1-20-2017

Uruguay Looks to Tame its Cold War-Era Intelligence System

Andrés Gaudán

Follow this and additional works at: https://digitalrepository.unm.edu/notisur

Recommended Citation

This Article is brought to you for free and open access by the Latin America Digital Beat (LADB) at UNM Digital Repository. It has been accepted for inclusion in NotiSur by an authorized administrator of UNM Digital Repository. For more information, please contact amywinter@unm.edu.
Uruguay Looks to Tame its Cold War-Era Intelligence System

by Andrés Gaudín
Category/Department: Uruguay
Published: 2017-01-20

More than three decades after the last civil-military dictatorship (1973-1985) ended, Uruguay is finally taking steps to replace its long-questioned intelligence apparatus with a system that would be under civilian control and the result, from the outset, of a broad political consensus.

Information gathering, special operations, counterintelligence, secret agents, creating false identity documents to protect the identities of those agents, classified and top-secret information, and strong parliamentary oversight are some of the principal contents of a bill introduced Jan. 6 to create a new Sistema Nacional de Inteligencia del Estado (National System of State Intelligence, SNIE). The president’s office expects Congress to approve the legislation in the early part of this year.

Consensus to move forward with the project coalesced quickly after the weekly Brecha denounced the military for continuing—just as it did during the bloody dictatorship years—to spy on political parties, labor and civil society groups, and judges and journalists it deems “enemies” and “subversives.”

The claims, made last year by journalist Samuel Blixen, prompted a visit to Uruguay by Edison Lanza, the special rapporteur for freedom of expression for the Organization of American States (OAS). In an interview with Brecha, the OAS representative expressed concern about “this discovery, which proves the existence of illegal activity and acts of intimidation that constitute a clear violation of personal integrity and privacy, and of freedom of expression as well.”

Lanza noted that there have been similar cases elsewhere in South America, including in Colombia, between 2002 and 2010, when intelligence services interfered with the country’s democratic processes. He also said that for countries like Colombia and Peru, which are democratic but have had authoritarian governments, complaints made to the Office of the Special Rapporteur for Freedom of Expression, a branch of the OAS’s Inter-American Commission on Human Rights, have been a constant.

“It’s time for Uruguay to have a serious discussion about placing these kinds of activities under parliamentary control,” Lanza advised.

Congressional oversight

The bill before Congress looks to regulate the intelligence work carried out by different state agencies. It establishes, in its opening article, that such activities “be done in strict adherence to the principles of a republican democratic governmental regime and with full respect for human rights.” It also touches on issues that the Uruguayan legal code had never addressed. The legislation would empower intelligence staff, for example, “to infiltrate certain areas as hidden agents,” use false documents to protect their real identities, and collaborate with outside informers.

It contains a section on counterintelligence as well, defining it as “an intelligence activity whose goal is to detect, localize and neutralize actions being taken by other nations or by people or
organizations that can affect the interests of the [Uruguayan] state.” With regards to intelligence sources, the bill distinguishes between two types: so-called “open sources” and “closed sources.” The website www.academia.edu, a research clearing house, defines “open sources” as things that offer only “freely available” and “non-classified information” such as radio and television news broadcasts, airline passenger manifests, and the names of public service users, bank clients or credit card holders. “Closed sources” are those with “counterintelligence measures in place to block access or knowledge of.” Such sources are difficult and costly to penetrate, especially at times of conventional war “given the logical increase in counterintelligence work and the fact that they contain classified information,” the website explained.

The legislation strictly establishes that SNIE personnel of all levels “be barred from carrying out repressive activities or taking on for themselves police or criminal investigation functions.” The law would also prohibit agents from “interfering with the country’s political, social or economic activities, foreign policy, or political parties.” Last but not least, the new rules call for strong civilian oversight of the SNIE—just as Lanza’s Office of the Special Rapporteur advises in all of the countries with which it consults. Internally, the intelligence body would have its own chain of command. External control, however, would be handled by Congress via a bicameral and permanent supervisory committee. To guarantee transparency, the committee would include delegates from all of the political parties represented in the legislature.

Eavesdropping software

The concerns Lanza raised in his interview with Brecha had previously been expressed in a press release that the Office of the Special Rapporteur issued on July 21, 2015. At the time, the OAS body said it was puzzled by widespread revelations proving that various Latin American governments had “purchased and implemented surveillance programs that could cause serious harm to the rights to privacy and freedom of thought and expression.” The press release noted that, 400 gigabytes of information had been exposed around that time from an Italian firm called Hacking Team, which sells special spying software, commonly known as “Da Vinci” or “Galileo” programs, to governments and government agencies.

The document went on to say that the surveillance software offered by Hacking Team is designed to bypass computer and mobile phone encryption, allowing users to access messages, telephone calls, e-mails, and chat communication. “This software can also remotely activate microphones and cameras,” the Office of the Special Rapporteur explained. The press release then quoted the Hacking Team website to show that “[e]vidence collection on monitored devices is stealth, and transmission of collected data from the device to the RCS server is encrypted and untraceable.”

Without mentioning names, the Office of the Special Rapporteur suggested that certain countries in the region, based on press reports and claims by civil society organizations, “are or used to be clients of Hacking Team and are using their software [as of July 2015] without the legal authority to do so.” In response to such revelations, some countries denied having anything to do with Hacking Team. “Others stated that they bought the software supported by law for the prevention and investigation of organized crime and terrorism,” the press release explained.

“On this disclosure, and facing possible impacts derived from the usage of this type of privacy-invading technologies and the right to exercise freedom of expression without illegal interferences, the Office of the Special Rapporteur would like to recall that according to international standards,
the use of programs or systems for the surveillance of private communications should be clearly and precisely established by law,” the document went on to say.

**Revamping and renaming**

In recent years, following the end of bloody dictatorships, as in Chile and Argentina, or far-right authoritarian governments, like the ones in Peru under Alberto Fujimori (1990-2000) and Colombia under Álvaro Uribe (2002-2010), various Latin American countries shut down their old intelligence services (NotiSur, April 3, 2015). “They were designed for the Cold War era and based on the model of the Central Intelligence Agency (CIA) in the US,” Brazilian sociologist Emir Sader wrote in an article published Jan. 4 on the website Carta Maior.

Chile’s notorious Dirección de Inteligencia Nacional (National Intelligence Directorate, DINA), for example, in 2004 went on to become the Agencia Nacional de Inteligencia (National Intelligence Agency, ANI) (NotiSur, June 3, 2005). In Argentina, the Secretaría de Inteligencia del Estado (State Intelligence Secretariat, SIDE), in 2015 became the Agencia Federal de Inteligencia (Federal Intelligence Agency, AFI).

In Peru, following a period during which it had been shuttered, the Dirección Nacional de Inteligencia (National Intelligence Directorate, DNI) was cautiously reorganized, and in September, President Pedro Pablo Kuczynski appointed a businessman with no security or intelligence experience to head it. In Colombia, the government closed down the Departamento Administrativo de Seguridad (Administrative Security Department, DAS), replacing it in November 2011 with the Dirección Nacional de Inteligencia (National Intelligence Directorate, DNI).

-- End --