lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

SUPPORT NETWORKS FOR JOURNALISTS AND HUMAN RIGHTS ACTIVISTS: A NEW COMPONENT OF SURVEILLANCE REGIMES IN MEXICO

Redes de apoyo para periodistas y personas defensoras de derechos humanos: un nuevo componente de los regímenes de vigilancia en México

Redes de apoio a jornalistas e defensores dos direitos humanos: um novo componente dos regimes de vigilância no México

Erik da Silva[a]

[(a)] Student in final year of Dual BA in European Social and Political Studies (Sciences Po and University College London), writing as associate of Political Observatory of Latin America and the Caribbean (OPALC). E-mail: erik.dasilva@sciencespo.fr.

Abstract

Journalists and human rights defenders face important physical and psychological risks in Mexico, especially since the beginning of the 'war on drugs' in 2006. The expansion of the use of Internet in Mexico has led to the existence of digital vulnerabilities which are exploited by the state surveillance regime. This article explores the perception of digital threats and studies a case of state-owned spyware Pegasus used to hack the investigative media Aristegui Noticias. In light of those new threats, support networks had to enlarge the scope of their mission. In combining the surveillance regime with transnational advocacy theory, this article sees how traditional and new human rights organisations engage in surveillance mechanisms to monitor and seek accountability for activities of the state surveillance regime against journalists and human rights defenders. In that sense, support networks are a new component of the surveillance regime of civil society in competition against the state surveillance regime.

Keywords: Support networks; Surveillance regime; Civil society; Digital threats; Advocacy.

Resumen

Los periodistas y defensores de los derechos humanos se enfrentan a importantes riesgos físicos y

psicológicos en México, especialmente desde el comienzo de la "guerra contra las drogas" en 2006. La expansión del uso de Internet en México ha llevado a la emergencia de vulnerabilidades digitales que son explotadas por el régimen estatal de vigilancia. Este artículo explora la percepción de las amenazas digitales y estudia el caso del spyware estatal Pegasus usado para hackear a los medios de investigación Aristegui Noticias. A la luz de estas nuevas amenazas, las redes de apoyo han debido ampliar el alcance de su misión. Al combinar la teoría de los regímenes de vigilancia con la de las redes transnacionales de apoyo ('advocacy' en inglés), este artículo analiza cómo las tradicionales y nuevas organizaciones de derechos humanos se involucran en mecanismos de vigilancia para monitorear y buscar la responsabilidad de las actividades del régimen estatal de vigilancia contra periodistas y defensores de los derechos humanos. En ese sentido, las redes de apoyo son un nuevo componente del régimen social de vigilancia en competencia con el régimen estatal de vigilancia.
Palabras clave: *Redes de apoyo; Régimen de vigilancia; Sociedad civil; Amenazas digitales; Apoyo.*

Resumo

Os jornalistas e os defensores dos direitos humanos enfrentam importantes riscos físicos e psicológicos no México, especialmente desde o início da "guerra contra as drogas" em 2006. A expansão do uso da Internet no México levou à creacoa de vulnerabilidades digitais que são exploradas pela regime de vigilância estatal. Este artigo explora a percepção das ameaças digitais e estuda o caso do spyware Pegasus, propiedade do Estado mexicano, para hackear a mídia investigativa Aristegui Noticias. À luz dessas novas ameaças, as redes de apoio têm tido que ampliar o escopo da sua missão. Ao combinar o regime de vigilância com a teoria do apoio transnacional ('advocacy' em Ingles), este artigo tenta entender como as novas e tradicionanis organizações de direitos humanos envolvem-se em mecanismos de vigilância para monitorar e buscar a responsabilidade por atividades do regime de vigilância do estado contra jornalistas e defensores de direitos humanos. Nesse sentido, as redes de apoio são um novo componente do regime de vigilância da sociedade civil em concorrência com o regime de vigilância do estado.
Palavras-chave: *Redes de apoio; Regime de vigilância; Sociedade civil; Ameaças digitais; Advocacia.*

INTRODUCTION

Since the beginning of the 'war on drugs' in 2006, journalists and human rights defenders face important threats in Mexico. Indeed, more than 125 journalists were murdered and 21 have disappeared since the year 2000. Between December 2012 and July 2017, more than 106 human rights defenders were assassinated and 81 have gone missing (Suárez & Zapico, 2017). Furthermore, a Canadian university laboratory found that the Mexican government used the spying software 'Pegasus', designed for use against terrorist groups, to hack journalists, human rights defenders and support networks around them (Article 19, Red en Defensa de los Derechos Digitales & SocialTIC, 2017). In this context of insecurity, Nelson Arteaga Botello (2015) showed that three surveillance regimes are currently in competition: the surveillance regime of the State, organized crime, and civil society. Using the concept of social sorting developed by Lyon and Bauman, Botello showed that they

practiced social sorting by collecting data to identify and classify specific groups of people in order to manage territories, control its population and define citizenry.

Surveillance by the State, as well as violence and impunity carried out by both the State and organized crime create a permanent threat for journalists and human rights defenders. Human rights non-governmental organizations (NGOs) have been present in Mexico since the 1980s, but the novel challenge of targeted digital surveillance means that traditional Human Rights NGOs and new NGOs need to include those specific digital threats in the scope of their action. They compose support networks to protect journalists and human rights defenders against the exploitation of their digital vulnerabilities. Furthermore, support networks receive help to do so from Transnational Advocacy Networks (TAN) (Keck & Sikkink, 1998). Indeed, domestic NGOs, international NGOs (INGOs), foundations, parts of governments and intergovernmental organizations among others are interconnected in their work to protect journalists and human rights defenders in Mexico. Support networks can be viewed as the latest component of the surveillance regime of civil society (also referred to as social surveillance regime) which aims to provide 'bubbles of protection' in the context of surveillance and insecurity in Mexico (Botello, 2015, p. 81), because they collect data to monitor the exploitation by the state surveillance regime of digital vulnerabilities of journalists and human rights defenders.

The intention of this article is to give a first account for the emergence of support networks to specifically protect journalists and human rights defenders targeted by the state surveillance regime in Mexico. Botello (2015, pp. 86-87) shows that researching surveillance and insecurity can be challenging because of the unavailability of reliable data and mistrust towards researchers. This study relies mainly on reports produced by support networks. The article proceeds as follows: First, it studies the digital threats and its perception against journalists and human rights defenders by the state surveillance regime. First, it examines what kinds of digital threats posed by the state surveillance regime journalists and human rights defenders face and how they perceive them. Then, it analyses the emergence of protection and accountability mechanisms of support networks which are embedded in the surveillance regime context.

DIGITAL THREATS AND PERCEPTIONS FACED BY JOURNALISTS AND HUMAN RIGHTS DEFENDERS IN MEXICO

Journalists and human rights defenders face important threats in Mexico. They receive death threats and risk being kidnapped, tortured and killed. Increasingly, digital vulnerabilities are being exploited by hostile organizations. This is critical. For instance, the hacking of a phone enables one to know the location of the journalist and putting them and their sources in danger. Traditional human rights NGOs start to integrate the necessity for digital training while other NGOs specifically concentrate on protecting digital vulnerabilities of journalists and human rights defenders as their mandate.

THE PERCEPTION OF DIGITAL THREATS

There seems to be few systematic academic accounts for what kind of digital threats journalists face and what the perception of those risks are, in Mexico at least. Jorge Luis Sierra (2013), as ICFJ Knight International Journalism Fellow, published 'Digital and Mobile Security for Mexican Journalists and Bloggers'. He wrote an interesting review of the threats journalists and bloggers face in Mexico based on an online survey of over 100 journalists and bloggers in 2012. While he recognizes that the outcome may not necessarily be representative of risks all journalists face in Mexico, it is nevertheless an interesting account of current perceptions of digital risks.

Regarding physical risks, the survey found that 70% of respondents had either received threats or suffered attacks during their career. Personal security was the main concern for about a third of respondents and around 20 % were more concerned for their family's security. Meanwhile, 10% put information security first and 5% prioritized the safety of sources. On the other hand, regarding digital threats, 35% perceived the hacking of personal accounts and 33% considered cyberspying to be a major digital threat. Meanwhile, 9% feared most that their website got hacked and 7% were most afraid of getting their equipment stolen. The report then outlined different digital safety practices and awareness such as encryption and strong passwords. It concluded with a series of recommendations for strengthening digital security by increasing resources in media organizations for digital safety, connecting with digital security trainers and building awareness (Sierra, pp. 7- 9, 14 f.).

The survey displays the awareness of the respondents about the nature of digital and physical threats. Both threats are well identified separately: physical threats are composed mainly by fear for personal and family's security and digital threats by cyberspying and personal account hacking. However, no explicit link was drawn between both risks, which is perhaps due to the design of the study itself. While causality remains to be demonstrated, it is certainly interesting to study the link between digital and physical threats, for instance research in how many cases hacked electronic devices enabled spying of ongoing investigations and the assassination of sources because it provided their names and locations to hostile organizations. Of course it is inherently difficult to obtain such data.

SURVEILLANCE REGIME OF THE STATE: THE CASE OF ARISTEGUI NOTICIAS

The case of Aristegui Noticias as shown by 'Gobierno Espia' (*Spy Government*) a report by Article 19, Red en Defensa de los Derechos Digitales and Social TIC (2017) provides a good example of the actions of the surveillance regime of the State against journalists and human rights defenders. Indeed, spyware only sold to States for the specific purposes of using against terrorist and criminal groups was used to hack electronic devices of journalists investigating cases of crime and corruption committed by public officials.

In November 2014, the online media published an investigation called 'la casa blanca de Peña Nieto' on a possible conflict of interest concerning the ex-governor of the State of Mexico, and since then President of the Federal State, regarding the construction of a private mansion worth 7 million USD and public contracts. Aristegui Noticias also played a key role in covering the massacre of 43 students educators of Ayotzinapa in 2013. Beginning 2014, the office of the media had already suffered an intrusion. From January 2015 till July 2016, reporters of the investigation of 'la casa blanca de Peña Nieto' as well as the son of head of the organization, Carmen Aristegui, had received text messages with a malicious link, which if clicked upon, would install Pegasus spyware on the electronic device. Such malware technology comes from NSO group, an Israeli firm which sells its services and products to States only for purposes already mentioned above. The report underlines a possible correlation between the investigations led by Aristegui, especially the 'casa blanca de Peña Nieto' case, and the hacking attempts. Indeed, the recurring occasions in which journalists received a text with a malicious link, sometimes referring to bank account issues in 2015 or with more refined

technique such as inviting the target to a funeral of a parent such as in 2016, correlate with the publication of investigations on corruption and crimes committed by public officials.

A striking example are the attempts targeted against the son of the head of Aristegui Noticias; Emilio Aristegui has been victim of over 40 phishing attempts, with the examples of two texts falsely informing on behalf of the media UNO TV in August 2015. The first one stated that the Presidency could ask for the names of the investigators behind the 'casa blanca de Peña Nieto' investigation and the second one related that the latter could be imprisoned for defamation. The same texts were sent to a journalist of the media (Article 19, 2017, pp. 18, 22-24).

Moreover, a potential connection between physical and digital threats can be seen in several examples. For instance, Aristegui Noticias published in August 2016 an investigation over plagiarism by President Peña Nieto in his undergraduate law thesis. The report related that two investigative journalists of Aristegui then received direct threats on Twitter with pictures of armed men as well as a picture of their name written on a sheet surrounded by bullet cartridges. In November 2016, five individuals forcefully entered the office of the media and specifically stole a computer of the journal's investigation department, with information about current investigation linking the army modifying a crime scene in Tlatlaya in 2014 (pp. 31,32).

EMERGENCE OF A TRANSNATIONAL ADVOCACY NETWORK TO PROTECT JOURNALISTS AGAINST DIGITAL THREATS

In the surveillance context of Mexico, support networks had to adapt and develop mechanisms to protect journalists and human rights defenders against the novel digital threats. The strategies used to do so are intertwined with surveillance practices by collecting information and using it effectively.

SUPPORT NETWORKS AS PART OF TRANSNATIONAL ADVOCACY NETWORKS

Support networks seeking to protect journalists and human rights defenders from digital threats by the state surveillance regime can be placed in the framework of TAN by Keck and Sikkink (1998). TAN are complex networks with reciprocal and horizontal relations between domestic NGOs, INGOs, foundations, parts of government and Intergovernmental Organisations. They seek to attract attention

on a specific issue and influence policy outcome, often by framing the issue through morality. They emerge when domestic NGOs are not able to dialogue and solve an issue with the government, either because of lack of political will or the government's inability to address the problem. Domestic NGOs are able to call upon more powerful actors to pressure their government and thus obtain leverage on their issue. The different members of the TAN share their expertise, resources and values to try and mobilize public opinion and governments on blocked issues. To do so, they use four different tools: information, symbolic, leverage and accountability politics (Keck & Sikkink, 1998, pp. 2, 9, 12, 16).

DIGITAL RISKS TAKEN INTO ACCOUNT BY SUPPORT NETWORKS

The intensification of violence and surveillance by the state in Mexico over the past years (Botello, 2015) implies that support networks need to enlarge the scope of risks to address. Indeed, the digitalisation of practices in journalism and the spread of use of Internet in Mexico meant the growth of digital risks, including hacking by the state surveillance regime. In other words, with more access to Internet came novel digital risks exploited by the state surveillance regime which had to be taken into account by support networks.

Traditional human rights organisations are active in Mexico since the 1980s only. Indeed, Mexico had carefully built an image of a strong supporter of international human rights by taking in refugees from Chile after the 1973 coup. This credible international image combined with strong attention on abuses committed in the Southern Cone and Central America meant Mexico was not under international scrutiny. This changed from 1984 onwards with the creation of the Mexican Academy for Human Rights by Amnesty International activist Mariclaire Acosta. The intent was to create a human rights research centre for Mexico and the project received funding by the Ford Foundation (Keck and Sikkink, 1998, pp. 110-112).

Americas Watch published in 1990 a large report on human rights violations in Mexico. It discussed the positive reputation built by the country by denouncing its record for violations of human rights including electoral fraud, violence against the press and use of torture. This played a key-role in setting human rights on the agenda. Indeed, the subsequent creation of the National Commission on Human Rights came four days before the official announcement of negotiations for NAFTA in June 1990. Meanwhile, the Interamerican Commission on Human Rights found that Mexico did violate the

American Convention on Human Rights. The reports of the National Commission on Human Rights were written in English and Spanish and sent by express mail to human rights NGOs based in the US (Keck & Sikkink, 1998, pp. 112, f.).

Traditional human rights NGOs and new NGOs recently started to take the digital issue into account. For instance, Freedom House opened an office in Mexico in 2011 to provide training for digital protection and develop surveillance mechanisms to collect data and report crimes committed against these vulnerable categories (Freedom House, 2017). On the other hand, NGOs more specialized in the field of digital rights like R3D appeared in 2014 informally and was recognized as an association in 2015 (Tizo, 2016). Deeper analysis is required of the training and practices as well as the dynamics among the different members of the support network.

TAN ACTIVITIES AS PART OF SOCIAL SURVEILLANCE REGIME

To advocate for the protection of journalists and human rights defenders against digital threats, support networks use four different tools: information, symbolic, leverage and accountability politics (Keck & Sikkink, 1998, p. 16). Information, symbolic and accountability politics involve surveillance mechanisms used by support networks to set the agenda and counter state surveillance regime.

Information politics are practiced by generating credible information to attract attention on an issue. This involves the collection of information. For instance, the report Gobierno Espia (2017) is the product of monitoring the use of state surveillance capacities against journalists and human rights defenders in Mexico with the example of the use of state-owned spyware Pegasus against Aristegui Noticias.

Symbolic politics involve the creation or use of symbols for a target audience which is often far away and could therefore hardly relate to the issue otherwise. In other words, this means shaping information to produce symbols which would speak and appeal to foreign public opinion. Gobierno Espia puts faces on the victims of digital attacks. For instance, it is able to present Carmen Aristegui as a symbol for courage and persistence in spite of the risks she faces. In that sense, the report includes an extract of her speech at her ceremony for the Knight Prize for International Journalism in which she mentions risks of death for common journalists and abusive trials for more important journalists in Mexico (Article 19, 2017, p. 32).

Accountability politics mean ensuring that governments follow to the obligations conferred upon them by national or international law that they committed to. An example would be holding the state accountable for its obligations under the American Convention on Human Rights. As in the Aristegui case, using the means of the State to hack journalists and their parents is among others a violation of the freedom of the press because it seeks to intimidate and prevent journalists from exercising their freedom to inform and criticize activities of public officials. This involves collecting information about activities of the State in contradiction with its previous engagements.

Leverage politics seems to share fewer characteristics with the surveillance regime principle, but is nevertheless interesting in the process of protecting the vulnerable categories. Domestic NGOs unable to cooperate easily with the State to address a particular issue can gain leverage by appealing to a more powerful actor capable of influencing the State towards policy change. For instance, Citizen Lab found that a team of independent investigators sent by the Interamerican Commission on Human Rights (IACHR or CIDH in Spanish) to investigate the case of the massacre of 43 students trained to become teachers in Ayotzinapa was also hacked through the use of Pegasus malware (Scott-Railton, Marczak, Razzak, Crete-Nishihata, & Deibert, 2017). The investigation is the result of a deal between the Mexican government, the CIDH and representatives of the 43 disappeared teacher students (Organization of American States, 2017). In this context, political entrepreneurs in the support networks should be able to appeal to the OAS for accountability on this case as well as constitute a precedent for the Aristegui case.

In competition against the state surveillance regime, support networks protecting journalists and human rights defenders are incorporated in the social surveillance regime and integrate the new digital threat in the scope of their mission. They had to develop countersurveillance mechanisms essential to accomplish their goal which involve the collection of information for information, symbolic and accountability politics. Further research is required to see how successful they are, not only by trying to measure policy change, but also how they change habits among journalists and human rights defenders when using electronic devices.

CONCLUSION

In the context of insecurity in Mexico, journalists and human rights defenders face important physical

and psychological risks of being attacked, tortured, killed and live under permanent threat. In recent years however, digital threats have been growing and their vulnerabilities are being used by the state surveillance regime. In return, support networks seem to have reacted by integrating the digital threat issue by providing training and protection. In a competition between the surveillance regimes of the State and civil society, support networks as members of the social surveillance regime developed instruments to monitor State surveillance activities regarding digital attacks targeted against the vulnerable categories studied here. The framework of Transnational Advocacy Networks developed by Keck and Sikkink fits well into surveillance regime theory because information, symbolic and accountability politics involve collecting information for a specific objective, in this case, counter the influence of the surveillance regime of the State. Further research is required to provide a deeper analysis of how support networks address digital threats faced by journalists and human rights defenders, the connection between digital and physical threats. It would also be important to unpack underlying assumptions at play in the reports**,** what kind of definitions of journalism and activism interplay and how support networks practice social sorting and behave as surveillance regimes in competition with undertakings of the state surveillance regime.

REFERENCES

Botello, N. A. (2015). Doing Surveillance Studies in Latin America: The insecurity context. *Surveillance & Society, 13*(1), 78-90.

Article 19, Red en Defensa de Derechos Digitales & SocialTIC (2017). *#GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos en México.* Article 19, Red en Defensa de Derechos Digitales, SocialTIC. Retreived August 2017 from https://r3d.mx/2017/06/19/gobierno-espia.

Freedom House. (n. d.). *Freedom House*. Retrieved November 2017 from https://freedomhouse.org/nosotros.

Keck, M. E., & Sikkink, K. (1998). *Activists beyond borders: Advocacy networks in international politics.* London: Cornell University Press.

Organization of American States (s.f.). Retrieved November 2017 from *http://www.oas.org/es/cidh/actividades/giei.asp*.

Scott-Railton, J., Marczak, B., Razzak B. A., Crete-Nishihata, M. & Deibert R. (2017, July 10). *Citizen Lab.* Retrieved August 2017 from 'Reckless III Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware' [https://citizenlab.ca/2017/07/mexico-disappearances-nso].

Sierra, J. L. (2013). Digital and Mobile Security for Mexican Journalists and Bloggers. *Freedom House and the International Center for Journalists*. Retrieved August 2017 from https://freedomhouse.org/sites/default/files/Digital%20and%20Mobile%20Security%20for%20Mexican%20Journalists%20and%20Bloggers.pdf.

Suárez, X. & Zapico, D. (2017). Silencing criticism in Mexico. *Forced Migration Review,* (56), 8-9.

Tizo, J. (2016, October 26). *Revista Mexicana de Comunicación.* Retrieved December 2017 from 'R3D: Defendiendo los derechos digitales' [http://mexicanadecomunicacion.com.mx/rmc/2016/10/28/r3d-defendiendo-los-derechos-digitales].