GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

COLOMBIA

Hacking information on the peace talks in Colombia

Colnodo
Ariel Barbosa (with the collaboration of Olga Paz)
www.colnodo.apc.org

Introduction

Colombia is a country with one of the highest internet penetration rates in Latin America. This is due to governmental policies and high investment from the private sector, aimed at opening and consolidating new markets.

One of the most recognised ministries in the current government, based on its initiatives and success, is the Ministry of ICTs. One of its leading initiatives is the Vive Digital Programme, which aims to expand not only ICT infrastructure but also the demand for internet services in the country. One of the outcomes of this strategy is that Colombia has more mobile phones than inhabitants and more than 60% of the population are internet users.

Although there has been great progress in providing internet access, services, applications and content, the country is still behind in defining adequate policies in order to strike the right balance between state surveillance and the right to privacy of citizens. Many recent cases have demonstrated the lack of effective policies and regulations controlling information and data storage, and appropriate penalties in cases where information has been illegally disclosed and obtained from citizens and public servants. Some of these cases are: the *"chuzadas"*[1] (particularly phone hacking) carried out by the former Security Administrative Department (DAS); Operation Andromeda; the hacking of phones and computers of participants in the agrarian strike of 2013; and, most recently, the hacking of phones and computers to sabotage the recent presidential election campaign.

Faced with these events, which caused great concern among the public, the government decided to draft a cyber security and cyber defence policy. The first step taken was to seek the technical assistance of the Organization of American States (OAS), which recommended the inclusion of civil society in defining the policy. However, the complete text of the policy has not been disclosed to the public and there is growing fear that it will only be disclosed when finalised, without the participation of civil society, which would help prevent imbalances between citizen rights and state surveillance.

Policies and regulation on cyber security and cyber defence

In comparison to other countries in the region, Colombia has made great progress in its technological and technical capacity, closing the gap with developed countries. However, regarding institutional coordination and operations there is still much to be done in terms of design and implementation.

One of the first policies outlining the guidelines for cyber security and cyber defence dates from 14 July 2011 (National Council for Economic and Social Policy – CONPES 3701).[2] This policy includes the national and international background, and spells out the regulations in the country regarding these issues. Based on this policy, the Cyber Joint Command, the Cyber Police Centre, the Colombian Information Security Coordination Centre (CSIRT) and the Response Group for Cyber Incidents in Colombia were created. These entities work together with the Army Technical Intelligence Central (Citec) and the Police Intelligence Directorate (Dipol).

Following the first state phone hacking scandal, known as "chuzadas" and carried out by the DAS, the national government closed DAS and passed the Intelligence Bill, which became law on 17 April 2013.

This law was put to the test following a second scandal known as "Andromeda", which revealed the failures in enforcing the law, mainly by members of the army who over several months spied illegally on civil servants and important public figures. In 2014, the government began to draft the cyber defence and cyber security policies, a process in which several civil society organisations (among them Colnodo) asked to be involved – as recommended by the OAS.

[1] "Chuzada" is a term used in Colombia when someone secretly taps a phone line without consent.

[2] www.mintic.gov.co/portal/604/articles-3510_documento.pdf

"Buggly", the "Ethical Hacking Community" centre where the Andromeda operation was carried out. PHOTO: eltiempo.com

Peace talks in Colombia

Since the 1950s at least three generations of Colombians have endured an internal conflict in the country caused by the huge inequality in the distribution of wealth – a conflict whose main actors have been different guerrilla groups and the country's armed forces.

In October 2012, President Juan Manuel Santos confirmed that the government was holding peace talks with FARC, the largest guerrilla group in the country, and the oldest in the world. The news was received both with optimism and scepticism given the failed attempts at peace talks in the past with the same guerrilla group during former president Andrés Pastrana's administration (one of the most infamous incidents during those talks, which took place in January 1999, is known as "the empty chair", referring to the absence of the FARC commander, Manuel Marulanda).[3]

This cycle of internal conflict and failed peace talks allowed intelligence agencies free rein, and some of their activities have not been fully identified.

Andromeda, a front for illegal surveillance of the peace talks

The distrust surrounding the peace talks was confirmed when on 3 February 2014, the weekly magazine *Semana*, which has one of the highest circulations in the country, published an article exposing "a military intelligence front where not all activities were legal"[4] that started operating one month before President Santos initiated the new peace talks. The investigation revealed how the military intelligence set up a front for their operations, and used this as a base to illegally surveil members of the government and public figures involved in the peace talks.

The surveillance base was located in a building in a residential neighbourhood in Bogota. On the second floor, above a restaurant on the ground floor, there was a so-called "Ethical Hacking Community" centre, offering courses on website design and information security and publications on how to spy on a chat site and how to create and detect web attacks, among others.

This centre had been legally opened and was registered in the Bogota Chamber of Commerce on 12 September 2012. *Semana*'s investigation revealed a series of illegal phone and computer hackings carried out by members of the national army, and a military hacking information centre located in a room known as the "Grey Room".[5]

The name of this secret operation was "Andromeda", and an official from the Number One Army Technical Intelligence Battalion (Bitec-1) was in charge of the operation. This battalion is part of Citec, recognised for its success in fighting the FARC by infiltrating their communications – in the past

[3] es.wikipedia.org/wiki/Di%C3%A1logos_de_paz_entre_el_gobierno_Pastrana_y_las_FARC

[4] www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

[5] www.semana.com//nacion/articulo/la-sala-desde-donde-se-hacian-las-chuzadas-del-ejercito/376079-3

this had led to the freeing of kidnapped citizens. However, *Semana* had evidence of how it was also carrying out espionage activities that compromised national security, and was engaged in the illegal phone hacking of recognised public figures. These actions were carried out by members of the army, but also by students, hackers, and participants in so-called Campus Parties (an annual event devoted to technological innovation, digital culture and research). They were not only paid, but handsomely rewarded depending on the political weight of the public figure and the difficulty of gaining access to their information.

After the *Semana* revelations, President Santos consulted internally, and, given the lack of clarity on the issue, asked for a public enquiry to determine "which dark forces are spying on our negotiators in Havana," where the talks are being held. "They are trying to sabotage the peace process. We need to know if (...) there are loose cannons in the intelligence agencies," he declared.

The Andrés Sepúlveda case: Intelligence information gathered in the middle of the presidential election campaign

Campaigning for presidential elections began in 2013, but gained momentum in 2014. The first round of the presidential elections took place on Sunday 25 May. Six candidates from different political parties took part in the presidential race. One of them was President Santos, who was looking for reelection. His most important contender was Oscar Iván Zuluaga, who was the candidate for the Democratic Centre – the political party of former president Alvaro Uribe – and who publicly expressed his disagreement with the peace talks in Havana.

The presidential elections were dogged by yet another espionage scandal. The national newspaper *El Tiempo* revealed that at the beginning of May 2014,[6] a man called Andrés Sepulveda had confessed before a prosecutor and a deputy attorney general to his involvement in hacking information on the peace talks, and how it was about to be sold to the National Intelligence Directorate (DNI).

One of the most disturbing events in those weeks was the broadcasting of a video[7] in which Sepúlveda introduces himself as a contractor for cyber security and social networks and discloses part of the information illegally obtained to Zuluaga.[8] The strategy, from what can be seen in the video, was to publish the information obtained from military sources through the website dialogosavoces.com and a Twitter account (https://twitter.com/dialogosavoces) in order to attack the peace talks and the government.

However, it is difficult to determine if these revelations affected the election process, and the voting. After the scandal was revealed by *El Tiempo*, the first round of presidential elections led to a run-off between Santos and Zuluaga. Santos was re-elected with a 5% advantage over his rival.

Drafting the Cyber Security and Cyber Defence Policy in Colombia

Simultaneously, and partly because of these issues, Colombia has been drafting a Cyber Security and Cyber Defence Policy, which began just when the Andromeda scandal was revealed.[9] For this purpose, a commission was formed, but without the active participation of civil society groups in Colombia. This commission has been limited to governmental officials, national experts in information security and representatives from the private sector with crucial infrastructure, such as the financial and energy sectors.

In March 2014 the non-profit organisations Dejusticia, the Karisma Foundation, the Foundation for Press Freedom (FLIP) and Colnodo sent an open letter to President Santos[10] asking that they be included in the surveillance commission. The aim of the organisations was for human and internet rights, specifically the right to privacy, to be represented in the policy-making process.

The Colombian government requested technical assistance from the OAS, whose report was presented on 4 April 2014. Its main recommendation was to create an entity that would oversee the operations of agencies in the armed forces in charge of cyber security, and which would report directly to the president. The OAS also recommended that this agency should be directed by a civilian and not a military person,[11] and that the government should aim to "harmonise the Colombian legislation with international legislation (Budapest Convention), particularly on issues of criminal procedural law." This would enable the implementation of clear policies to prevent human rights violations and to protect the country's sovereignty.

[6] www.eltiempo.com/politica/justicia/los-archivos-del-hacker-sepulveda-acusado-de-espiar-proceso-de-paz/13972255

[7] www.semana.com/nacion/articulo/el-video-del-hacker-con-oscar-ivan-zuluaga/388438-3

[8] www.eltiempo.com/politica/justicia/los-archivos-del-hacker-sepulveda-acusado-de-espiar-proceso-de-paz/13972255

[9] www.enter.co/chips-bits/seguridad/ciberdefensa-colombia-politica

[10] colnodo.apc.org/destacamos.shtml?apc=l-xx-1-&x=3777

[11] www.elespectador.com/noticias/judicial/colombia-no-se-rajo-el-tema-de-ciberseguridad-y-ciberde-articulo-485831

The OAS has contributed an interesting perspective to the conception of the Cyber Security and Cyber Defence Policy, since it openly declares the importance of incorporating the Budapest Convention in the policy in order to balance national security issues with the defence of human rights.

The Andromeda and Andrés Sepúlveda information hacking cases have yet to come before the court. These cases exposed the flaws in the Intelligence Law (1621 of 17 April 2013) and ultimately the law failed the test. The reason is partly the lack of a centralised body directly responsible to the president, as proposed by the OAS.

Action steps

Civil society organisations should stay actively involved in the design of policies on cyber security and cyber defence in Colombia in order to keep a balance between the defence of the state and privacy rights. It goes without saying that the government should create spaces for civil society participation.

The mission of civil society is to ensure that when laws are created, limits must be defined, as well as to remind the government that its utmost priority is to protect its citizens. The government needs to ensure that laws are "necessary and proportionate" according to the 13 International Principles on the Application of Human Rights to Communications Surveillance[12] – particularly when the crucial peace negotiation process, which has been going on for two years, could be gravely affected.

It is important for these new laws to consider the following points:

- Communications metadata could be more relevant than content.
- To collect information without permission is a crime, even if no one gets to use the information.
- When information about a citizen is requested to solve a court case, it should be because it is necessary, adequate and proportionate.
- It is important to strike a balance between privacy and cyber defence. That is, the right to privacy is equal to the right to build safe communications systems.

[12] https://en.necessaryandproportionate.org/text