**European Parliament Hearing**
*Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries*

January 21, 2015

Prepared by Sarah A. McKune
sarah.mckune@utoronto.ca

Senior Legal Advisor, The Citizen Lab
Munk School of Global Affairs
University of Toronto
http://citizenlab.org/

Thank you for the opportunity to participate in today's hearing. My name is Sarah McKune, and I am Senior Legal Advisor to The Citizen Lab, an interdisciplinary laboratory housed at the Munk School of Global Affairs, University of Toronto. For over a decade, the Citizen Lab has researched and documented information controls (e.g., Internet censorship and surveillance) that impact the openness and security of digital communications and pose threats to human rights. We use a mixed methods approach that combines techniques from network measurement, information security, law, and the social sciences to provide holistic analysis of the technical aspects and legal or policy ramifications of digital threats.

Assessing the impact on human rights of digital surveillance and intrusion systems is a critical inquiry. The question of impact speaks to the stakes involved in confronting this problem, the need for measures of prevention and redress, and the responsibilities associated with development and use of certain advanced technologies. Yet raising the question of impact also highlights the fact that there is a great deal we don't know about the scale and use of digital surveillance, as well as the short- and long-term repercussions of that surveillance on individual lives. By their very nature the surveillance industry and entities that engage in digital intrusion operate out of view of the public. Moreover, the combination of rapid advancements in technical capabilities, lack of transparency and public debate surrounding the dual-use technology industry, and the close ties of surveillance technology manufacturers with the apparatus of state security, has resulted in legal and regulatory gray areas in which companies have thus far operated with little oversight and relative impunity.

Through our research the Citizen Lab has sought to fill this gap in knowledge with empirical evidence regarding digital threats. We recently completed a four-year study of targeted digital threats[1] against civil society organizations and published a report, *Communities @ Risk*, that

[1] We distinguish targeted digital threats from mass surveillance, in that this type of threat is leveraged specifically against a chosen individual or entity, often for political reasons and tailored to the particular interests, systems, and operational landscape of the target.

details our findings.[2] Using malware analysis, interviews, and fieldwork, our study focused on the experiences of ten civil society groups, which provided greater visibility into the technical, social, and political nature of targeted digital threats. Additionally, we have studied the global deployment of technology that can be utilized for politically-motivated censorship and surveillance, including both spyware and "dual-use" technologies such as Internet filtering equipment.

We find that the human rights risks presented by digital threats are exacerbated by the quandary in which society now finds itself: nearly all parts of society are wired in some form, but only a privileged few are adequately secured.[3] Rarely do the privileged include civil society actors. Such imbalance presents a golden opportunity for government actors to exert digital control over their own populations, as well as dissent originating from abroad. It also creates points of leverage for threat actors that may not be government-linked. We have only just begun to scrape the surface of this rapidly evolving situation.

I'd like to share with the members of the European Parliament what we *do* know regarding the characteristics and impact of targeted digital threats, based on our research efforts; and some thoughts on what we *don't* know, but should find out as a matter of priority, through collaboration, transparency and accountability initiatives, and additional evidence-based research. I will then conclude with some final recommendations.

## What We Know

1. In the digital realm, civil society organizations face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.

Some of the very same threat actors targeting civil society for cyber intrusion and obstruction also target companies and government entities. In our research we identified ten distinct targeted malware campaigns, five of which had connections to threat actors and previous campaigns known to target government and private industry. Indeed, we found evidence that the widely reported-on group known as "Advanced Persistent Threat 1," which has been linked to the Chinese military and reported to have targeted Fortune 500 companies, embassies, and other high-value targets, targeted two of the groups participating in our study. This finding suggests that cyber espionage against civil society actors is deemed of sufficient strategic importance for attackers to pursue alongside industrial and state secrets. Yet civil society is insufficiently resourced, trained, and equipped to defend against such intrusion.

2. Counterintuitively, technical sophistication of malware used in these attacks is low, but the level of social engineering employed is high.

[2] Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society*, November 11, 2014, https://targetedthreats.net/.

[3] See generally Sarah McKune, "Privacy and security in cyberspace: right of all or luxury of the few?," openGlobalRights, December 16, 2014, https://www.opendemocracy.net/openglobalrights-blog/sarah-mckune/privacy-and-security-in-cyberspace-right-of-all-or-luxury-of-few.

We found that the technical sophistication of targeted malware delivered to groups in our study was relatively low, especially when juxtaposed with the commercial "lawful intrusion" surveillance kits that we've examined in other research. The majority of computer exploits we observed in our study were for known vulnerabilities that have been widely reported on and patched for long periods of time. We encountered only one zero-day exploit over the entire length of the study.

**Impact, however, does not necessarily correlate with technical sophistication**. Some of the most significant impacts are generated from the deployment of relatively unsophisticated malware. Once a compromise occurs, basic malware is no less dangerous than more advanced malware—even unsophisticated exploits can permit installation of Trojans providing the ability to search for and exfiltrate files and contacts, activate a device's video and audio recording, and log keystrokes. Many of the attackers we have encountered appear to employ malware that is only as technically advanced as it needs to be to generate results, investing fewer resources to rely on known exploits so long as their targets remain susceptible to them for behavioral reasons. Instead, attackers appear to invest more effort in crafting effective social engineering[4] by "getting to know" their target, through research and possible preliminary reconnaissance. Accordingly, while addressing the use of advanced intrusion software and IP network surveillance systems is essential, the problem is not discretely confined to such technology, and export controls are but one element of the response. We must concern ourselves as well with the broader practices at play, and make sure we address more generic and in-house capabilities that may never implicate official export channels.

3. Digital attacks against civil society organizations are persistent, adapting to targets in order to maintain access over time and across platforms.

Our analysis of attacks against civil society groups over four years allowed us to track how attackers change tactics. For numerous malware samples, we observed several versions of the malware appearing over time and showing evidence of technical improvements. In some cases we also observed threat actors quickly changing tactics to adapt to shifting platform adoption (e.g., changes in operating systems or use of mobile applications) and user behavior.

Such persistence demonstrates a disturbing level of commitment to a target. In the case of civil society organizations, which typically do not possess financial resources that would entice attackers, it is highly probable that this targeting is based on political and strategic rationales. At its core this is politically-motivated espionage. The targets are of long-term strategic value to the

[4] Social engineering is the attacker's method of crafting the delivery vector for the malware—typically an email—in a manner designed to entice recipients to open the infected payload. Social engineering techniques include "spoofing" the sender identity to appear as someone the target already knows and trusts; referencing timely and target-specific issues and events; repurposing real content taken from other sources of interest to the target; or attempting to exploit the emotions of the target by addressing sensitive, provocative, or inflammatory subjects. A high percentage of the emails we analyzed in our study were specifically tailored to the target through such techniques.

attackers, and targeted entities will find it difficult to “shake” an attacker and evade compromise over the long term.

4. Targeted digital threats undermine civil society organizations’ core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety.

The impact of targeted digital attacks against technical systems is apparent and receives ample attention from researchers. In the civil society context, however, we found evidence of wider impacts that are not always as obvious.

At one end of the spectrum of severity, targeted digital threats may undermine organizational efficiency, as staff time required for mission objectives is instead allocated to assessing and remediating an attempted intrusion. Additionally, an organization may incur significant financial burdens to prevent or remediate intrusions. Security assessments, remediation, secure communications infrastructure, and technically proficient staff are all expensive, and typically priced for a commercial market, not struggling nonprofits.

More significantly, targeted digital threats generate psychosocial impacts. They have resulted in chilling effects on online expression and use of particular digital mediums. For example, digital tools such as Skype and WeChat are both popular with audiences and effective in communicating with individuals around the world, but are known to have been targeted for government compromise in the past, and are therefore frequently avoided by civil society actors. In certain instances, the goal of an attacker may simply be communications degradation: to render untrustworthy promising communication techniques on which civil society might rely to conduct its work. Beyond chilling effects, impacts can include emotional and psychological strain. For example, within our study one individual described the discovery of an active compromise of a Skype account as “a huge invasion. It was quite upsetting. I think it sort of paralyzed us emotionally . . . for a few days.”

In the most serious instances, targeted digital threats have the potential to compromise an organization's human rights mission and individual safety. For example, Citizen Lab recently documented a customized malware attack against a Syrian citizen media group critical of the Islamic State of Iraq and Syria (ISIS); the attack was designed to obtain data revealing the group members’ physical location, and may have been the work of ISIS-linked hackers.[5] Other cases have been documented in which information obtained through the use of digital surveillance served as the basis for arrest, detention, and even torture.

5. Targeted digital threats extend the “reach” of the state (or other threat actors) beyond borders and into “safe havens.”

[5] John Scott-Railton and Seth Hardy, in collaboration with Cyber Arabs, “Malware Attack Targeting Syrian ISIS Critics,” December 18, 2014, https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/.

Digital espionage and cyber attack provide an effective means for threat actors, including state-linked attackers, to compromise groups and individuals located beyond physical borders. Diaspora and exile communities are frequently involved in discussion and support of rights movements in their country of origin; indeed, many individuals who have sought refuge overseas have done so to avoid persecution for involvement in political opposition or rights advocacy at home. Our research indicates that threat actors use targeted digital threats for extraterritorial compromise: to surveil and undermine overseas-based opposition, as though those individuals were still in the country from which they fled. The work of civil society is thereby rendered vulnerable regardless of the physical location from which it is conducted. This outcome raises significant questions concerning state sovereignty, use of existing channels for law enforcement cooperation, and the state's obligation to protect citizens and others within its jurisdiction from criminal activity.

For example, within our study we saw Tibetans targeted as a community for intrusion and digital espionage, with organizations located in Dharamsala and North America subject to constant attack. We have also seen the targeting of overseas exile organizations in the context of Ethiopia[6] and Bahrain,[7] with independent media and activists targeted by Hacking Team and FinFisher spyware, respectively.

## What We Don't Know

A few important topics that we **don't** know enough about, around which more research inquiries and transparency initiatives should be structured, include:

- *The relevant actors and products*. New technologies and industry players emerge regularly. What we do know about the companies active in this space, technical capabilities, and products of concern has been hard won, primarily through leaks and civil society investigations. At present we have no way to ensure a high-level, comprehensive, and up-to-date visibility into this space. What mechanisms are possible to acquire such visibility?

- *Companies' internal mechanisms for evaluation of human rights risks and grievances*. While some companies claim to perform human rights due diligence and take steps to prevent misuse of products, there is little to no transparency about these efforts. How can we better ensure corporate social responsibility measures and regulatory compliance are themselves open to public scrutiny and dialogue?

[6] Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Hacking Team and the Targeting of Ethiopian Journalists," Citizen Lab, February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/.

[7] Morgan Marquis-Boire and Bill Marczak, "From Bahrain With Love: FinFisher's Spy Kit Exposed?," Citizen Lab, July 25, 2012, https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/.

- *Distribution chains, resale and transshipment of sensitive technologies.* Some companies offering “dual-use” technologies rely on distributor networks and other mechanisms for product sales that render them one or more steps removed from the end user of the product. More information is necessary concerning distribution models and participants in such networks in order to strengthen accountability and oversight.

- *What use is made of information acquired through cyber espionage against civil society.* Much of what we know about digital threats centers around the intrusion itself, while very little is known about the systems, methods, and actors involved in analyzing and acting on the information acquired through such intrusion – the “post-processing.” This issue bears significantly on impact, and on the extent of the services offered by the private sector developers of intrusion software.

- *Who is affected.* Given how the technology at issue operates, and the evidence gathered thus far concerning its deployment, it is highly probable that widespread digital compromise is occurring of which we simply have no knowledge. While what we understand at present is of great concern, we must appreciate that we have obtained only a small glimpse of the problem through the research undertaken to date. We know for a fact that civil society is targeted – yet many of those affected have yet to be revealed.

## Recommendations

While the outlook for human rights in cyberspace has grown increasingly ominous, we are at a stage right now where smart and effective pushback against practices that infringe human rights is still possible. A few recommendations toward that end:

- To understand the extent and impact of digital surveillance and intrusion, we need better **tracking and documentation** of digital threat incidents. Concerted, collaborative efforts around gathering and analysis of data, which also respect the confidentiality and other concerns of those affected, are required.

- Trade-related measures such as export controls, with a focus on end users and end uses, are important to address digital threats. At the same time, such measures must go hand-in-hand with **political support** and **concrete sustained assistance** to civil society actors affected by digital threats. Diplomacy should unequivocally stress that civil society should be off-limits for digital espionage and attack, and confront the extraterritorial nature of digital targeting. States should also support a wide mandate for a **Special Rapporteur on the right to privacy** within the United Nations human rights system, which could serve as a linchpin in efforts to document and address digital threats.

- More action is necessary to **rectify imbalances in public access to digital security**. The gravity of this situation requires a rethink of the security standards applied in software and hardware used by the average person on a daily basis, to democratize security solutions and prevent compromise in the first instance. We need to further explore options for privacy by design and end-to-end encryption, and business models that do not rely on advertising methods that undermine privacy and generate security holes. With respect to civil society in particular, sustained, committed technical support is required to improve awareness, prevention, and response. Civil society organizations and individuals need to be equipped with straightforward frameworks and tools to discern and prevent compromise.

- In the private sector, human rights considerations must be normalized and understood as a part of doing business for all companies – large and small, as well as new market entrants. Introduction of **transparency requirements** in the surveillance industry is an important first step.

- **Security-related research and tools must be protected and encouraged**.
Cooperation with the technical community is critical to developing lasting solutions that protect society from digital surveillance and intrusion. Lawmakers should explore options for safe harbor legislation addressing security research that is in the public interest. Governments should also pursue policy measures to curb the growth of the market for tools that undermine encryption and digital security standards, and avoid driving such demand themselves.

Thank you.