Testimony for the U.S. Commission on International Religious Freedom (USCIRF) Hearing on Transnational Repression of Freedom of Religion or Belief, 10 May 2023.

Marcus Michaelsen, Senior Researcher, the Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto

To the Commissioners, thank you for the invitation to testify at USCRIF and the opportunity to provide information on digital transnational repression and its implications for the freedom of religion or belief.

My work focuses on digital transnational repression against political exiles and diaspora activists of different origins and across different host countries. My input builds on research carried out by myself and my colleagues. It represents my own views and not necessarily those of the Citizen Lab.

In my statement I will highlight some methods of digital transnational repression and their impacts on the targeted individuals and communities. I will also give recommendations on how the U.S. government should work in coordination with its European partners to counter digital repression and authoritarian reach across borders.

First, let me stress that digital technologies are a key element of all forms of transnational repression. The internet and social media have allowed migrants to stay closely connected to families and friends in their countries of origin. They have also helped diaspora activists and exiled dissidents to amplify their message and mobilize for human rights and political change from afar.

Yet, authoritarian power holders are using these very same technologies to monitor, threaten and intimidate political opponents and critics in other countries. Digital technologies have given repressive regimes new tools and methods for political control and repression beyond borders.

Regime agents comb through social media feeds and online media to gather so-called open source intelligence: information on media interviews, conference participations, meetings, friends and social relations which they can use against diasporas to blackmail and threaten them, or to prepare other, more targeted attacks.

They use tailored messages to trick targets into opening files compromised with malware, hack into their email and social media accounts and steal confidential information. For operations of targeted surveillance, governments purchase sophisticated spyware on a thriving, but obscure market of surveillance technologies.

The companies working in this field exploit vulnerabilities in widely used operating systems and applications to provide their customers with access to phone calls, personal files, emails, chats and geolocation data of targets.

Regimes also rely on paid trolls and artificial social media accounts to shape online narratives, spread disinformation and silence critical voices. Women activists and journalists are particularly exposed to defamation and disinformation campaigns that instrumentalize their gender to intimidate and discourage them from speaking out.

Second, digital transnational repression can have deep, and often very disturbing impacts. In interviews, the targets of online harassment or intrusive surveillance report mental stress, paranoia and social isolation. They reduce contacts to families and friends; they engage in self-censorship, or withdraw entirely from activism. Moreover, digital threats are often intertwined with other methods of transnational repression, such as threats against families in the home country and even physical assaults. With these methods regimes spread fear and mistrust in entire diaspora communities.

Third, digital transnational repression clearly interferes with the fundamental and human rights of those targeted. The most important among these rights are certainly the rights to privacy and to freedom of expression. Digital threats can also target individuals and communities on the basis of their religious identity or belief. To give a few examples:

- The Uyghur diaspora has been subjected to a wide range of digital attacks, including phishing campaigns, infiltrations of online meetings, smear campaigns on social media, and threatening calls on WhatsApp and other platforms from the homes of relatives in China's Uyghur region. China's large-scale campaign against the entire Uyghur society and culture is highly technologized, and China uses digital technologies to extend repression and surveillance across borders.
- Members of the Baha'i community have been targeted by hackers affiliated to the Iranian regime who tried to spy on them and steal their personal data. The attackers used an application that pretended to offer information relevant to the community but actually infiltrated the devices of users who installed it.
- In a number of host countries, women rights activists in the Iranian diaspora supporting the "Woman, life, freedom" protests against religiously motivated gender discrimination have been targeted by phishing attacks and defamation campaigns, among others.
- Women rights activists and journalists originating from Saudi Arabia and other Gulf countries had their smartphones infiltrated with the Pegasus spyware, an advanced surveillance tool.

Fourth, liberal democracies must work together to counter the authoritarian practices of digital transnational repression that undermine security, rule of law and democratic institutions. In Europe, where I live and conduct most of my research, the issue of transnational repression is often still blurred into discussions on foreign interference. (We also observe a similar tendency in Canada.) In particular when it comes to the link between globalized authoritarianism and digital technologies, the policy debate is primarily focused on disinformation campaigns and election manipulation as threats to the national security of European democracies. Under this view, diasporas with ties to authoritarian countries are seen as vectors for foreign interference and not as communities who require support and protection. Rather than as risk factors, migrants from authoritarian contexts (who were often persecuted for upholding their liberal rights) should be considered as strategic allies in the fight against expanding authoritarianism.

The U.S. government has recently taken a number of promising steps to coordinate efforts across different government branches to combat transnational repression, including in its digital variants. Civil society and researchers working on transnational repression will observe the implementation and impact of these measures with great interest. The U.S. government should pursue efforts to reach out to its European partners in order to get to a common, comprehensive definition of transnational repression and coordinate responses.

With regards to digital transnational repression, I'd like to highlight three areas of collaboration:

1) **Countering the proliferation of surveillance technologies**

In the European Union, the regulation of spyware falls under the umbrella of national security which is still the domain of each member state. This makes it harder for the EU to follow the example of the United States and ban or blacklist specific commercial spyware on an EU-wide level. Finding an agreement on the regulation of trade in and use of spyware in the EU will still take time. The U.S. government should push its European allies at the national level to establish fundamental conditions for oversight, transparency and a human-rights compliant safeguards regime.

The German government, for instance, is still absent from the list of signatories of the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. As a key EU member state, Germany has reportedly purchased the NSO Group's invasive Pegasus spyware. German intelligence agencies are also known to withhold information on vulnerabilities in commercial hard- and software to exploit them for surveillance operations. Other European governments, who either have used spyware against their own citizens or provided a harbor for key exporters in the spyware trade, have also not endorsed the Joint Statement. Commercial spyware companies should not be allowed to benefit from the EU's free market and reputation to sell their products to repressive governments.

2) Strengthening the digital resilience of civil society

More participatory and cross-sectoral mechanisms are needed for documenting, investigating and deterring cyber operations against civil society. Governmental cybersecurity organizations can play a key role in sharing threat intelligence, attributing attacks to perpetrators, and coordinating countermeasures. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has announced measures to bring technology companies, civil society organizations, and government together to strengthen the cybersecurity of US-based civil society organizations under threat of transnational repression. A key challenge will be to identify the right interlocutors among civil society and diaspora organizations, build trust, and find a common language. CISA should transparently share any lessons learned in this program with its counterparts in other democracies.

3) Improve the report and remedy mechanisms of platforms in cases of digital transnational repression

Targets of digital transnational repression still face hurdles in reporting threats and getting support from big tech companies. Victims of online harassment and defamation are expected to gather, review and share potentially traumatizing material. Automated reporting mechanisms do not allow to capture smear and disinformation campaigns in their entirety as they prioritize the review of single incidents. Tech companies need more staff with training on human rights, gender issues, and language skills to specifically liaise with targeted human rights defenders and activists, and provide direct assistance. Targets of digital transnational repression often complain that they don't have any interlocutors at the companies to address their requests for support and assistance.

Together with its European partners, the U.S. government should pursue efforts to bring platforms to improve the mechanisms for reporting and accountability for individuals and communities targeted by digital transnational repression (e.g., under the framework of the U.S.-EU Trade and Technology Council, TTC).