INTER PRESS SERVICE
News Agency

Journalism and Communication for Global Change

Active Citizens, Civil Society, Crime & Justice, Democracy, Featured, Global Governance, Headlines, Human Rights, Latin America & the Caribbean, Regional Categories, TerraViva United Nations

Mexico – Both Victim and Victimiser in Cyberespionage

By Emilio Godoy

Map showing the NSA's collection of intelligence from computer networks around the world. The colour scheme ranges from green (least subjected to surveillance) through yellow and orange to red (most surveillance). Credit: Creative Commons

MEXICO CITY, Jun 1 2014 (IPS) - A lack of controls, regulation and transparency marks the monitoring and surveillance of electronic communication in Mexico, one year after the revelations of cyberespionage shook the world.

This Latin American country of 118 million people was one of the targets of the massive illegal cyberespionage practiced by the U.S. National Security Agency (NSA). But no substantial changes have been made in response, to prevent further interception.

"There is no legislation on surveillance and intervention, no good practices for companies," Jesús Robles, with the non-governmental organisation Propuesta Cívica, told IPS. "There is a legal vacuum. They could be gathering metadata."

Metadata is information that describes other information – data generated as people use technology, such as the date and time of a phone call, the location where someone last accessed their email, who sent or received an email, or where someone made a phone call and how long it lasted.

The British newspaper The Guardian reported on Jun. 5, 2013 that the NSA had been collecting the telephone metadata of the customers of Verizon Wireless, the biggest U.S. mobile phone provider, both within and outside the United States.

It was just the first of a series of leaks to the press about the secret operations of the agency, made by Edward Snowden, a former U.S. Central Intelligence Agency (CIA) contractor, now hiding under guard in Russia, which granted him political asylum.

The NSA used the PRISM internet surveillance programme to spy on a number of countries, including Mexico, in areas like anti-drug efforts, energy and security.

And with BLARNEY, the international version of the PRISM programme, the United States intercepted the communications of several embassies in Washington, including Mexico's. Using another tool, Boundless Informant, it illegally intercepted phone calls and email that passed through U.S. telecoms networks.

On Sep. 1, 2013, U.S. journalist Glenn Greenwald revealed that in 2012 the NSA had spied on the email of Brazilian President Dilma Rousseff and Mexican President Enrique Peña Nieto, in the latter case during his presidential campaign.

The United States has ignored Mexico's protests, including a diplomatic note demanding an investigation and a condemnation by Congress.

Greenwald's online U.S. publication The Intercept reported on May 19 that a surveillance programme, Mystic, collects metadata on the nearly 100 million cell phones operating in Mexico.

"Not much has been done," Cédric Laurant, one of the four founders of the Mexican non-governmental group Son Tus Datos (It's Your Information), dedicated since 2012 to advocating the protection of privacy in communications, told IPS. "If the public knew more, they could pressure local and foreign businesses to exert more pressure on the government."

Mexico also acquired computer programmes to record voices and track phone calls, emails, chat conversations, visited website addresses and social networks.

Since 2010, Mexico's Federal Law for the Protection of Personal Information Data guarantees the right to privacy and establishes that, if an institution wants to transfer information to third parties at home or abroad, it must give the owners of the information notice and explain the purpose for which it was authorised.

But the law's guarantees were undermined when a Law on Geolocalisation entered into force in 2012. This legislation allows the government to gather, without notification and in real time, geographic data from cell-phone users.

Furthermore, the new national penal procedures code in effect since March allows the authorities to access real-time geo-location data without a court order.

In March 2013, the interdisciplinary Citizen Lab at the University of Toronto in Canada
reported that FinFisher surveillance software command and control servers, made by the U.K.-based company Gamma Group, were hosted on two Mexican Internet service providers: Iusacell, a small provider; and UniNet, one of the largest in Mexico, a subsidiary of Teléfonos Mexicanos (Telmex).

After this was discovered, Propuesta Cívica and the digital rights collective ContingenteMX asked the Federal Institute for Access to Information and Data Protection (IFAI) to investigate the Obses company for the use of the programme.

In March IFAI approved sanctions against Obses for selling FinFisher to the government at more than double the market rate. Obses is a Mexican firm that has received dozens of no-bid governmental projects.

On May 12 a British court ruled that UK Revenue & Customs acted unlawfully in refusing to disclose information on the status of an investigation into the export of British Gamma International's FinFisher surveillance technology, paving the way for a review of the programme's sales abroad.

In February, Citizen Lab produced two reports on the use of spy programmes. In one of them, "Mapping Hacking Team's 'Untraceable' Spyware", it reported that agencies in 21 countries used or use the Remote Control System (RCS), sophisticated computer spyware marketed and sold exclusively to governments by the Milan-based Hacking Team, including Mexico, Colombia and Panama.

The RCS can copy files from a computer's hard disk, record Skype calls, emails, instant messages, and passwords, and turn on a device's webcam and microphone to spy on a target.

Citizen Lab reported that it mapped out "covert networks of 'proxy servers' used to launder data that RCS exfiltrates from infected computers, through third countries, to an 'endpoint,' which we believe represents the spyware's government operator. This process is designed to obscure the identity of the government conducting the spying.

"For example, data destined for an endpoint in Mexico appears to be routed through four different proxies, each in a different country."

And in another article, "Hacking Team's U.S. Nexus", Citizen Lab said that in at least 12 cases, U.S.-based data centres are part of a "dedicated foreign espionage infrastructure."

Citizen Lab states that in tracing these "proxy chains," it found that U.S.-based servers appeared to assist the governments of 10 countries, including Mexico and Colombia, in espionage and/or law enforcement operations.

Citizen Lab found 14 IP addresses, 12 of which are apparently still active.

Mexico's legislation does not require telecommunications companies to reveal government requests about the activities of Internet users.

"The action taken has not proven to be effective; rights are violated," Robles said.

"Awareness-raising is needed among users so that a larger number of them exercise mass pressure on companies, in order for users to take privacy into their own hands, using new tools that are available," Laurant said.