the cyberspace at a national level, the most common ones being the fraudulent access to systems; the purchase, sale and storage of child pornography; computer sabotage, and illicit banking operations (phishing).

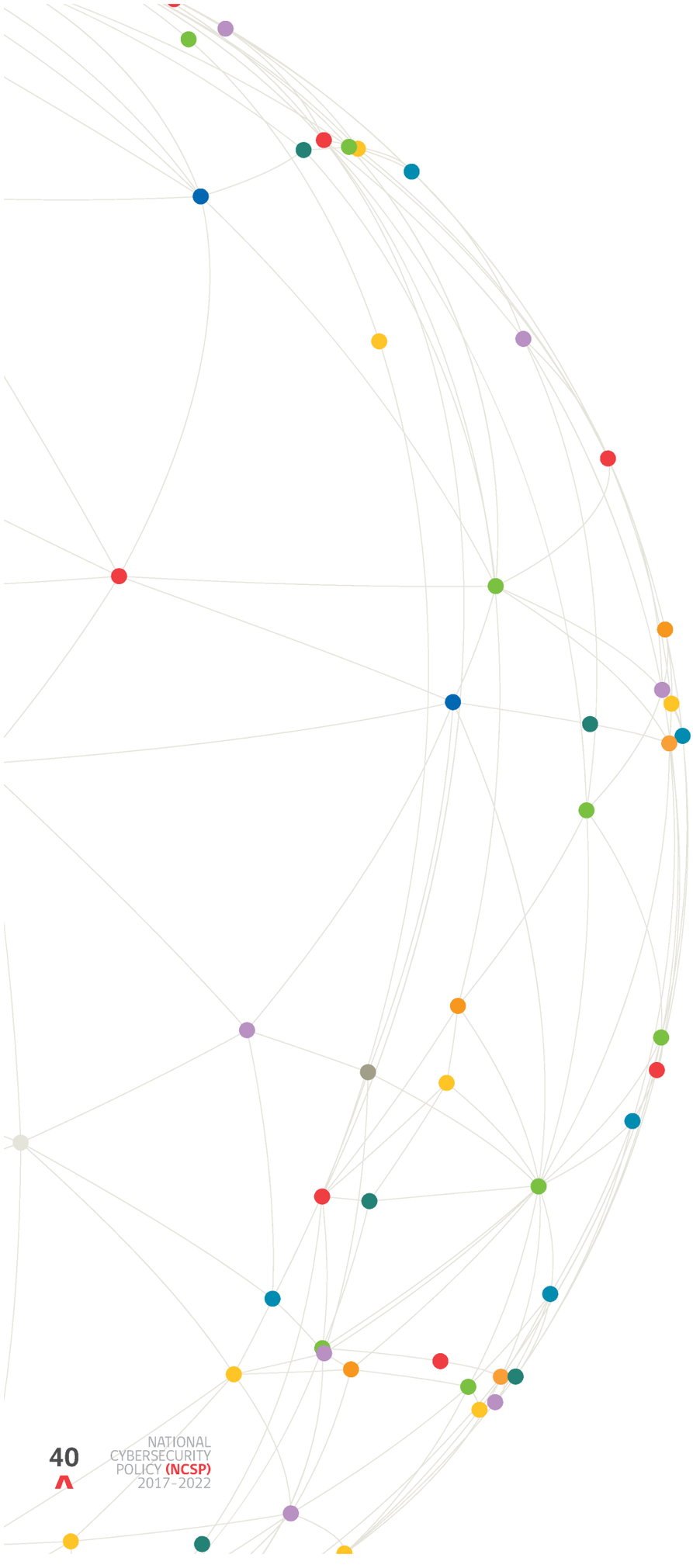
18 Chilean Office of the Prosecutor. A brief description of the current state of regulations and sentences in Chile regarding cybercrime. Specialised Unit for Investigating Money Laundering, Economic Crimes, Environmental Crimes and Organised Crime. As stated in the document mentioned, data presented are not the real total number of the cases as many of them are reported as fraud (Page 6).

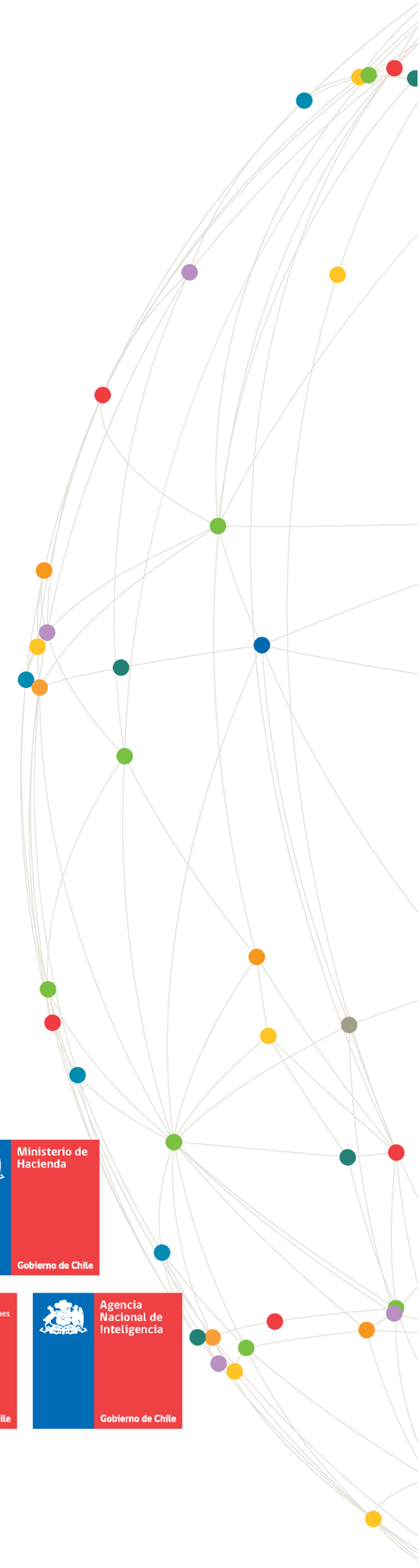
Likewise, cybercrime perpetrated in Chile confirm the cross-border nature of illicit acts in the cyberspace, specifically regarding the fraudulent use of credit and debit cards, where people from different nationalities have been found to plan and perpetrate such crimes.

Conclusion

The information contained in this document represent a threat for the confidentiality, integrity, availability and traceability of information in the cyberspace, which affects all users and deprives them from using cyberspace in a safe fashion, violating state and trade secrets and threatening people's fundamental rights, especially the rights connected with the protection of private life and communication inviolability.

For the reasons described above, it is essential to have policies in place to manage and minimize risks take into account such risks and threats, especially with regard to critical information infrastructure, with proper consideration of the special regulation set out for the purchase and operation of technological solutions and taking into account the international context in the field of cybersecurity.





CICS Comité Interministerial sobre Ciberseguridad

www.ciberseguridad.gob.cl

Subsecretaría del Interior
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ministerio de Relaciones Exteriores
Gobierno de Chile

Subsecretaría de Defensa
Gobierno de Chile

Ministerio de Hacienda
Gobierno de Chile

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

Ministerio de Economía, Fomento y Turismo
Gobierno de Chile

Ministerio de Justicia y Derechos Humanos
Gobierno de Chile

Subsecretaría de Telecomunicaciones
Gobierno de Chile

Agencia Nacional de Inteligencia
Gobierno de Chile