The House of Commons Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development

"Digital Transnational Repression: Tactics, Impacts, and Recommendations to Combat It"

January 9, 2025
Written Testimony
Based on an Oral Testimony Delivered on Tuesday, November 26, 2024

By: Noura Aljizawi
Senior Researcher at The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

Mr. Chairman and esteemed members of the committee, thank you for the opportunity to testify today and for your efforts to address the pressing issue of transnational repression.

My testimony today draws upon my research at the Citizen Lab. The Citizen Lab is an interdisciplinary research laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto, focused on research, development, and strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.[1]

Over the last two decades, the Citizen Lab has studied digital threats targeting civil society and human rights defenders in their home countries and across borders. In light of these threats, in 2019, the Citizen Lab launched a research program to specifically examine the growing trend of digital attacks against exiled human rights defenders, the chilling effects on those targeted,[2] and

[1] "About the Citizen Lab," The Citizen Lab, https://citizenlab.ca/about/.
[2] Nina dos Santos and Michael Kaplan, "Jamal Khashoggi's Private WhatsApp Messages May Offer New Clues to Killing," *CNN*, December 4, 2018, https://www.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html.; Raphael Satter, "Experts See Iranian Link in Attempt to Hack Syrian Dissident," *Associated Press*, August 2, 2016, https://www.apnews.com/6ab1ab75e89e480a9d12befd3fea4115. ; Andrea Peterson, "Spyware Vendor May Have Helped Ethiopia Target Journalists – Even After it Was Aware of Abuses, Researchers Say," *The Washington Post*, March 9, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/03/09/spyware-vendor-may-have-helped-ethiopia-spy-o

the connection between online and offline transnational threats. The aim of this program is to investigate the emerging phenomenon of *digital transnational repression*, defined below, by identifying the tactics used by state and non-state actors, assessing the impact of these tactics on human rights defenders, and providing recommendations for best practices that host countries, such as Canada, should adopt to address these human rights violations.

The Government of Canada pays significant attention to the threats posed by foreign interference (FI), including efforts by foreign states to influence elections, conduct cyber espionage, and attack critical infrastructure. *Foreign interference* refers to covert, deceptive, and malign actions undertaken by foreign state or non-state actors, or their proxies, aimed at undermining the sovereignty, national interests, or democratic institutions of a target state. In the digital era, these activities often leverage advancements in technology to disrupt critical infrastructure, manipulate public discourse, and influence political or social processes.[3]

While foreign interference is widely recognized, *digital transnational repression* (DTR)—a distinct and under-recognized subcategory of FI—represents a growing global threat to exiled human rights defenders, journalists, dissidents, and diaspora communities. Unlike FI, which primarily violates states' sovereignty, targeting states, their democratic processes, and institutions, DTR targets individuals and violates their human rights, including the rights to privacy, freedom of expression, and security.[4]

This form of repression undermines human rights, democracy, and civil liberties in Canada and other democratic countries. Yet, despite its far-reaching implications, DTR remains largely overlooked by policymakers, leaving exiled human rights defenders and vulnerable communities unprotected against this escalating threat.

What Is Digital Transnational Repression?

Transnational repression (TNR) is not a new phenomenon. It involves the extension of authoritarian practices to target diaspora members who have sought safety outside their country of origin. TNR extends domestic coercive methods to silence exiled human rights defenders by applying various methods, including assassination, kidnapping, and physical intimidation. More

---

n-journalists-even-after-it-was-aware-of-abuses-researchers-say/?noredirect=on.; Joseph Cox, "Bahraini Activists Claim They Were Targeted by FinFisher Surveillance in the UK," *Vice*, October 13, 2014, https://www.vice.com/en/article/bahraini-activists-claim-they-were-targeted-by-government-surveillance-in-the-uk/.;

[3] Dowling, Melissa-Ellen. 2021. "Democracy under Siege: Foreign Interference in a Digital Era." *Australian Journal of International Affairs* 75 (4): 383–87. doi:10.1080/10357718.2021.1909534.
[4] United Nations (n.d.), *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights.; Government of Canada, Department of Justice. 2022. *Rights and Freedoms in Canada*. Last modified March 23, 2022. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/index.html.

subtle tactics also play a key role in TNR, such as misusing Interpol notices to arrest and deport exiled dissidents, cancelling passports, and denying access to consular services, among other mobility controls.[5]

Digital technologies have made it easier for states to expand their repression beyond borders. *Digital transnational repression* arises when states use digital tools and services to surveil, intimidate, and silence dissenting voices in exiled and diaspora communities. These tactics include the use of spyware and malware; phishing (a malicious attempt to obtain sensitive information through emails, text messages, or websites by impersonating trusted persons or entities); harassment; disinformation; and smear campaigns aimed at discrediting targeted individuals.[6] Private companies that develop and sell surveillance technology or offer surveillance services play a critical role in DTR by further enabling states to target human rights defenders and dissidents in exile.

The line between online and offline repression is often unclear, as digital threats frequently evolve into physical intimidation. For example, in 2018, the Citizen Lab revealed that Saudi activist Omar Abdulaziz, based in Montreal, had his phone compromised with Pegasus spyware.[7] This attack, attributed to a Saudi-linked operator, gave full access to Abdulaziz's device and private communications with fellow dissidents, including messages exchanged with journalist Jamal Khashoggi just weeks before Khashoggi's assassination. Abdulaziz also endured physical threats and attempts to lure him back to Saudi Arabia.[8]

This incident inspired the Citizen Lab to look at how exiled dissidents are targeted and impacted by digital threats.

Targets of Digital Transnational Repression

It is a common misconception that exile inherently provides safety for vulnerable individuals. However, transnational repression and its digital dimensions tell another story. The targets of

---

[5] Freedom House (n.d.), "Transnational Repression," https://freedomhouse.org/report/transnational-repression; Nate Schenkkan and Isabel Linzer (2021), "Out of Sight, Not Out of Reach," *Freedom House https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf*

[6] *Ibid.;* On coercion-by-proxy, see Fiona Adamson and Gerasimos Tsourapas (2020), "At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression," *Freedom House,* https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression.

[7] Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ronald Deibert, "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," The Citizen Lab, October 1, 2018, https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

[8] Nina Dos Santos and Michael Kaplan, "Jamal Khashoggi's WhatsApp Messages May Offer New Clues to Killing," *CNN*, December 4, 2018, https://www.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html.

digital transnational repression are often exiled diaspora human rights defenders (HRDs).[9] Many HRDs have sought refuge in democratic countries, assuming these environments provide them space to exercise their human rights and escape political repression by their home governments. Yet, even in exile, human rights defenders remain vulnerable to harassment, intimidation, and threats from their home states.

These threats are especially stark for individuals who fall at the intersection of multiple high-risk groups. Asylum seekers, refugees, and migrants often face systemic discrimination in host countries, compounded by other barriers of language, economics, and a lack of social support. At the same time, their human rights activism makes them targets of transnational repression by their home state and its state-related actors.[10] These individuals are particularly vulnerable, as they must navigate the challenges of day-to-day life and systemic inequities in a new environment, while continuing their activism and resisting threats and harassment from state actorsseeking to silence them.

This vulnerability is further exacerbated for exiled women human rights defenders, as state and state-related actors orchestrate gender-based attacks that mirror the political and gender-based repression they faced in their home countries. Exiled and diaspora women human rights defenders targeted through digital transnational repression endure not only the same digital threats as their male counterparts but also gender-specific forms of online harassment, abuse, and intimidation.

Findings from Citizen Lab's Research on DTR

Over the past five years, my colleagues at the Citizen Lab and I have studied the experiences of 103 exiled dissidents in Canada and other democracies. This figure represents the combined total from two major research studies. In the first study, we interviewed 18 exiled dissidents in Canada.[11]. In the second study, we examined DTR on a global scale,[12] drawing on interviews

[9] We use the term Human Rights Defender to refer to diverse areas of activism, such as human rights, law, journalism, advocacy, political activism, research, and art.

[10] Scott-Railton, John. "Security for the high-risk user: separate and unequal." *IEEE Security & Privacy* 14, no. 2 (2016): 79–87. https://ieeexplore.ieee.org/document/7448342?denied= . See also: Nunez, Bryan, Elizabeth Eagen, Eric Sears, John Scott-Railton, and Michael Brennan. "Digital Security & Grantcraft Guide: an Introduction Guide for Funders." Ford Foundation (2017). https://www.fordfoundation.org/wp-content/uploads/2017/02/digital-security-grantcraft-guide-v10-final-22317.pdf.

[11] Aljizawi, Noura, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ronald Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab*, https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/.

[12] Aljizawi, Noura, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybulla, Muetter Iliqud, Nicola Lawford, Émilie LaFlèche, Gabby Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang. "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression*," The Citizen Lab,* Report No. 180, University of Toronto, December 2024. https://citizenlab.ca/2024/12/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/.

with 85 participants residing in 23 countries, including the United States, Germany, Canada, France, the United Kingdom, Sweden, and Norway. Participants of both studies were interviewed anonymously using semi-structured interviews, employing a trauma-informed approach to ensure sensitivity to their past experiences. We analyzed the participant data through thematic analysis, incorporating an intersectional lens to account for the complex interplay of factors such as gender, race, refugee or immigration status, and histories of trauma. Particular care was taken to address participants' vulnerabilities and safeguard their confidentiality. Our research revealed:

1. **Widespread perpetration**: Our interviews with targets revealed that over 20 state actors[13] are engaged in digital transnational repression. Participants in our study on digital transnational repression in Canada originated from diverse regions and countries, including Syria, Saudi Arabia, Yemen, Tibet, Hong Kong, China, Rwanda, Iran, Afghanistan, East Turkestan, and Balochistan.[14]
2. **Blurred lines with offline repression**: Digital threats often escalate into physical threats, such as surveillance, stalking, the disruption of events, in-person confrontations, verbal harassment, and even direct threats against or the targeting of family members, including children. In some cases, individuals are physically targeted, blurring the boundaries between online and offline threats and compounding the fear experienced by targets.
3. **Chilling effects**: Despite their resilience, targets reported experiencing the chilling effects of DTR. They described significant impacts on their well-being, sense of security, and personal freedoms. Many reported emotional, psychological, professional, and financial distress. Some became socially isolated, felt compelled to cut ties with family and friends back home, or decided to cease their activism altogether. A particularly troubling consequence of DTR is its impact on refugee, immigration, and citizenship status. Targets shared that they faced legal and bureaucratic challenges, including delayed or denied refugee recognition, suspension of accommodations, and scrutiny over their eligibility for citizenship or residency.[15]
4. **Gendered dimensions of digital transnational repression**: Women targeted by DTR experience additional layers of gender-based harassment and abuse. States exploit patriarchal norms and gender and sexual identities to silence exiled women activists through gender-based digital transnational repression. Strategies like targeting their reputations, violating their privacy, and disseminating false

[13] *Ibid*.
[14] Aljizawi et al., "Psychological and Emotional War,"
[15] See: Dounian's story in Aljizawi et al., "No Escape"; Maria Kartasheva, "For Anti-War Russians Abroad Like Me, Nowhere Feels Safe," *The Moscow Times*, June 14, 2024, https://www.themoscowtimes.com/2024/06/14/for-anti-war-russians-abroad-like-me-nowhere-feels-safe-a85404.; Committee to Protect Journalists. "CPJ Partners Call for Transparency as Exiled Syrian Journalist Applies for UK Citizenship." *Committee to Protect Journalists*, October 2024. https://cpj.org/2024/10/cpj-partners-call-for-transparency-as-exiled-syrian-journalist-applies-for-uk-citizenship/.

images or narratives online aim not only to discredit exiled women human rights activists but also create a ripple effect of social pressure within their close communities. Families or partners of targets often face shame and stigma, urging women to cease their activism.[16] Leveraging societal norms and expectations for the purpose of gender-based digital transnational repression allows states to weaponize both direct harassment and the resulting communal backlash. This forces women to navigate a complex web of personal, familial, and social constraints, compounding the challenges they face as exiled activists. These overlapping struggles—activism, repression, social backlash, and exile—intensify the obstacles to their work and amplify their vulnerability.

5. **Inadequate host state responses**: Many victims reported to law enforcement but found responses insufficient. Several documented incidents and accounts from affected individuals highlight this concern. For example, the Saudi dissident, Omar Abdulaziz was subjected to digital transnational repression via Pegasus spyware in 2018[17] and faced offline threats by two Saudi emissaries who approached him in Montreal to coerce his return to the kingdom while in Canada.[18] Despite the severity of these incidents, preventive measures were not taken. It was only two years later that the Royal Canadian Mounted Police (RCMP) warned Abdulaziz that he was a "potential target" of the Saudi government and advised him to take proactive measures.[19]
6. **Inaction by host states can embolden perpetrators to escalate their attacks**: Exiled Chinese activists in Canada like Sheng Xue, a Chinese-Canadian journalist and human rights advocate, have reported persistent harassment and intimidation by actors linked to the Chinese Communist Party (CCP).[20] These threats have been raised with law enforcement, media, and policymakers, yet limited action has been taken. This perceived inaction coincided with the escalation of CCP transnational repression in Canada, particularly over the last decade. This includes the expansion of the scope of targets, the establishment of unauthorized police

---

[16] Aljizawi et al., "No Escape"; Noura Aljizawi, Siena Anstis, and Marcus Michaelsen, "Exiled Women," *Middle East Report* 307/308 (Summer/Fall 2023), https://merip.org/2023/09/exiled-women/.

[17] Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ronald Deibert (2018), "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," *The Citizen Lab* https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

[18] Douglas Quan, "In the Crosshairs of a Crown Prince? Canadian Hit-Squad Claim Just Latest Allegation Against Controversial Saudi Royal," *The Star (Vancouver Bureau)*, February 13, 2021. https://www.thestar.com/news/canada/in-the-crosshairs-of-a-crown-prince-canadian-hit-squad-claim-just-latest-allegation-against/article_16de2623-6ec6-5c50-b864-fca0c024f7e6.html.

[19] Hinnant, Lori, and Maggie Michael, "Exclusive: Saudi Dissident Warned by Canadian Police He Is a Target," *The Guardian*. Last modified June 21, 2020. https://www.theguardian.com/world/2020/jun/21/exclusive-saudi-dissident-warned-by-canadian-police-he-is-a-target.

[20] Isabella Chai, "China's Transnational Repression Campaign Reaches Canadians," *New Canadian Media*, March 12, 2021. https://www.newcanadianmedia.ca/chinas-transnational-repression-campaign-reaches-canadians/.

service stations, and the targeting of Canadian elected officials like MP Michael Chong.[21] Additionally, inadequate responses to Iran's online and offline transnational repression have coincided with the reported Iranian state's attempted assassination of Canada's former justice minister Irwin Cotler.[22] These examples underscore the potential consequences of insufficient responses, which may embolden perpetrators to expand their repression and escalate their threats in liberal democracies like Canada.

Recommendations to Address Digital Transnational Repression

Digital transnational repression poses a growing threat to democracy and civil liberties in Canada and other democratic countries. Our research reveals a strong correlation between online and offline threats. This overlap amplifies the risks of transnational repression, as host states' failure to investigate and protect vulnerable individuals from online attacks may embolden perpetrators to escalate to physical violence.

Researchers outside the Citizen Lab have proposed a range of recommendations to address transnational repression, including its digital dimensions and the spread of spyware.[23] These recommendations address various actors implicated in transnational repression, including host states, social media and technology companies, and civil society organizations. Other research gives substantive recommendations on tackling technology-facilitated gender-based violence, emphasizing the role governments, social media platforms, and civil society can play in preventing and mitigating these harms.[24]

---

[21] Global Affairs Canada. (n.d), "WeChat and Transnational Repression: Protecting Canada's Democracy." https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/wechat.aspx?lang=eng.

[22] CBC News. "RCMP Says It Foiled Iranian Plot to Kill Former Justice Minister Irwin Cotler." November 18, 2023. https://www.cbc.ca/news/politics/rcmp-foils-plot-to-kill-irwin-cotler-1.7386253.

[23] See, for example, Freedom House (undated), "Policy Recommendations: Transnational Repression," https://freedomhouse.org/policy-recommendations/transnational-repression; Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ronald Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf; Siena Anstis, Ronald J. Deibert, and John Scott-Railton (2019), "A Proposed Response to the Commercial Surveillance Emergency," *Lawfare,* https://www.lawfaremedia.org/article/proposed-response-commercial-surveillance-emergency.; Noura Aljizawi, Gözde Böcü, and Nicola Lawford (2024), "Enhancing Cybersecurity Resilience for Transnational Dissidents," *Center for Long Term Cybersecurity* https://cltc.berkeley.edu/publication/cyber-resilience-for-transnational-dissidents/.

[24] Cynthia Khoo (2021), "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence," *Women's Legal Education and Action Fund* https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf.; Suzor, Nicolas, Molly Dragiewicz, Bridget A. Harris, Rosalie Gillett, Jean Burgess, and Tess Van Geelen (2018), "Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online," *Policy & Internet* 11(1), https://doi.org/10.1002/poi3.185.

To address the escalating threat of digital transnational repression on human rights defenders in Canada, I recommend that the Government of Canada prioritize action in four key areas:

1. **Legislative and Policy Reforms**
    - **Close legislative gaps**: Develop laws specifically addressing digital transnational repression, and revise national security, immigration, and refugee frameworks to prevent harms to targets.
    - **Differentiate digital transnational repression from broader foreign interference**: Address DTR as a distinct systemic threat requiring targeted solutions.
2. **Hold Perpetrators Accountable:**
    - Both **state** and **private actors should be held accountable.**
        - For state actors:
            - Make official statements against digital transnational repression and ensure that the Canadian government's policies and activities demonstrate that the protection of human rights both at home and abroad is a priority.
            - Examine the possible use of targeted sanctions against foreign states, individuals, and entities that are responsible for, or complicit in, transnational repression, including its digital dimension.
            - Review foreign state immunity laws in Canada and implement the necessary changes to ensure that individuals subjected to digital transnational repression by foreign state actors are able to pursue legal remedies in Canada.
        - For the private sector:
            - **List surveillance technology vendors**: Identify companies whose tools are used in DTR and implement sanctions or export bans, building on efforts like the US government's export restrictions on mercenary spyware vendors.
            - **Engage with platforms**: Demand transparency from tech companies facilitating repression and require stronger safeguards, such as mandatory encryption and two-factor authentication.
3. **Support for Targets**
    - **Establish a dedicated governmental institution:** Create a "whole-of-government" agency to monitor, report, and respond to DTR systematically.
    - **Empower targets:** Develop dedicated reporting mechanisms and provide digital security resources, legal assistance, and mental health support to targets.
    - **Engage with diaspora communities:** Work directly with exiled activists and their organizations to design actionable, inclusive policies.

- **Adopt an intersectional approach:** Recognize the unique vulnerabilities of women, racialized groups, and other marginalized targets of DTR, and ensure tailored responses.

4. **Global Cooperation**: Transnational repression is a global problem that requires a global response.
5. **Ensure Human Rights-Centered Treaties and Agreements:** Canada must critically assess international treaties and agreements to ensure these instruments do not facilitate transnational repression or undermine human rights. For example, the draft *UN Convention Against Cybercrime* has been widely criticized by experts and civil society organizations for its potential to become a powerful tool for authoritarian governments, which might abuse its expansive surveillance and cross-border cooperation mechanisms for the purposes of digital transnational repression.[25]

Conclusion

Digital transnational repression threatens not only the human rights of targeted individuals and communities but also the security, rule of law, and democratic institutions of host countries. By adopting a whole-government approach, holding perpetrators accountable, engaging the private sector, supporting the resilience of communities at risk, and expanding global cooperation, Canada can take meaningful steps to respond to and prevent DTR.

Thank you for your time and attention. I am happy to answer any questions or provide further insights to support your work on this critical matter.

[25] See the open letter jointly submitted by civil society organizations and experts, which outlines specific flaws in the draft treaty and emphasizes the importance of prioritizing human rights safeguards in international agreements. Alexandra Posadzki, "Canada Urged to Not Sign 'Deeply Flawed' UN Cybercrime Treaty," *The Globe and Mail*, December 12, 2024. https://www.theglobeandmail.com/business/article-canada-urged-to-not-sign-deeply-flawed-un-cybercrime-treaty/.