WHEN THE STATE "HACKS"[1]*

ANALYSIS OF THE LEGITIMACY OF THE USE OF HACKING TOOLS IN COLOMBIA

KARISMA FOUNDATION
By Juan Diego Castañeda

Elaborate by:
Karisma Foundation
karisma.org.co

With the support of Privacy International

PRIVACY INTERNATIONAL

Fundación Karisma
www.karisma.org.co

December 10th 2015

Karisma Foundation, in a continuing effort to make its documents more accessible —that it, in a format that allow the content to be read by as many people as possible, regardless of their disability or context of use— linked the bibliographical sources in the content itself. However, the bibliographical sources utilized can be found in the References section.

Check this analysis on-line at

https://karisma.org.co/cuando-el-estado-hackea-3/

Index

When the State "hacks"[1]

Analysis of the legitimacy of the use of hacking tools in Colombia

Karisma Foundation
By Juan Diego Castañeda

An Argentinean prosecutor receives a PDF file in his inbox called "secret and strictly confidential.pdf" and luckily tries to open it on his Android phone. Had he opened it on his computer "the file would have shown nothing but a single blank page. While [the prosecutor] pondered this, spying software would have been installed on his machine."[2]. A Colombian journalist is investigating a case of police corruption when "suddenly the telephone rings and he sees the mouse arrow start to move by itself, as if possessed or remotely controlled, and delete the document"[3] he was working on. These cases demonstrate that communications can not only be censored or intercepted, they can also be subject to computer attacks, since the devices we use every day are vulnerable, and they store personal information that can be of interest to attackers.

The internet is affected by all types of control measures that determine to what extent it is a free, open, and safe medium. Ron Deibert classifies controls in the following way[4]: The first generation of controls consists in defensive content-blocking and filtering systems. The second generation stems from the collaboration between governments and the private sector, imposing or requesting access to "back doors" to hardware or software, establishing greater requirements for internet

access, such as registering with biometric data, or by banning the use of security and encryption tools.

Third generation controls are offensive in nature and they include the use of directed attacks by governments, by means of their own capabilities or by the use of private sector technology, such as that offered by Hacking Team. States, then, have been acquiring technological capacities to surreptitiously access electronic devices and gather information from them, or even turn on their webcams or microphones and record what they pick-up[5], that is, to hack them to achieve objectives in criminal investigations, but also the suppression of dissidence and intelligence gathering[6].

The use of these tools by governments and private parties creates problems for the exercise of human rights, since it entails total intrusion into the target individual's private life, and can thus affect, among others, the right to freedom of speech. Even though these tools are present not only in Colombia but also in several Latin American countries, there hasn't yet been a debate about their legitimacy, nor about the challenges that these activities pose for the human rights legal frameworks in our countries.

On the other hand, it has been asserted that the use of these tools by law enforcement is a necessity in the fight against crime and terrorism, since it levels the playing field between criminals and the authorities[7]. Others maintain that the use of hacking tools can be legitimate as long as there is a judicial order to make use of vulnerabilities in computer systems. The legalization and application of judicial controls to this activity could result in the setting of limits, and would thus minimize its negative effects. This alternative would prevent the creation of new vulnerabilities, since it only exploits existing ones, and it would ease the pressure on manufacturers and service providers to collaborate with governments[8]. However, these are discussions that deserve our attention, and that haven't yet occurred in our country.

Hacking Team in Latin America

In Latin America, only in 2015 did the citizenry find out that hacking tools were part of the region's surveillance authorities' portfolio.

In March 2013, a CitizenLab report documented for the first time the use of Finfisher in Mexico[9]. Soon after, in April of that same year, a new report by this organization showed it's expansion into Panama[10]. In the last report from October 2015, CitizenLab shows how Finfisher is also being used by Venezuela and Paraguay.[11]. On the other hand, since February 2014, thanks to another CitizenLab investigation, the use of malware sold by Hacking Team has been discovered in at least three countries in

the region: Mexico, Panama and Colombia[12]. 2015 revelations about leaks about the Italian company Hacking Team confirmed this investigation, and even established that the extent of the use of this tool in the region was much greater than what was initially reported[13]. It was also established that Ecuador, Chile, and Honduras had at some point acquired or used this software[14], that Brazil had obtained the necessary authorizations to use it and that it planned to use it as a surveillance mechanism for the upcoming Olympics[15], that the tool was being demonstrated in Peru,[16] and that contacts were being made in Argentina[17].

Governments in the region have reacted in various ways to these revelations. Ecuador's National Intelligence Secretary denied it's relationship with Hacking Team[18]. Nonetheless, there is evidence that suggests the use of this software in Ecuador against opposition figures and groups[19]. In Chile, the Investigations Police admitted having acquired Hacking Team software and justified its purchase as part of its modernization projects "aimed at improving the operational capacity for investigating organized crime, international terrorism, and large scale drug trafficking"[20].

Finally, in Mexico, the leaks made it clear that 14 authorities, both federal and state, were clients of the Italian firm, and the legality of these activities was later put into question[21]. According to the leaked documents, Mexico made the biggest payment ever made by a public or private company in the history of the Harking Team when it purchased 600 licenses to conduct simultaneous monitoring[22].

Hacking tools in Colombia

The email leak from the Italian firm Hacking Team confirmed that its remote control system had been solid in Colombia and that it was probably being used. The buyer turned out to be the National Police Directorate (DIPON). In a press release, the Police did not deny the use of Hacking Team products, but denied having any relation with this company. It also affirmed having had no commercial contact with Hacking Team, although it admitted having "acquired a technology tool with the company Robotec Colombia S.A.S, which offers security equipment. The purpose of this purchase -it said- was bolstering the threat detection capabilities against terrorism and organized crime in the Colombian cyberspace[23]."

What the police acquired was a remote control system called "Galileo", which installs itself in the target device through files specially designed to be opened by the target user, allowing the attacker to take control of the device, take information, access the microphone or webcam, and even record what is typed on the keyboard[24].

In an initial case with suspected use of hacking tools, the Colombian Prosecutor General announced on December 3 that an investigation would commence derived from the report presented by journalist Vicky Davila for alleged interception of her private communications, as well as those of her family and members of her team. The motive behind these attacks against journalists appears to be the fact that they possessed information previously leaked about the Police that points to serious cases of corruption, as well as a supposed prostitution network that benefited senior members of this institution[25].

Although apparently there was also illegal physical surveillance[26], journalist Juan Pablo Barrientos, who investigated the police scandal, was the person who experienced the story presented in the first paragraph. Suddenly, some files he was working on in his computer were deleted, not by accident, but as if someone had taken control of the device.

Hacking Problems

Taking control over someone else's device, regardless of the technical means employed, is equivalent to interception of communications in Colombia and, therefore, requires the existence of a law so authorizing it and that there be judicial control of said activity [27]. Many of the tools the authorities have at hand today are in some way limited in scope. The interception of calls or emails only extracts information coursing through those means and that the person concerned has decided to share with others. However, access to a computer system, whether a personal computer or a mobile phone, may involve the collection of all kinds of personal information such as photos, work or personal documents, browsing history, access to microphones and webcams, and even control the device itself; all the foregoing without the person being aware of the intrusion or being able to establish a time limit to its execution. Hacking clearly delivers far more information than would be obtained, for example, in a raid of the home of the person concerned, though, in contrast, there are many more controls for the latter measure than for the former.

Intrusion on the devices of persons is a violation of their privacy, but also affects their right to freedom of expression and opinion. As stated by the Special Rapporteur of the United Nations (UN) on the Promotion and Protection of the Right to Freedom of Opinion and Expression, in the digital age, the exercise of these rights is not limited to one's own volition, it is also exercised in the use of search engines or in the storage of files located on devices or on the cloud [28].

The debate over the legality of hacking in Colombia, on the possible scope of a law that allows it and the obligation to add controls to its execution to prevent abuse, such

as, for example, setting prior judicial control, are not the only elements nor do they constitute the highest standards that currently exist if one is to consider that a restriction on fundamental rights such as hacking is legitimate. For the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, the legitimacy of surveillance measures on communications derives from the observance of certain conditions decanted from the various documents of the Inter-American Human Rights System[29]. These requirements are:

1. Legally enshrined
2. Seeks an imperative goal
3. Need, appropriateness and proportionality of the measure to attain the objective pursued
4. Due process and judicial restraint

The Rapporteur for Freedom of Expression of the OAS, in regard to the revelations about the use of the products and services of the Italian firm Hacking Team on the part of governments around the world, noted that:

> in accordance with international standards, the use of programs or surveillance systems in private communications must be set clearly and precisely in law, be truly exceptional and selective, and be limited to that which is strictly necessary for the performance of imperative ends such as investigating serious crimes as defined in legislation [30] .

Finally, the International Principles on the Application of Human Rights to the Surveillance of Communications must be taken into account, which were developed from the conceptualizations that have been made about international human rights law in the digital milieu[31] in a process that was led by various organizations of civil society and that included the participation of industry representatives and subject-matter experts. The principles that should govern the application of communications surveillance measures are: legality, legitimate purpose, need, appropriateness, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, guarantees for international cooperation and safeguards against unlawful access and the right to an effective remedy.

No country in Latin America has a legal framework on its books for the performance of the activity of intrusion or 'hacking' of devices. Therefore, the first requirement of legality as a guarantee of the legitimacy of a measure restricting rights is not satisfied. The existence of a law in the formal and material sense presupposes a public debate on the need, proportionality and adequacy of the measure, from which it follows that these requirements are not met either.

The current illegality of the use of hacking tools is more noticeable if one considers that there are laws that criminalize this. In Colombia, abusive access to a computer system, computer data interception and the use of malicious software, among others, are crimes[32]. In Peru, illicit access to computer systems and interception of private communications are penalized[33]. In México, the interception of private communications is a crime[34] and in Brazil, the invasion of computing devices is punished[35]. Despite the apparent illegality of the activities alleged through the scandals of Hacking Team, at least in Colombia, there are no investigations against individuals or entities responsible.

Conclusions

If a rule were to be proposed to legalize the use of hacking tools by the authorities, said rule would need to be clear about the types of tools that can be used and the purposes of the equipment that could be affected, for example, access to files stored within the device, to recording what is typed or what is captured by the microphone or webcam. Likewise, it needs to be clear about how long such a tool can be employed, which authorities and under what conditions can it be done (e.g. investigations of certain crimes).

The extent to which the measure is limited in terms of the media on which it would operate (networks, personal computers, mobile phones, security cameras, internet traffic, etc.) also needs to be analyzed, in regard to the data it would access, and the maximum time it could be implemented, not forgetting that the grounds for employing such a power should also be limited to certain specific cases.

The lack of precision in any of these issues can be a blank check for the authority that might deploy the measure, from where the requirement of a legitimate goal might fail, as well as the requirement of need and proportionality because it would be permissible to restrict a person's rights for vague and unsubstantiated reasons.

It is clear that the hacking would require a court order, therefore, an application procedure should be established wherein the satisfaction of the requirements that would be mandated in law for use of the measure could be verified. This procedure should be designed to prevent abuse, and it should also contain provisions regarding the chain of custody, the notification to the person concerned so that they can exercise the right of defense, and the submission of transparency reports by the authorities on the frequency of use and effectiveness of the measure.

Finally, one needs to consider that the extent to which hacking is a legitimate form of communications surveillance may contain a contradiction vis-à-vis other duties

of the State. On the one hand, these types of measures are based on the existence of computer vulnerabilities, i.e., security flaws. On the other hand, States currently carry out cyber-security policies, following their duty to ensure the safety of citizens. If the State does not report the vulnerabilities it finds, it maintains unsecure conditions in breach of its obligations. If it reports these, however, it reduces the opportunities for using them, wasting the time and resources it used to exploit them. Overcoming this contradiction is an issue that must necessarily be part of the public debate on the legalization of hacking.

Check this analysis on-line at

https://karisma.org.co/cuando-el-estado-hackea-3/

Notes

1 Hacking" is an expression that identifies an ethic of providing access to technology to empower people, and was later understood as the activity of finding vulnerabilities in information systems, essentially with the goal of reporting them and repairing them. Finally, it began to be used in the sense of seeking vulnerabilities in information systems in order to exploit them illegally. For Karisma, the correct expression when one "hacks" to cause harm is to "crack", so using the expression "hacking" in this sense is incorrect. However this is the popularized use. For ease of understanding, we have decided to use the term "hacking" to mean "cracking" in this document, although we are aware that this is only one of the meanings of this word.

2 Marquis-Boire M. "Inside the spyware campaign against argentine troublemakers". The Intercept, 21 of August, 2015. Retrieved from https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/

3 Vélez, L. "El precio de denunciar". El Espectador, 6 of December, 2015. Retrieved from http://www.elespectador.com/opinion/el-precio-de-denunciar

4 Deibert, R. (2015). Cyberspace under siege. J*ournal of Democracy*, 26(3).

5 LaRue, F. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/23/40,p. 37.

6 *See*, for example, McCullagh, D. (2007). *Feds use keylogger to thwart PGP, Hushmail. CNET*. Retrieved from http://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/; Nagaraja, S., & Anderson, R. (2009). T*he snooping dragon: social-malware surveillance of the Tibetan movement. University of Cambridge Computer Laboratory;* Glance, D. (2011, October 11). Ein spy: is the German government using a trojan to watch its citizens? *The Conversation*. Retrieved from https://theconversation.com/ein-spy-is-the-german-government-using-a-trojan-to-watch-its-citizens-3765-.

7 Vincenzetti, D. (2015, July 29). Terrorists and criminals have a lot less to worry about since we were hacked. *International Business Times*. Retrieved from: http://www.ibtimes.co.uk/hacking-team-ceo-terrorists-criminals-have-lot-less-worry-about-since-we-were-hacked-1513148. Vicenzetti is the CEO of the Italian company Hacking Team.

8 Bellovin S.M., et al. (2014). Lawful hacking: using existing vulnerabilities for wiretapping on the internet. *Northwestern Journal of Technology and Intellectual Property*. 12, p. 1. Retrieved from http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1.

9 Marquis-Boire, M. et al. (2013). *For their eyes only: the commercialization of digital spying*. Toronto: Canada: Citizen Lab. Retrieved from https://citizenlab.org/2013/04/for-their-eyes-only-2/.

10 Marquis-Boire, M. et al. . (2013). *You only click twice: FinFisher's global proliferation*. Toronto, Canadá: University of Toronto. Retrieved from https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

11 Marczak, B. et al. (2015, October 15). *Pay no attention to the server behind the proxy: mapping FinFisher's continuing proliferation*. Toronto, Canadá: CitizenLab. Retrieved from https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/.

12 Marczak, B. et al. (2014). Mapping Hacking Team's "untraceable" spyware. Toronto, Canadá: Citizen Lab, p. 17. Retrieved from https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

13 When hackers are hacked (2015, July 11). *Revista Semana*. Retrieved from http://www.semana.com/nacion/articulo/los-lios-de-hacking-team-por-informacion-hackeada/434391-3

14 Karisma Foundation (2015, July 7). *Civil society in Latin America rejects Hacking Team's spy software*. Retrieved from https://karisma.org.co/sociedad-civil-de-america-latina-rechaza-software-espia-de-hacking-team/.

15 Viana, N. (2015, July 27). Hackeando o Brasil. *Agencia Pública*. Retrieved from http://apublica.org/2015/07/hackeando-o-brasil/.

16 State agencies linked to Hacking Team (2015, July 12). *RPP noticias*. Retrieved from http://rpp.pe/politica/actualidad/vinculan-a-entidades-del-estado-con-empresa-de-espionaje-hacking-team-noticia-816283.

17 Dubove, A (2015, July 13). Hacking Team made contacts in Argentina to sell spy software. *Panam Post*. Retrieved from http://es.panampost.com/adam-dubove/2015/07/13/hacking-team-hizo-contactos-en-argentina-para-vender-software-espia/.

18 The National Intelligence Secretary denies any contract with companies offering spy services (2015, July 10). *El Universo*. Retrieved from http://www.eluniverso.com/noticias/2015/07/10/nota/5011474/secretaria-inteligencia-niega-contratos-empresa-que-ofrece.

19 APNewsBreak: leaked Hacking Team emails suggest Ecuador illegally spied on opposition (2015, August 6). *US New*. Retrieved from http://www.usnews.com/news/business/articles/2015/08/06/apnewsbreak-email-leak-suggests-ecuador-spied-on-opposition.

20 PDI confirms purchase of software created by hacked Italian company (2015, July 6). *El Mercurio*. Retrieved from http://www.emol.com/noticias/Tecnologia/2015/07/06/724738/PDI-confirma-compra-de-software-creado-por-empresa-italiana-que-fue-hackeada.html.

21 Sánchez, J. (2015, 6 de julio). Hacking Team Hack Confirms Spy Abuse in Mexico. *El Economista*. Retrieved from http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico.

22 Ángel, A. (2015, July 21). In 2015, Sedena negotiated the purchase from Hacking Team of licenses to spy on 600 people. *Animal Político*. Retrieved from http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas/.

23 National Police denies links with the firm Hacking Team (2015, July 8). *W Radio.* Retrieved from http://www.wradio.com.co/noticias/actualidad/policia-nacional-niega-vinculo-con-la-firma-hacking-team/20150708/nota/2841301.aspx.

24 Botero, C. & Sáenz, P. (2015, August 24)."In Colombia, PUMA is not what it appears to be." Digital Rights Latin America & the Caribbean. Available at: http://www.digitalrightslac.net/es/en-colombia-el-puma-no-es-como-lo-pintan/.

25 Coronell, D. (2015, December 8). "Los caballeros de la noche". Revista Semana. Retrieved from: http://www.semana.com//opinion/articulo/daniel-coronell-el-caso-del-general-palomino-la-banda-de-prostitucion-en-la-policia/452337-3

26 "El informante de las 'Chuzadas'" (2015, December 7). *El Espectador*. Taken from: http://www.elespectador.com/noticias/investigacion/el-informante-de-chuzadas-articulo-604187

27 Constitution of Colombia. Article 15.

28 Kaye, D (2015). Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32, para. 20. Retrieved from: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

29 CIDH (2013). Freedom of expression and the Internet. OEA/Ser.L/V/II.149 doc.50, Chapter IV, para. 55.

30 Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the OAS (2015, July 21). Press release on the acquisition and implementation of monitoring programs by states in the hemisphere. Retrieved from Http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2.

31 International Principles on the Application of Human Rights to the Surveillance of Communications. Retrieved from Https://es.necessaryandproportionate.org/text.

32 Penal Code. Items 269A, 269C and 269E respectively.

33 Law No. 300096 (2013). Articles 2 and 7, respectively.

34 Federal Criminal Code Article 177.

35 Criminal Code Section 154A.