PRIVACY INTERNATIONAL

ADC / Asociación por los Derechos Civiles

Special report

Who's watching the Watchers?

A comparative study of intelligence organisations oversight mechanisms in Latin America

ADC / Asociación por los Derechos Civiles

con el apoyo de

PRIVACY INTERNATIONAL

policy paper

Who's watching the watchers? A comparative study of intelligence organisations oversight mechanisms

In societies that are in the process of transition towards democracy, democratic control of intelligence organisations is both an indispensable requirement and a pressing need. In many cases, the most serious human rights violations committed by dictatorial governments were intrinsically linked to draconian surveillance and control systems. Systematic spying on trade unions, students and dissident groups was a common feature of 20th-century dictatorships. The persistent violation of citizens' privacy increased the efficiency of crimes committed by the state, which new democracies formed in the late 20th century have since sought to avoid.

Intelligence organisations have undergone a major transformation as a result of those political changes. Democratic societies need professional intelligence services formed by highly trained and skilled staff, with access to sufficient resources to meet the demands of national defence and the fight against terrorism. However, democracies also need their political bodies to exert strict controls to ensure that the secrecy that usually shrouds intelligence activities does not become an excuse to abuse or violate rights. Attaining this goal is a considerable challenge: many ostensibly consolidated democracies have not yet managed to assert their power over intelligence organisations, which retain levels of autonomy that are incompatible with a democratic community.

This Association for Civil Rights (ADC)[1] document has two objectives. First, to introduce several basic concepts linked to the sphere of intelligence in the context of the global debate on the scope of surveillance activities carried out by states. Second, to review the various types of democratic control models in existence around the world, with a particular emphasis on Latin America. Through these two objectives, we seek to inform the public debate that Argentina needs to have on the way our democracy controls its intelligence services.

I. Some basic intelligence-related concepts

Intelligence is usually understood as a *process*, a *product* and an *organisation* (Bruneau and Boraz, 2007: 7).

1. **Process**. It is the means through which a certain kind of information is requested, collected, analysed and disseminated, and the way in which certain activities are conceived and carried out. It is information aimed at meeting the needs of policymakers in the areas of foreign policy, defence and internal security, understood in regard to the threats to the democratic system, though it also includes counterintelligence and covert operations (Ugarte, 2012: 16).

2. **Product**. The outcome of these processes, that is to say, the information obtained through the intelligence process and the intelligence operations themselves.

3. **Organisations**. They are the operational units that carry out intelligence information collection, analysis and dissemination activities. In general, it is not a single organisation, but instead a set of state actors located at various levels of the governmental structure, which is known collectively as the *intelligence community*.

Intelligence has at least two goals: to inform public policies and to serve as a support for operations linked to the defence of state security. And these goals are achieved through four intelligence activity *functions*: collection, analysis, counterintelligence and covert activities.

Collection

Intelligence organisations collect information. But how do they do it? There are various types of intelligence, as described in Figure 1.

1 This paper was produced in May 2014 by Ramiro Álvarez Ugarte and Emiliano Villa, from the Privacy Area of ADC.

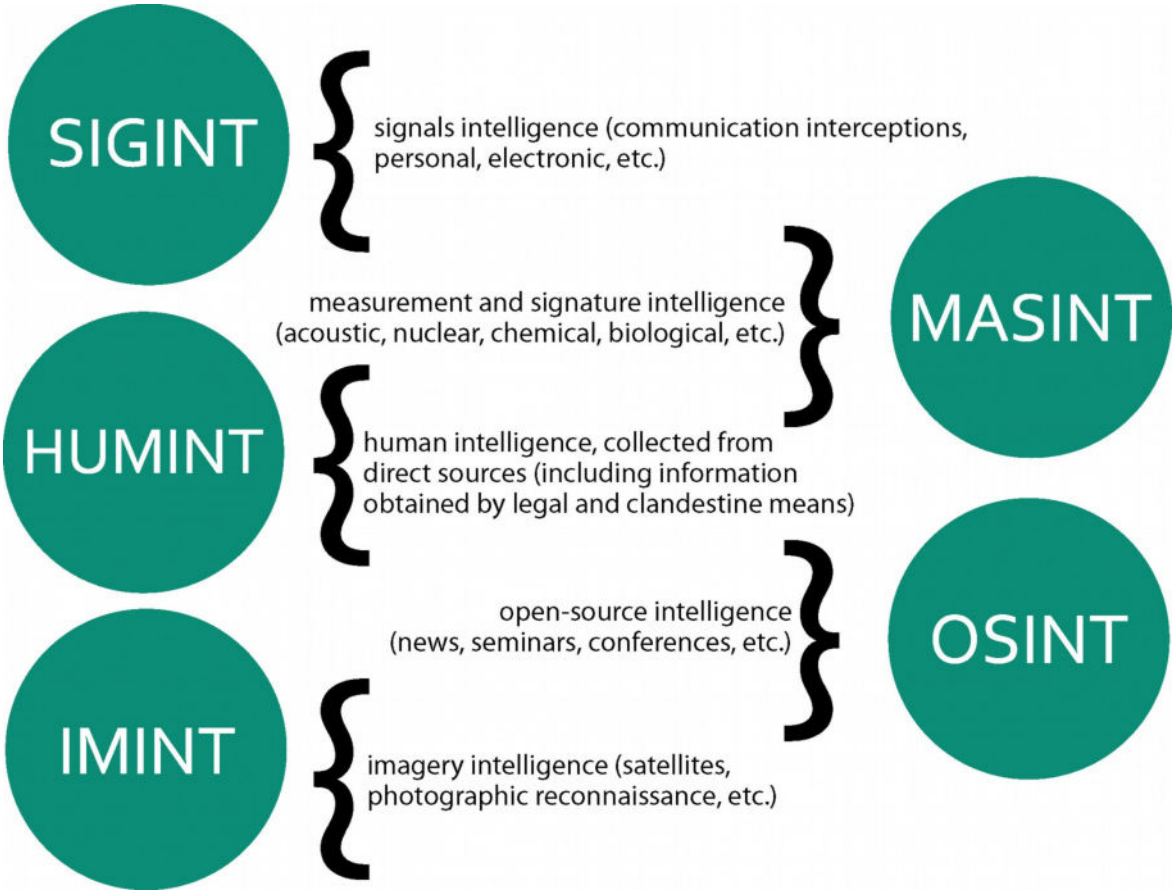


Figure 1. Types of intelligence activity

To a lesser or greater extent, some of these activities conflict with citizens' human rights. For example, open-source intelligence (OSINT) collects information from public and unrestricted sources and – generally– does not appear to be contradictory to any right. In contrast, signals intelligence (SIGINT) is based on the interception of private communications and is therefore only permissible in exceptional cases and, generally speaking, with a court order.

Analysis

Information in its own right is not useful: it has to be analysed. According to Bruneau and Boraz, analysis is the best aptitude and the main challenge for intelligence practitioners (Bruneau and Boraz, 2007: 9). It is about examining various types of information and drawing conclusions from that analysis. Information collection and analysis go hand in hand, and they follow a cycle that is described in Figure 2.

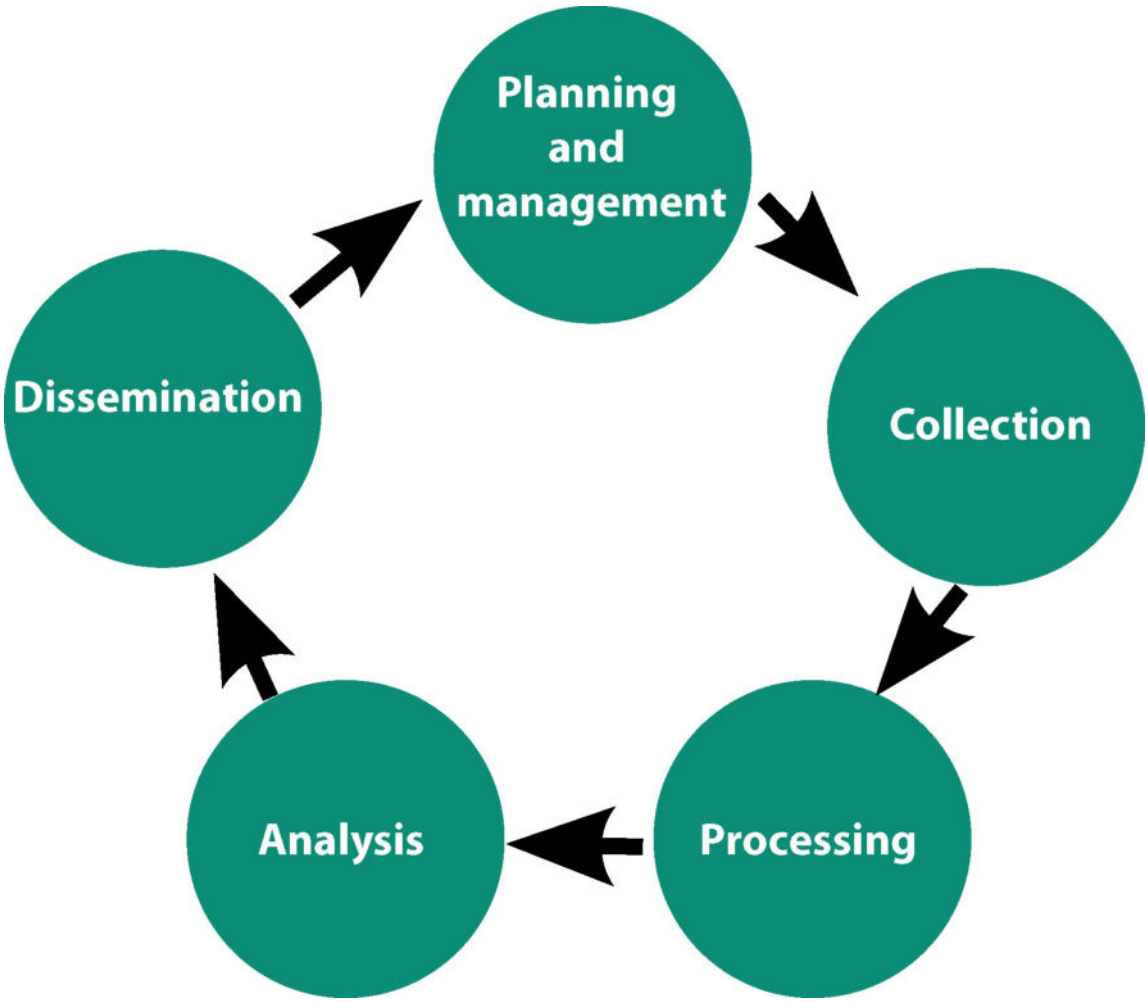


Figure 2. Intelligence circuit. Adapted from Bruneau and Boraz, 2007: 9.

Bruneau and Boraz provide a hypothetical example.

"It begins with the policymaker and his planning staff (for example, in the U.S., the president and his National Security Council staff) expressing a need for intelligence information to help them make a national security-related policy decision. Intelligence managers convert these requests into collection plans to acquire the information. The raw data are collected by various intelligence methods [...] and given to analysts for integration, evaluation, and analysis for producing finished intelligence products (written reports or oral briefings, for example). These products are disseminated to the consumers (in this example, the president and planners of the NSC), who provide feedback to the intelligence managers for additional or more focused information" (Bruneau and Boraz, 2007: 9).

Counterintelligence and covert actions

It is an intelligence activity that concentrates on protecting the state and its secrets and, according to Ugarte, it is one of the areas most difficult to control properly. There are various definitions of what counterintelligence actually is, though it is generally accepted that its aim is to tackle external threats. In Argentina, and according to

Article 2.2 of Act 25520 (*Ley Nº 25520*), counterintelligence is defined as the activity inherent to the field of intelligence, performed for the purpose of avoiding intelligence activities by actors that represent threats and risks to the security of the national state. Covert actions are those aimed at exerting influence over other countries through surreptitious mechanisms.

II. Intelligence, security and defence

Accurately defining intelligence-related issues in democratic societies is a considerable challenge, especially in countries seeking to establish democratic oversight mechanisms over autonomous structures that, in the past, were linked to human rights violations and crimes committed by dictatorial governments. This challenge is particularly significant in countries such as the ones in Latin America that, at some time in their history, lived under the paradigm of the "national security doctrine". This doctrine allowed a person to be characterized "as 'subversive' or as an 'internal enemy,' and this could be anyone, who genuinely or allegedly supported the fight to change the established order" [2]. In the Case of Goiburú *et al. v.* Paraguay, the Inter-American Court of Human Rights held that:

"Most of the Southern Cone's dictatorial governments assumed power or were in power during the 1970s, […] The ideological basis of all these regimes was the 'national security doctrine,' which regarded leftist movements and other groups as 'common enemies,'[…]"

This circumstance led many countries in the region to include the reform of their intelligence systems as part of their democratisation processes. For example, in Argentina's National Intelligence Act (*Ley de Inteligencia Nacional*), a section referring to the *protection of the inhabitants' rights and guarantees* is included as Title II. It contains several explicit prohibitions for intelligence organisations associated with past abuses[3].

2 Inter-American Court of Human Rights. *Case of Molina Theissen* v. *Guatemala. Judgment of May 4, 2004*. Series C No. 106, para. 40(2).

3 According to Article 4 of National Intelligence Act 25520, no intelligence organisation shall: // 1. Perform any repressive tasks, possess compulsive faculties, fulfil, in its own right, any policing or criminal investigation functions, unless it has a specific warrant issued by a competent judicial authority in the context of a particular case subject to its jurisdiction or it is authorised by law to do so. // 2. Obtain information, produce intelligence or store data on people, by the simple fact of their race, religious faith, private actions or political opinion, or membership of or belonging to party, social, trade union, community, cooperative, care, cultural or labour organizations, or by any other lawful activity that they carry out in any sphere of action. // 3. Exert any influence over the institutional, political, military, police, social or economic situation of the country, over its foreign policy, over the internal affairs of legally constituted political parties, over public opinion, over people, over broadcast media or over legal associations and groups of any type. // 4. Disclose or divulge any type of information, acquired in the performance of its functions, relating to any inhabitant or legal person, whether public or private, unless there is a judicial dispensation or order to do so.

However, the 2001 National Intelligence Act must be read in conjunction with the 1988 National Defence Act (*Ley de Defensa Nacional*) and the 1991 Internal Security Act (*Ley de Seguridad Interior*). Together, these three Acts seek to delimit activities and set out precise prohibitions with the explicit aim of preventing abuses. One of their main objectives is to make a precise distinction between *national defence* and *national security*[4].

According to Saín:

> After the state terrorism perpetrated by the military government during the National Reorganisation Process (PRN) came the redefinition of civil-military relations in terms of imposing civil-society control over military institutions, which, among other issues, included favouring national defence as a sphere exclusively organised and operated by the armed forces, reformulating the institutional missions and functions of the armed forces and, in particular, dismantling the set of legal and institutional prerogatives over internal security that these forces had or, in other words, *demilitarising internal security* (Saín, 2001).

In 1988, The National Defence Act clearly delimited the armed forces' scope of action to tackling external aggressions. And in 1992, the Internal Security Act underpinned this concept by excluding the armed forces from issues relating to internal security except under exceptional circumstances, where the Executive deems that it cannot deal with a specific threat with conventional security forces (Federal Police, Naval Prefecture, National Gendarmerie and provincial police forces).

More recently, Decree 727/06 (*Decreto Nº 727/06*) regulating the National Defence Act insisted upon this distinction. According to this Decree, the National Defence System "cannot contemplate hypotheses, instances and/or situations pertaining to the sphere of internal security, as delimited by Internal Security Act 24059, in the formulation of its doctrine, in planning and training, in forecasting the procurement of equipment and/or means, or in activities relating to intelligence production". The same Decree restrictively defined *external aggressions*, stating that they are "aggressions perpetrated by armed forces belonging to another/other states/s". New threats such as terrorism and drug trafficking fell outside the armed forces' jurisdiction. Thus, the legal system seeks to establish an impermeable membrane between security and defence (De Vergara, 2009).

Despite this difference established by the legal system, intelligence activities seem to cross the divide proposed under the Internal Security Act and the National Defence Act. Indeed, the definition of national intelligence under Act 25520 refers to the Nation's internal and external security. However, it distinguishes between *criminal* and *military strategic* intelligence and therefore appears to fit the categorical distinction made by the Internal Security Act and the National Defence Act.

In the National Intelligence Act, *criminal* intelligence refers to specific criminal activities that, because of their nature, magnitude, foreseeable consequences, dangerousness or modalities, affect the inhabitants' freedom, life or property, their rights and guarantees, and the institutions of the national representative, republican

4 According to Article 4 of the National Defence Act, in order to clarify issues related to National Defence, the fundamental difference between National Defence and Internal Security should be taken into account at all times.

and federal system, as established by the National Constitution. As can be seen, it is a definition that aligns with the definition of *internal security* contained in Act 24059 (*Ley Nº 24059*). In charge of this is the National Directorate of Criminal Intelligence, which reports to the Secretariat of Internal Security.

Military strategic intelligence, on the other hand, is linked to knowledge of the capabilities and weaknesses of the military potential of countries of interest from a national defence perspective, and of the geographical environment of operational strategic areas, as determined by military strategic planning. In charge of this is the National Directorate of Military Strategic Intelligence, which reports to the Ministry of Defence.

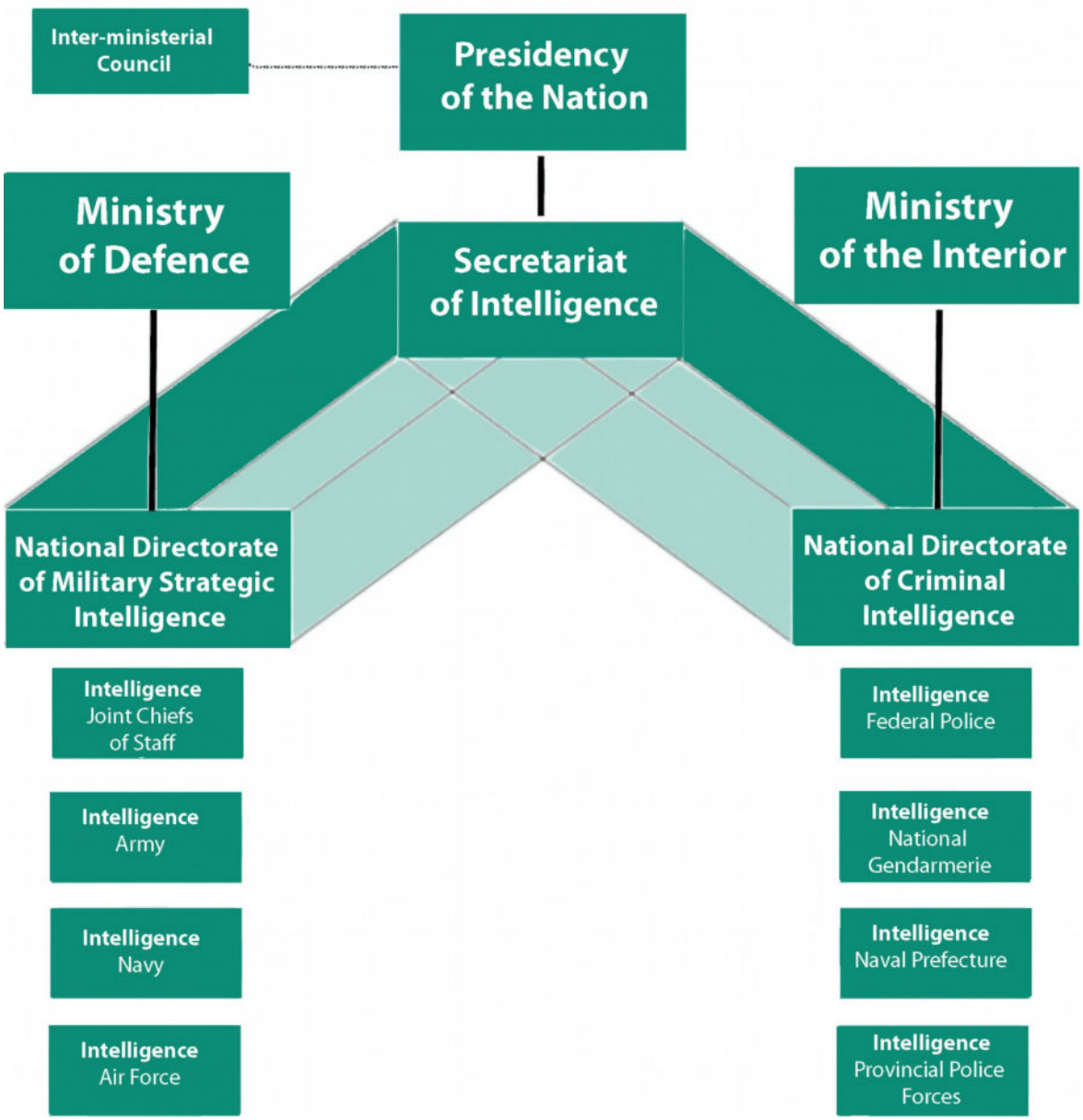


Figure 3: Organisation chart of the national intelligence system

The organisation chart of the national intelligence system in Figure 3 clearly shows the division of intelligence tasks within the State. It should be noted that none of the current regulations authorise political intelligence tasks, and there is no organisation whose function includes this type of activity. In fact, Title II of Act 25520 specifically seeks to prevent this type of abuse. However, the legal system's definitions serve little purpose unless they are accompanied by effective oversight mechanisms that transform legal requirements into specific practices within the controlled organisations.

III. Controlling intelligence activity

Democratic authorities' control of intelligence activities is closely linked to the issue of *democratisation* of such bodies. Swenson and Lemozy suggest that this is linked to the evolution "of a national system that ranges from the use of an institutional framework to address primarily internal security issues that threaten the survival of principal officials of the state (a Security State), to its use to ensure the survival of democratic principles in a State of Law [...]" (Russell and Lemozy, 2009: 2).

Russell and Lemozy's characterisation indicates a process of change: the democratic state *asserts* its power over state bodies, which unsurprisingly adopt the characteristics of the places they come from. Thus, many intelligence organisations around the world are strongly hierarchical and assign priority to military issues because their origins can often be traced back to military intelligence (Russell and Lemozy, 2009: 8). In addition, and particularly in societies in transition, intelligence organisations formed part of the web of security forces tasked with repression under the former authoritarian regimes. According to Bruneau and Boraz, over time these organisations gained independence from public policymakers and managed to keep themselves isolated from any type of scrutiny (Bruneau and Boraz, 2007: 12).

Consequently, democratic oversight of intelligence organisations is a considerable challenge: the organisations themselves try to resist change and the legislators tasked with implementing oversight efforts– or in some cases leading them – lack the necessary knowledge about what they are expected to oversee. In this respect, it makes sense to evaluate the various oversight models used around the world from a comparative perspective.

For a start, intelligence systems usually report to the Executive, either in the figure of President in a *presidential* system or of Prime Minister in a *parliamentary* system. This allows us to make an initial distinction between different oversight systems, depending on whether the supervising body is within the Executive (*internal*) or outside the Executive (*external*).

Depending on the body performing the activity, oversight may be *administrative*, *legislative* or *judicial* (Gasparini, 1995: 531). There may also be *horizontal* and *vertical* controls: the former involve a *controlling* body and a *controlled* body that are

peer counterparts, while in the latter there is a hierarchical relationship between them, both political and administrative (Dromi, 1973: 91). Furthermore, *horizontal* oversight mechanisms are divided into *intra-organic*, operating inside the body's own internal legal and administrative organisation, and *inter-organic*, operating outside the intelligence body itself.

The various oversight models used around the world suggest that, in practice, the issue is more complex than would appear from the classification outlined above. For instance, the parliamentary control system sometimes observes the composition of the legislative body and, in a bicameral parliament, two specialist (or select) committees are tasked with outlining the monitoring tasks[5]. On other occasions, however, bicameral parliaments choose to have unified oversight bodies, in which members of both chambers are represented.

There are various possibilities within the Executive too. Although it is an *internal* control because it is performed within a specific hierarchical structure and within the context of one of the three powers of the state, it is vital to distinguish between internal accountability mechanisms *within the intelligence body itself* and those that are within the Executive yet external to those bodies. This happens, for example, when control is carried out by a ministry that has no connection with the intelligence system (Ugarte, 2012: 35).

Analysed in greater detail below are the various types of oversight models in existence around the world.

Executive body oversight

Many countries choose to establish accountability schemes within the sphere of the Executive. However, countries that choose this type of oversight usually have parliamentary systems, where the division between the executive and the legislative branches is not as categorical as it is in presidential systems. In fact, there are many political and functional relations between the parliament and the cabinet. There are various alternatives within this type of oversight.

Oversight sometimes falls on a minister, generally of the Interior or of Justice. In practice, this type of oversight establishes an instance of political responsibility prior to that of the heads of state, meaning that irregular handling or abuses within the intelligence organisations generally entails the direct responsibility of the minister tasked with control, but not that of the Head of Government (Ugarte, 2012: 33). This intermediate political responsibility is the safety valve chosen by many parliamentary systems such as Belgium, Canada, Spain, France, the Netherlands and the United Kingdom.

In this type of oversight system, the minister tasked with supervision is also the person politically responsible for intelligence activity and, as such, will be in charge of formulating policies and strategies on intelligence issues (Ugarte, 2012: 35). Thus, the

5This is the case, for example, in the Unites States of America, where select committees on intelligence operate in both chambers of the Congress.

activity of *management* is linked to the activity of *oversight*, which, according to Bruneau and Boraz, may suffice in certain cases (Bruneau and Boraz, 2007: 15).

However, many experts consider that the delegation of oversight to a cabinet minister may *politicise* intelligence activities. According to Bruneau and Boraz, the main problem associated with an oversight system based purely on the Executive is the danger that the intelligence apparatus may be used for non-democratic ends (Bruneau and Boraz, 2007: 15), such as when intelligence services are used for local political espionage.

There are moderated ministerial dependence alternatives like those in Italy, for example. There, the Prime Minister has a coordination and oversight body that reports to her: the Security Intelligence Department (DIS). In addition, there is an assistance and advisory council formed by a minister without portfolio, to whom she can delegate powers on intelligence matters not exclusively assigned to the Prime Minister. According to Ugarte, such delegation allows for a better allocation of tasks within the internal organisation of intelligence activity and, at the same time, reduces the risk of politicisation (Ugarte, 2012: 34).

Parliamentary oversight

Parliamentary oversight functions as one of the external accountability mechanisms that many countries prefer and, according to some, it is the most effective. Such control is exercised through specific committees, set up on a permanent basis, and formed by subject experts. Their origin can be traced back to 1976, when the United States Senate issued resolution 400 creating the *U.S. Senate Select Committee on Intelligence*[6]. The following year, a parallel committee was created in the House of Representatives.

In countries that have a unicameral Congress, the committee exercising parliamentary oversight of this activity usually operates on a permanent basis, and is formed by members of the single chamber. However, in bicameral systems – like Argentina's – the type of oversight is different. In some cases, there is a single committee formed by members of both chambers, as is the case in Argentina, Brazil, the United Kingdom and Italy. In others, there is an oversight body in each chamber of the Congress, as is the case in the United States and Spain. According to the comparative study conducted by José Manuel Ugarte, a unified oversight system is preferred by countries that opt for parliamentary controls (Ugarte, 2012: 92).

While there are good reasons to assume that the *Bicameral Committee* model is better than the other models mentioned, particularly as it is the most widely used around the world, some observers see advantages in the United States' system because they consider that, besides exercising oversight of intelligence activity itself, it also allows for the Committees to control each other, thereby considerably reducing the risks associated with co-option to which highly political organisations are exposed (Sneider, 2004: 17; Ugarte, 2012: 92). In contrast, other observers maintain that a single oversight system allows for much stricter control over the secrecy of issues

6 Select Committee on Intelligence, Res. 400, 94th Cong., 2d session (1976).

addressed in it, making the Committee more effective and capable of taking action to resolve issues quickly (Halchin and Keiser, 2012).

Judicial oversight

Judicial oversight of intelligence activity basically refers to the review and authorization of activities involving an invasion of citizens' privacy. According to Ugarte, the objective of this type of oversight is to check that the exclusive purpose of such actions is warranted, and that intrusion into the private sphere is kept to a minimum (Ugarte, 2012: 163).

In principle, this type of oversight is not specific to intelligence systems. In fact, its origin can be traced back to the Judiciary as the place where citizens go to defend their rights. Hence, when those rights are violated, it is the Judiciary that is in principle tasked with remedying and stopping those abuses. Regarding intelligence matters, however, some countries have incorporated activity-specific oversight systems into their courts, while others have kept the courts outside of the control system.

The most obvious example of judicial oversight *incorporated* into the intelligence system are the courts created in the United States by the *Foreign Intelligence Surveillance Act* of 1978. There were many years of debate in the United States about whether or not electronic surveillance measures were covered by the Fourth Amendment, which requires judicial intervention in order to access people's private papers and homes. Constant tension therefore developed between the Executive and the Supreme Court: while the former wanted to use these techniques for internal security issues, the Supreme Court in the *Katz* and *Keith* cases[7] took an increasingly committed stance towards the need for a court order. The Congress responded by creating highly controversial special courts, known as *Foreign Intelligence Surveillance Courts* (also called *FISA Courts*), in order to meet requests to authorise interceptions linked to external intelligence, and which operate through secret procedures.

A pragmatic approach to oversight

While we have tried to distinguish between the various control models, there is no reason to assume that they cannot be superimposed. Indeed, during the legislative review process that led to internal espionage being carried out by the FBI and the CIA against the peace movement in the 1970s, both the Executive and the Congress sprung into action. There were judicial oversight at all times, especially when the abuses that were made public involved the violation of citizens' rights (Boraz, 2007: 28). In the United States today, there are multiple oversight systems operating in the three powers of the state, and other countries also apply similar practices. It is important to highlight that the various oversight models are not mutually exclusive, but are complementary.

7 The cases are Katz *v.* United States, 389 U.S. 347 (1967) and United States *v.* United States District Court, 407 U.S. 297 (1972) (also known as the Keith case).

IV. The Argentine legal framework

As mentioned earlier, there are three Acts that need to be studied together in order to understand the issue of intelligence organisation oversight in Argentine democracy. They are the 1988 National Defence Act, the 1991 Internal Security Act and the 2001 National Intelligence Act. The three Acts form the legal architecture for the state's response to the issue of civil-military relations in the transition stage. All three seek to set limits, establish limited scopes of action and introduce strict prohibitions. National Intelligence Act 25520 tried to attain this objective in regard to intelligence organisations, but Internal Security Act 24059 had previously regulated the matter.

Situation prior to Act 25520

In 1991, Internal Security Act 24059 created the *Bicameral Committee for the Oversight of Intelligence and Internal Security Bodies and Activities*. With this Act, Argentina was the first country in Latin America to establish external control of its intelligence activity. According to Article 33 of the above-mentioned Act, the Committee was tasked with the mission of oversight and control of the existing intelligence and internal security organisations and bodies, of those created by that Act and all those that might be created in the future.

According to the then national deputy Jesús Rodríguez, although the work of the committee got off to a promising start, it ended up being a lacklustre experience.

> It should be said that the Bicameral Committee for Oversight was granted limited powers of external oversight and control, and no powers to make viable the internal oversight and control of the functional organic dynamics and structure of the State's intelligence and information organisations and activities; these tasks were fundamentally based on the control of intelligence and information operations and policies, and on the funding and budgetary control of those activities and organisations[8].

However, in some situations, it did manage to act in the face of irregularities that became public. For example, as noted by Ugarte, in mid 1993, the Committee intervened in cases of illegal intelligence on trade unions and student organizations (Ugarte, 2012: 170). The Committee managed to discover that this *political* surveillance had been backed by a Ministry of the Interior directive, which was the reason why the Committee recommended its repeal. The request was accepted by the Ministry at that time (Ugarte, 2012: 171).

Situation after Act 25520

The legal structure

National Intelligence Act 25520 was passed in 2001. Regarding the control and oversight of the activity, it replaced the committee created by the Internal Security Act with the current *Bicameral Committee for the Oversight of Intelligence Bodies and*

8 *Diputado Jesús Rodríguez y otros, Proyecto de Ley de Control de las Actividades y Gastos de Inteligencia, Cámara de Diputados de la Nación, Expte. 5406-D-97, presentado el 9/10/1997* (Deputy Jesús Rodríguez et al., Bill on the Control of Intelligence Activities and Expenditure, Chamber of Deputies of the Nation, File 5406-D-97, submitted 9/10/1997).

Activities. The Bicameral Committee created by the Internal Security Act was then limited to the oversight of internal security bodies and activities.

According to Article 32 of the National Intelligence Act:

> The National Intelligence System's organisations shall be supervised by the Bicameral Committee, for the purposes of overseeing that their operation strictly complies with the constitutional, legal and regulatory rules in force, verifying strict observance of and respect for the individual guarantees enshrined in the National Constitution, and with the strategic guidelines and general objectives of National Intelligence policy.
>
> The Bicameral Committee shall have wide-ranging powers to control and investigate *proprio motu*. Upon the Committee's request, and in accordance with the procedures set out in Article 16, the National Intelligence System's organisations shall supply the information or documentation that the Committee asks for.

Act 25520 added aspects relating to the verification of proper operation as regards the political directives of National Intelligence. That means that the Bicameral Committee must give an opinion on any draft legislation that may be connected with intelligence activities. In addition, it must prepare a secret annual report on issues relating to the National Intelligence System's effectiveness in terms of operation and organisation, and submit it to the National Executive and the National Congress[9].

Similarly, the Committee is also tasked with supervising interceptions of private communications made by the Secretariat of Intelligence. Such oversight applies to interceptions made in the course of intelligence and counterintelligence activities, as well as those called for in crime investigation. Judicial authorisation is required in both cases (Ugarte, 2012: 175). This is so because Act 25520 granted the Secretariat of Intelligence's *Directorate of Judicial Surveillance* an exclusive monopoly over the interception of telephone and electronic communications, a choice that Ugarte considers questionable because the Secretariat of Intelligence reports to the Executive, and there are multiple signs to suggest that the Secretariat has been used for political ends (Ugarte, 2000).

Operation in practice

The Committee began operating in earnest in 2004, when sufficient funds were allocated to it for the appointment of financial auditors and advisors, without whom it was impossible to articulate its functions[10]. Four sub-committees were formed for different functions: intelligence staff training, intelligence expenditure supervision, the system's constituent organisations' compliance with the National Intelligence Plan, and control of communication interceptions.

The Committee's activities are kept strictly under wraps: under the *Comisiones* (Committees) tab of the websites of both the *Honorable Cámara de Diputados de la Nación-República Argentina* (Chamber of Deputies) and the *Honorable Senado de la Nación Argentina* (Senate), there is no information about its meetings, reports or

9 *Cf. Ley Nº 25520, art. 33.4* (Act 25520, Article 33.4).

10 The Bicameral Committee sets its own budget. It constitutes a specific programme within the budget (Code 25 Parliamentary Control of the Intelligence System – Bicameral Committee for the Oversight of Intelligence Bodies and Activities Executive Unit within the National Congress's budget).

work agenda. The only report that the Committee has to submit to the Congress and the Executive, as mandated by Article 33.2 of the Act, is the annual report, and it is expressly classified as secret. After consulting with various deputies in office for several years, ADC found that none of them had ever received a copy of that report.

Another significant fact is that this body's control activity is severely limited by Article 16, which makes a wide-ranging and broad classification of intelligence activities, the staff assigned to them, the documentation and the databases of the organisations, and Article 32.2, which regulates the way in which the National Intelligence System has to supply the Bicameral Committee with information. Similarly, Articles 11 and 20 of Regulatory Decree 950/2002 (*Decreto Reglamentario Nº 950/2002*) makes the Committee's ability to access classified intelligence documentation dependent on the Secretariat of Intelligence's authorisation: thus, the Regulatory Decree makes the performance of acts of control subject to the will of the body being controlled (Ugarte, 2012: 189).

In late December 2012, ADC and the Latin American Institute for Security and Democracy (ILSED) submitted an information access request to the *Bicameral Committee* within the context of the Citizen's Initiative for Control of the Intelligence System (ICCSI). Although intelligence-related issues are usually secret, the information requested is not: ADC and ILSED wanted to know the number of meetings held in a three-year period; the reports produced for the purpose of appointing the last three Secretaries of Intelligence; the number of requests for reports made by the Committee to the Secretariat of Intelligence in a three-year period, etc. The request was not answered and, in February 2014, after nearly a year of demarches in Congress to secure a reply, a writ of amparo was filed to access the requested information.

V. Control systems in Latin America

Brazil

In Brazil, the intelligence system was reformed in 1999 and, as in the case of Argentina, should be understood as part of its process of transition towards democracy. In fact, the Brazilian intelligence system derives from the *National Information Service* (SNI) created in 1964 and strengthened during the last military dictatorship (Duarte, 2013).

"In this context, and free from oversight, the SNI began to increase its control over the information centres of the three armed forces and to expand its local networks so that they covered police services and other civilian organisations, including trade unions and public companies. It was even able to obtain veto power in Brazil's National Security Council – the highest body and inner sanctum of the military regime" (Duarte, 2013).

According to Duarte, it is no surprise that the organisation retained a considerable amount of power in the context of a *negotiated* transition towards democracy, such as that experienced by Brazil after 1974. Nevertheless, attempts at reform and control were made in the 1990s. The first step towards establishing democratic oversight on

intelligence activity was the passing of Act 9883 (*Lei Nº 9883)* of 7 December 1999, which constituted the Brazilian Intelligence System (SISBIN) and created the Brazilian Intelligence Agency (ABIN).

The Brazilian Intelligence Agency centralises intelligence in Brazil: it advises the President and plans, coordinates, supervises, controls and carries out the country's intelligence activities nationally. And that includes internal and external intelligence, and counterintelligence (Ugarte, 2012: 230).

The Act established the main oversight mechanism within the Executive, articulated through the *Joint Committee for the Control of Intelligence Activities*, which began operating in 2000 and, since then, has held two or three meetings a year (Ugarte, 2012: 239). According to Ugarte, the Committee has not taken a lead role in investigations of alleged irregularities, though it has summoned officials to provide explanations (Ugarte, 2003: 9).

Regarding oversight within the Executive, while there are bodies whose competencies include specific powers of control of this activity – the Director-General of the ABIN for internal oversight and the Chamber of External Relations and National Defence of the Government Council for external oversight, its functions do not appear to be aimed at carrying out permanent and routine supervision activities.

Finally, in Brazil – as in the majority of Latin American countries – there is no legislation specifically regulating judicial oversight. In fact, Act 9883 makes no mention of this, though certain basic tasks of intelligence activity do require judicial authorisation, such as telephone interceptions. It should be noted that, very recently, Act 12965 (*Lei Nº 12965*) of April 2014, also known as the *Civil Rights Framework for the Internet*) has established the need for a court order to access electronic communication data (Article 10.1).

Chile

Like many countries in the region, Chile has built its current intelligence system on a deep-seated reform of the system it inherited from the last military government. In fact, the restoration of democracy sought to dismantle the former system focused on the fight against Communism and the control and persecution of political dissidents.

The first step in this direction was the creation of the *Select Committee on Intelligence Services* in the Chamber of Deputies of Chile. In January 1993, that Committee produced a full report about the organisation of the activity, which until then had not been subject to any form of oversight (Ugarte, 2012: 279). Although that was a first step, it was not until State Intelligence System Act 19974 (*Ley Nº 19974 sobre el Sistema de Inteligencia del Estado*) was passed, which created the *National Intelligence Agency* of the Republic of Chile (ANI), that specific oversight of intelligence activity was formally organised. Until then, it only had a relatively small civil intelligence organisation with coordination functions limited to internal security in general, and to preventing threats to democratic institutions in particular.

ANI reports to the Ministry of the Interior, an instance of political responsibility distinct from the highest state authority, which, as seen earlier, some oversight models in parliamentary systems have adopted. Act 19974 also establishes parliamentary oversight over intelligence activity, but – in Ugarte's opinion – the powers it has are relatively modest because it lacks expressly investigative powers (Ugarte, 2012: 285).

Colombia

Until 2011 Colombia, had the *Administrative Department of Security* (DAS), a civil intelligence organisation reporting to the highest state authority, with powers on matters of internal and external intelligence, and counterintelligence, and typical police-related powers and functions, which included migration control, foreigner identification records and criminal identification records, among other activities. It also served as a National Office of INTERPOL[11]. However, Decree 4,057 of 2011 (*Decreto Nº 4.057 de 2011*) put an end to that organisation as a result of systematic irregularities that created a whole variety of scandals and shook the Colombian political system.

Indeed, all kinds of abuse were attributed to DAS. One of the first to become public was that of the *parapolitics* scandal linking DAS to paramilitary groups on matters of both administrative corruption and serious practices of persecuting social and trade union leaders[12]. One of the latest was the *chuzadas* scandal, which was revealed when *Semana* published an investigation in February 2009 documenting that this organisation had been illegally spying on leaders of the opposition, magistrates, journalists and state officials. It even discovered the existence of a manual for DAS operatives containing instructions on how to threaten journalists.

Act 1288 of 2009 (*Ley Nº 1288 de 2009*) was the Colombian parliament's response to the unleashed scandal. However, the Act was questioned by human rights organisations because it went through the ordinary legislative procedure: they argued that, as it was a precept that affected fundamental rights enshrined in the Constitution, the procedure for passing the Act should have been *Statutory*, thereby requiring an absolute majority. The Constitutional Court found in their favour in late 2010, and declared the Act unconstitutional.

That led to a new legislative process that culminated in the Intelligence and Counterintelligence Statutory Act 1621 (*Ley Estatutaria de Inteligencia y Contrainteligencia Nº 1.621*), passed on 17 April 2013, after it had been reviewed by the Constitutional Court. The new Act created a legal committee to monitor the intelligence and counterintelligence activities of the Congress of the Republic, and an

11 *Cf. Decreto Nº 643 of 2004, por el cual se modifica la estructura del Departamento Administrativo de* Seguridad (Decree 643 of 2004, modifying the structure of the Administrative Department of Security).

12 *Cf.* Observatorio de Derechos Humanos de la Coordinación Colombia-Europa-Estados Unidos. *La pesadilla del DAS*. Documentos temáticos No. 3, Bogotá: December 2006. See also, Revista Semana, *El DAS y los paras*, Printed Edition, article published February 2006. Available at: http://m.semana.com/portada/articulo/el-das-paras/75769-3.

advisory committee for intelligence and counterintelligence archives and data cleaning.

However, it does not seem to have stopped the abuses: In January 2014, *Semana* once again revealed illegal spying on important political actors, in this case the negotiators in the peace process talks being held in Havana[13].

Peru

As in the case of Chile, the control of intelligence activity arose after the collapse of the government headed by Alberto Fujimori, a time when there was much questioning of the illegal activities carried out by the *National Intelligence Service* (SIN) under the command of Vladimiro Montesinos. In October 2000, SIN was deactivated by Fujimori himself after the payment of bribes through that organisation became publicly known.

The first reform attempt took the form of Act 27479 (*Ley Nº 27479)* of June 2001. However, according to Ugarte, the system did not function as expected and, in 2006, a new Act (28664) created the *National Intelligence System* (SINA) and the *National Directorate of Intelligence* (DINI), the governing body specialising in national intelligence in non-military spheres and functionally reporting to the President of the Republic (Ugarte, 2012: 257).

Procedures relating to intrusion of privacy actions were a salient aspect of this new Act. Unlike other countries in the region, where any competent magistrate can be asked to issue authorisation, Peru has chosen to limit this power to certain magistrates of its highest Court of Law (Ugarte, 2012: 265).

Regarding oversight, the new Act broadened the scope of the *Intelligence Committee of the Congress of the Republic*'s oversight, allowing it to supervise the activities of all matters falling within SINA's sphere. In addition, the Committee can investigate *proprio motu*, a prerogative that should be understood in conjunction with the requirement to use DINI as an intermediary, which significantly limits the Committee's real investigative capacity[14].

Uruguay

Prior to the restoration of democracy, two intelligence organisations stood out in particular in Uruguay. A military intelligence organisation called the *Armed Forces Intelligence Service* and an organisation heading the police force called the *National Directorate of Information and Intelligence* (DNII), reporting directly to the Ministry of the Interior.

---

13 *Cf.* Revista Semana. *Chuzadas: Así fue la historia*. 8 February 2014. Available at: http://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3.

14 *Cf. Ley del Sistema de Inteligencia Nacional Nº 28.664* (National Intelligence System Act 28664), sections 21.1 and 21.2 of article 21 on "Control por la Comisión de Inteligencia del Congreso de la República y funciones" (Control by the Intelligence Committee of the Congress of the Republic and functions).

In 1986, the National Congress undertook an initial reform to transform the *Armed Forces Intelligence Service* into the *Directorate General of Defence Information* (DGID) reporting to the Ministry of National Defence. In 1999, the Executive turned DGID into the current *National Directorate of State Intelligence* (DINACIE) and made reforms to the organisation's structure and powers. It was assigned responsibility for producing intelligence at the highest national level by coordinating and planning all of the information and counter-information activities carried out by the existing specific organisations.

It should be noted that Uruguay lacks any specific external oversight systems, though the Congress has occasionally intervened on issues relating to intelligence activities (Ugarte, 2012: 544). The Uruguayan parliament recently debated an *Intelligence Framework Bill* that proposes the creation of a National Intelligence System (SIN) that would have parliamentary control through a standing committee of the General Assembly. The Bill also provides for the creation of a parliamentary commissioner figure for SIN, who would be the person responsible for receiving complaints lodged by citizens or intelligence officials[15].

It should be noted that this Bill is being debated while Uruguay is investing in technology to intercept electronic communications; various parliamentarians have questioned whether it should be implemented without first setting up an effective control system[16].

Venezuela

In the Bolivarian Republic of Venezuela, there is widespread intelligence activity in the country's civil life, and there are numerous and distinct organisations that range from high-level directorates (such as the *Directorate General of Military Counterintelligence* and the *Directorate General of Strategic Intelligence*) to intelligence organisations of the armed forces and security forces. Of particular importance is the *Bolivarian Intelligence Service* (SEBIN), which reports to the Ministry of Popular Power for Internal Affairs, Justice and Peace.

Despite the existence of many organisations, Venezuela does not have any oversight mechanisms. Although the National Assembly approved a Bill in 2000 that sought to establish some degree of supervision and coordination, it was vetoed by the then President Hugo Chávez, apparently due to the armed forces' objection to the advance of civilian oversight over intelligence activities (Ugarte, 2003: 17).

Act 6067 (*Ley Nº 6067*) was passed in 2008, creating the *National System of Intelligence and Counterintelligence*, formed by two sub-systems: *Civil Intelligence,*

15 *Cf. Proyecto de ley de la* Comisión de Defensa Nacional; Carpeta Nº 1216 de 2011. Available at: http://www.parlamento.gub.uy/repartidos/AccesoRepartidos.asp?url=/repartidos/camara/d2011100722-00.htm.

16 *Cf.* El País. July 2013. *Piden aprobar ley de Inteligencia antes de activar a "El Guardián".* Available at: http://www.elpais.com.uy/informacion/piden-aprobar-ley-inteligencia-activar-guardian.html, and El País. July 2013. *Gobierno compró "El Guardián" para espiar llamadas y correos.* Available at: http://www.elpais.com.uy/informacion/gobierno-compro-guardian-espiar-llamadas-correos.html.

reporting to the Ministry of Popular Power for Foreign Affairs, and *Military Intelligence,* reporting to the Ministry of Popular Power for Defence[17]. Ugarte considers that while it is right for the sub-systems to report to the technical Ministries linked to the object of their scope of action, it is still necessary to have a central coordination body reporting to the highest state authority, with the ability to coordinate and produce national strategic intelligence (Ugarte, 2012: 466). In this respect, the previous Bill seemed better suited than the version finally enacted.

In any event, that Act passed by the Assembly was repealed in the same year by President Hugo Chávez's Decree 6156 (*Decreto Nº 6156*). According to Ugarte, Venezuela is facing a serious problem as a consequence of not only the opacity of the activities carried out by its main intelligence organisations, but also of their scope (Ugarte, 2012: 467). In Venezuela, there is, in fact, an indistinct blending of intelligence functions and political-activity policing functions, an abuse that is becoming more acute due to the lack of internal and external oversight mechanisms, thus making the Venezuelan intelligence system an especially problematic space from the perspective of democratic control of its intelligence organisations.

VI. Conclusion

This document has sought to provide an introduction to the intelligence activities and various control mechanisms in existence around the world, with a particular emphasis on Latin America.

It is an initial attempt to shed some light on an activity that is usually carried out with excessive secrecy. In this respect, the presentation of basic concepts about intelligence enables a better understanding of the role that organisations like these should play in a democratic society. A review of the current legal frameworks in Latin America shows that the challenge of achieving effective control also exists at a regional level.

Argentina has a complex legal structure that tries to separate *internal security* from *national defence* but, for intelligence-related issues, it has an organisation that manages intelligence processes in a wide-ranging manner for both purposes. The national intelligence system is controlled by a Bicameral Committee in the National Congress, also under a veil of excessive secrecy: it is neither possible to find out if it works effectively nor if it simply works.

By exploring other control mechanisms in existence around the world, we find that it does not tell us much about the particular situation in Argentina or the situation in Latin American: in all countries which recently experienced transition to democracy, exercising effective control over their intelligence organisations is a considerable challenge. And that is due to the collision between two contradictory principles: that of *transparency* on the one hand, which democracy requires as an accountability mechanism in regard to state activities, and that of *secrecy* on the other, which an

17 *Cf. Decreto Nº 6.067 del 14 de mayo de 2008* (Decree 6,067 of 14 May 2008), Gaceta Oficial *Nº* 38.940 del 28 de mayo del 2008 (Official Gazette 38,940 of 28 May 2008).

activity like intelligence demands. Striking the right balance between these two opposing forces is not easy, but a democratic society must try to achieve it. In this respect, intelligence activities should only be secret to the extent *necessary for a democratic society, and proportionate* not only to the purposes warranting them, but also to the rights that they affect. Public officials tasked with supervising these activities must never have their hands tied by such secrecy.

The various oversight mechanisms that we have reviewed in this document offer a comparative view of a complex topic that is important yet often ignored. In this respect, generating information plays a fundamental role in driving forward an agenda for change like the one being carried out by ADC in conjunction with organisations like ILSED and the Fundación Vía Libre in the context of the Citizen's Initiative for Control of the Intelligence System (ICCSI).

References

- [1] Steven C. Boraz. *Executive privilege. Intelligence Oversight in the United States*. In Thomas C. Bruneau and Steven C. Boraz, editors, Reforming Intelligence. Obstacles to Democratic Control and Effectiveness, pages 27–50. University of Texas Press, Austin, 2007.
- [2] Thomas C. Bruneau and Steven C. Boraz. *Intelligence reform: Balancing democracy and effectiveness*. In Thomas C. Bruneau and Steven C. Boraz, editors, Reforming Intelligence. Obstacles to Democratic Control and Effectiveness, pages 1–24. University of Texas Press, Austin, 2007.
- [3] Evaristo de Vergara. *Las diferencias conceptuales entre Seguridad y Defensa*. Instituto de Estudios Estratégicos de Buenos Aires, February 2009.
- [4] Roberto Dromi. Instituciones de Derecho Administrativo. Astrea, Buenos Aires, 1973.
- [5] Erico Duarte. *The politics of Brazilian intelligence and foreign relations with the United States*. Royal United Services Institute Newsbrief, November 2013.
- [6] Diógenes Gasparini. *Direito Administrativo*. Ediciones Saraiva, 4th edition, 1995.
- [7] L. Elaine Halchin and Frederick Keiser. *Congressional oversight of intelligence*. Congressional Research Service, 2012.
- [8] Marcelo Fabián Saín. *Las "nuevas amenazas" y las Fuerzas Armadas en la Argentina de los '90*. In XXIII International Congress Latin American Studies Association (LASA), Washington, DC, United States 6-8 September 2001. Latin American Studies Association (LASA), September 2001.

- [9] Britt Snider. *Congressional Oversight of Intelligence: Some Reflections on the Last 25 Years*. Center for Law, Ethics, and National Security. Duke University School of Law, 2004.
- [10] Russell G. Swenson and Susana C. Lemozy. *Framework for a normative theory of national intelligence*. In Democratization of intelligence. Melding strategic intelligence and national discourse, Washington D.C., 2009.
- [11] José Manuel Ugarte. *Sistema de inteligencia nacional argentino: ¡Cambiar Ya!* In XXII International Congress of the Latin American Studies Association March 16-18, 2000, Miami. Latin American Studies Association (LASA), March 2000.
- [12] José Manuel Ugarte. *El control de la actividad de inteligencia. Realidad actual y tendencias hacia el futuro: Un análisis centrado en América Latina*. In VI Seminario sobre Investigación y Educación en Estudios de Seguridad y Defensa, Santiago de Chile, 27-30 October 2003. Red de Seguridad y Defensa de América Latina (REDES), October 2003.
- [13] José Manuel Ugarte. *Repensando el control de la actividad de inteligencia en Argentina*. Revista AAInteligencia, March 2008. Santiago de Chile.
- [14] José Manuel Ugarte. *El control público de la actividad de inteligencia en América Latina*. Ediciones CICCUS, Buenos Aires, 2012.