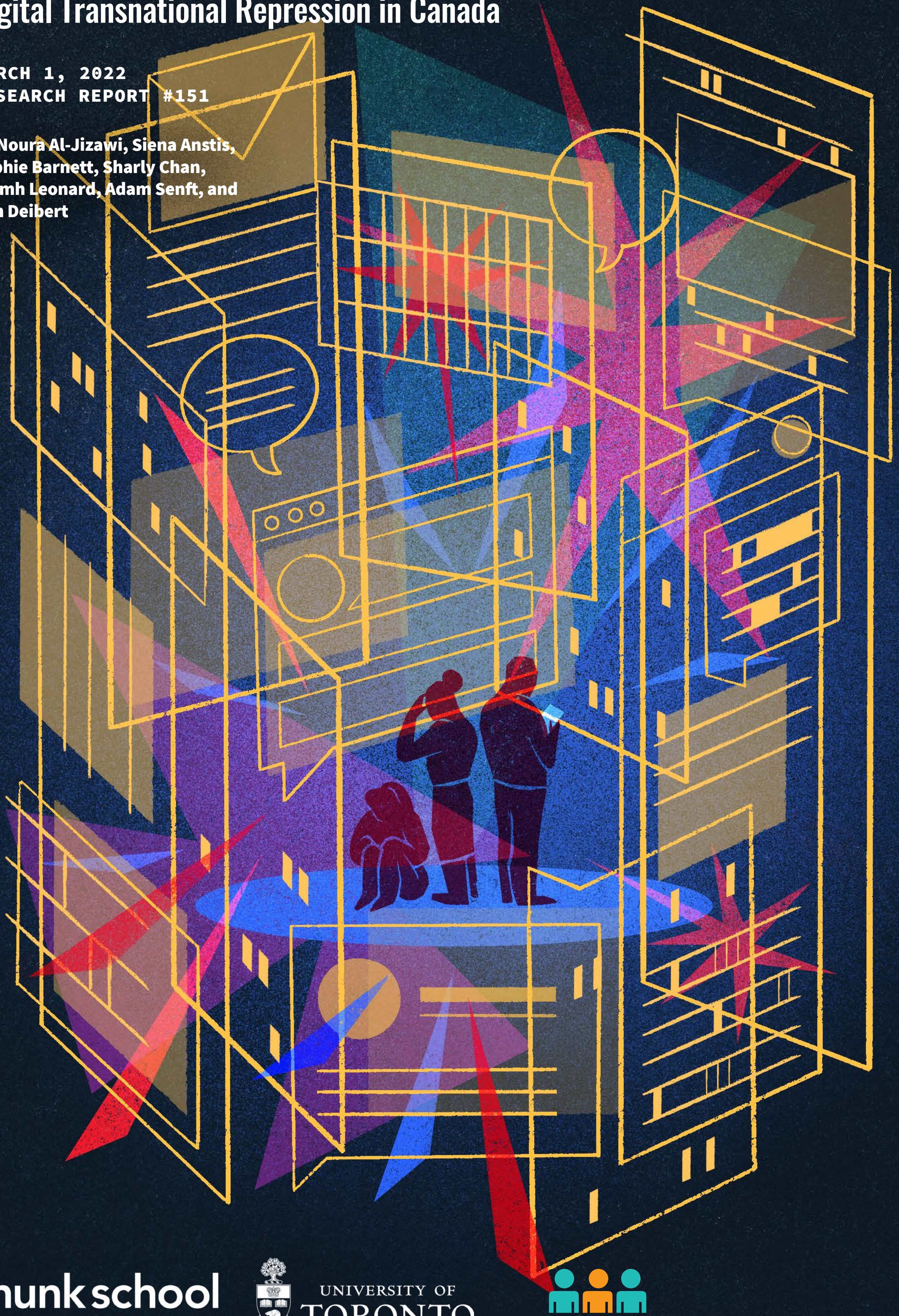
PSYCHOLOGICAL AND EMOTIONAL WAR

Digital Transnational Repression in Canada

MARCH 1, 2022
RESEARCH REPORT #151

By Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert



munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THE CITIZEN LAB

Copyright

Document Version: 1.1

Suggested Citation

Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert. "Psychological and Emotional War: Digital Transnational Repression in Canada," Citizen Lab Research Report No. 151, University of Toronto, March 2022.

Acknowledgements

We would like to acknowledge and thank all research participants who generously agreed to be interviewed for this report and to share their personal experiences. Their stories underscore the courage it takes to engage in human rights activism, and we are grateful for their willingness to speak with us.

We would also like to thank Masashi Crete-Nishihata and Marcus Michaelsen for their peer reviews of this report, Céline Bauwens, Émilie LaFlèche, and Joyce Parsons for copyediting, Bill Marczak, Bahr Abdul Razzak, and John Scott-Railton for their assistance in digital investigations, and Mari Zhou and Miles Kenyon for their assistance in designing and formatting this report. The cover illustration and the activist profile illustrations are by Ryookyung Kim.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Introduction

The efforts of authoritarian states to suppress dissent are not territorially limited. Over the past few years, there have been many notable cases of *transnational repression*—states implementing repressive policies to silence or coerce nationals located outside their territorial borders—including the Saudi killing of Jamal Khashoggi in Turkey,[1] the assassination of Rwandan opposition members and dissidents in South Africa and elsewhere,[2] and the harassment and intimidation of Chinese dissidents in Canada and the United States.[3] While transnational repression is not a new phenomenon, such practices are expanding through the market growth of digital technologies and the spread of Internet connectivity, among other factors.[4] This digital dimension of transnational repression—which we refer to as *digital transnational repression*—is rapidly becoming the cornerstone of everyday transnational repression and is a threat to the rights and freedoms of dissidents and activists who are living in exile.

In this report, we describe how activists and dissidents living in Canada are impacted by digital transnational repression. We conclude that *digital transnational repression has a serious impact on these communities*, including their ability to undertake transnational advocacy work related to human rights. *Yet, there is little support for victims who experience such targeting and policy efforts by the Canadian government to date have been insufficient*. This finding is troubling, considering that the Trudeau government purports to welcome migrants and refugees to Canada and has made the promotion of democracy and human rights a cornerstone of its political platform. While the government has begun to address the threat of foreign interference in Canada—a term broad enough to capture digital transnational repression—its focus has primarily been on digital threats related to Canadian democratic institutions, economic interests, and critical infrastructure. The protection of the rights and freedoms of migrants and refugees appears to be of little concern.

[1] BBC News (2021), "Jamal Khashoggi: All You Need to Know About the Saudi Journalist's Death," *BBC News* (24 February 2021) <https://www.bbc.com/news/world-europe-45812399>.

[2] Abu-Bakarr Jalloh (2021), "Rwanda: The Mysterious Deaths of Political Opponents," *DW* (15 September 2021) <https://www.dw.com/en/rwanda-the-mysterious-deaths-of-political-opponents/a-59182275>; BBC News (2021), "Rwandan Seif Bamporiki Killed in South Africa," *BBC News* (22 February 2021) <https://www.bbc.com/news/world-africa-56119088>.

[3] Catherine Porter (2019), "Chinese Dissidents Feel Heat of Beijing's Wrath. Even in Canada," *New York Times* (1 April 2019) <https://www.nytimes.com/2019/04/01/world/canada/china-dissident-harassment-sheng-xue.html>.

[4] In this report, we consider transnational digital repression to include anything from social media harassment campaigns (such as public, semi-public, or private harassment on Twitter or Facebook) or online messaging and communications platforms (such as WhatsApp or Skype) to the use of sophisticated spyware and malware. In all cases, these activities feature a digital technology component on either the part of governments or those targeted by them.

In light of this policy deficit, the threat to democracy and human rights, and the impact of digital transnational repression on Canadian communities, we make a series of recommendations for the Canadian government where concrete action could be taken to address digital transnational repression. These recommendations include:

- issuing official statements against digital transnational repression and taking practical action to deter such activities, such as deploying targeted sanctions, strengthening export controls for dual-use technologies, reviewing foreign sovereign immunity law, pursuing criminal prosecutions, and ensuring that the Canadian government's own use of digital surveillance technology is transparent and in compliance with Canadian human rights law and international human rights law
- providing support to the victims of digital transnational repression by creating a dedicated government agency to address the issue of transnational repression in Canada, instituting a dedicated hotline or reporting mechanism, and undertaking community outreach efforts to better understand the scale of the problem and how to address it
- improving coordination across Canadian government bodies, training government officials in identifying, addressing, and responding to digital transnational repression, and providing greater resources for community organizations to address such threats
- requiring transparency from technology companies regarding how they respond to government requests to remove content or access user information, engaging with these entities to understand how they address digital transnational repression and what other measures have to be taken, and examining the role of business actors more broadly (for example, social media companies and other private sector facilitators such as domain registrars, web-hosting companies, and other companies whose technology is used in undertaking digital transnational repression) to determine whether new regulation is required to address their role

In **Section 1** of the report, we introduce traditional mechanisms of transnational repression and the exercise of extraterritorial authoritarianism. In **Section 2**, we review existing research on how digital transnational repression manifests itself and impacts activists and dissidents in exile. In **Section 3**, we summarize the findings that were drawn from interviews we conducted with activists and dissidents who moved or fled to Canada from their country of origin and who were targeted by various forms of digital transnational repression in Canada. In closing, in **Section 4**, we set out a series of recommendations for the Canadian government to begin addressing digital transnational repression in Canada.

Section 1: An Introduction to Transnational Repression

The term transnational repression describes how authoritarian states "reach across national borders to silence dissent among diaspora and exile communities."[5] It can be distinguished from so-called soft power efforts in that transnational repression "do[es] not seek to win influence through the powers of attraction, but instead aim[s] to divide, subvert, co-opt, and coerce."[6]

States that engage in transnational repression use a variety of methods to silence, persecute, control, coerce, or otherwise intimidate their nationals abroad into refraining from transnational political or social activities that may undermine or threaten the state and power dynamics within its borders. Thus, nationals of these states who reside abroad are still limited in how they can exercise "their rights, liberties, and 'voice'" and remain subject to state authoritarianism even after leaving their country of origin.[7]

Indeed, transnational repression breaks down boundaries between domestic forms of control and efforts aimed at controlling those who reside abroad.[8] It is a phenomenon that "challenge[s] the singular conceptualization of sovereignty and encourage[s] new understandings of the idea of 'state space.'"[9] Rather than managing a territory with boundaries and closed borders, authoritarian states are now increasingly managing the "'space of flows,' the ever-shifting transnational spaces formed by travel, migration, and international financial structures."[10] The result is the production of "a 'state effect' far beyond their own frontiers."[11]

[5] Nate Schenkkan and Isabel Linzer (2021), "Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression," Freedom House at 3 <https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf> [Schenkkan and Linzer, Freedom House Report].

[6] *Ibid* at 8.

[7] Dana M Moss (2016), "Transnational Repression, Diaspora Mobilization, and the Case of The Arab Spring," *Social Problems* 63(4) at 481 <https://academic.oup.com/socpro/article/63/4/480/2402855> [Moss, "Case of the Arab Spring"]; Fiona B Adamson (2020), "Non-State Authoritarianism and Diaspora Politics," *Global Networks* 20(1) at 153 <https://doi.org/10.1111/glob.12246>.

[8] Fiona B 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> [Adamson and Tsourapas, "Coercion-by-Proxy"].

[9] David Lewis (2015), "'Illiberal Spaces:' Uzbekistan's Extraterritorial Security Practices and the Spatial Politics of Contemporary Authoritarianism," *Nationalities Papers* 43(1) at 141.

[10] *Ibid*.

[11] *Ibid* at 143.

While acts of transnational repression have long been undertaken by states, researchers have noted that such acts are increasing as states are "integrated into a global system of transnational economic flows and international migration."[12] The following four categories of transnational repression emerge:

- *Direct attacks* are those in which "an origin state carries out a targeted physical attack against an individual abroad."
- *Co-opting other countries* describes a situation where states manipulate other states "to act against a target through detention, unlawful deportation, and other types of forced renditions, which are authorized through pro forma but meaningless legal procedures."
- *Mobility controls* define tactics including "passport cancellation and denial of consular services, preventing the target from travelling or causing them to be detained."
- *Threats from a distance* include "online intimidation or surveillance and coercion by proxy, in which a person's family, loved one, or business partner is threatened, imprisoned, or otherwise targeted."[13]

In this report, we focus on the use of digital transnational repression, which falls under the final category of threats from a distance.

Between 2014 and 2020 alone, researchers who studied transnational repression identified 608 cases of direct, physical transnational repression. This figure, which is likely incomplete due to the exclusion of cases that have no or insufficient public documentation, includes 31 states—China, Rwanda, Russia, Iran, Saudi Arabia, and Turkey among them—that have been conducting transnational repression in 79 host countries.[14] It identifies a clear link between authoritarian perpetrators and overseas victims. In China, for example, victims included overseas Tibetans, Falun Gong practitioners, advocates for democracy in Hong Kong, and Taiwanese citizens. Likewise, the victims of Russian suppression efforts include Chechen citizens residing in Turkey, and it is well-documented that Saudi dissidents Jamal Khashoggi and Omar Abdulaziz were targeted by the Saudi regime.[15]

Despite the severity of the threat to the rights and freedoms of activists and dissidents outside their country of origin—as well as to democracy and the rule of law more generally—that is posed by transnational repression, perpetrators are rarely held to account

[12] *Ibid* at 141.

[13] Schenkkan and Linzer, Freedom House Report at 9.

[14] *Ibid* at 2.

[15] *Ibid* at 15–41.

and the practice continues to grow. Transnational repression is increasingly seen as "a common and institutionalized practice used by dozens of regimes" to control millions of people worldwide.[16]

The threat of transnational repression has grown across the following three dimensions: (1) states' perception of the threat posed by exiles, (2) availability of resources and capacity for suppression by states, and (3) cost-benefit calculations for exercising suppression with benefits surpassing costs.[17] While physical or in-person transnational repression is perhaps the most visible tactic (and, even then, much of this activity likely occurs in the shadows), it is only the tip of the iceberg. The tactics of "everyday transnational repression"—particularly acts of digital transnational repression—are simultaneously much less visible and understood but much more widespread.[18]

One major impact of transnational repression is a global chilling of political and social speech and activity (for example, silencing activists who are living abroad through self-censorship and self-restraint to avoid punishment).[19] Canadian Chinese community members, for instance, have reported that they do not ask questions at public events or attend protests or other events in Canada out of fear that Chinese government agents are watching them.[20] Some testified to a Canadian Senate Committee that they were "threatened with rape or even death" if they kept "speaking out against [human rights] violations committed by China."[21]

One study with Iranian journalists and activists in exile observed how the Iranian government sought to disable the dissidents' "voice."[22] This silencing effort was easily delivered through digital tactics, which activists interpreted as a message from Iranian security agencies that they were being surveilled.[23] While these tactics may not always stop the

[16] *Ibid* at 2.

[17] *Ibid* at 5.

[18] *Ibid* at 2.

[19] Marcus Michaelsen (2020), "Silencing Across Borders: Transnational Repression and Digital Threats Against Exiled Activists from Egypt, Syria, and Iran," Hivos <https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf> [Michaelsen, "Silencing Across Borders"].

[20] Yaqiu Wang (2019), "Why Some Chinese Immigrants Living in Canada Live in Silent Fear," *The Globe and Mail* (25 February 2019) <https://www.theglobeandmail.com/opinion/article-why-some-chinese-immigrants-living-in-canada-live-in-silent-fear/>.

[21] Charles Burton (2020), "China Threatens and Intimidates People Within Canada as Ottawa Remains Silent," *The Toronto Star* (8 September 2020) <https://www.thestar.com/opinion/contributors/2020/09/08/china-threatens-and-intimidates-people-within-canada-as-ottawa-remains-silent.html>.

[22] Marcus Michaelsen (2017), "Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran," *Surveillance & Society* 15(3/4) at 467 <https://doi.org/10.24908/ss.v15i3/4.6635> [Michaelsen, "Far Away, So Close"].

[23] Marcus Michaelsen (2016), "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State," *Globalizations* 15(2) at 256 <https://doi.org/10.1080/14747731.2016.1263078> [Michaelsen, "Exit and Voice"].

work of activists, they do "create pressure and additional costs, as activists are forced to consider their online behavior and protect their communications."[24] Repression also sends a message to other members of the diaspora that they should refrain from engaging in similar behaviour.[25] Further, self-censorship leads "victims of transnational repression to purposefully avoid alerting local law enforcement to threats to their personal safety."[26] Repression undermines the capacity of the diaspora to engage in independent journalism, curbs the ability of universities to ensure free speech, and makes public demonstrations in host countries a dangerous activity.[27]

Family members who reside in the country of origin may also be caught in the practice. Authoritarian regimes threaten and detain exiled dissidents' family members within their borders to send a warning to halt anti-regime activity abroad.[28] The Iranian regime, for instance, has paired threats against dissidents with threats against or the detention of family members who reside within Iran.[29] Iranian activists have sought to protect their relatives back home by keeping them "at arm's length."[30] Dissidents are forced to either silence themselves or cut ties with their family members in order to protect them. Through interviews with Syrian activists based in the United States and the United Kingdom in 2016, researchers similarly observed how many dissidents ultimately experienced "network erosion" with their family members due to the digital presence of pro-regime agents.[31]

[24] *Ibid* at 256.

[25] See also Emanuela Dalmasso, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohammad, and Dana Moss (2017), "Intervention: Extraterritorial Authoritarian Power," *Political Geography* 64 at 4 <https://doi.org/10.1016/j.polgeo.2017.07.003> [Dalmasso et al., "Intervention"].

[26] Dana M Moss (2020), "The Importance of Defending Diaspora Activism for Democracy and Human Rights," Freedom House <https://freedomhouse.org/report/special-report/2020/importance-defending-diaspora-activism-democracy-and-human-rights> [Moss, "Defending Diaspora Activism"].

[27] *Ibid*.

[28] Adamson and Tsourapas, "Coercion-by-Proxy."

[29] Schenkkan and Linzer, Freedom House Report at 37.

[30] Freedom House (2021), "Iran: Transnational Repression Case Study," Freedom House <https://freedomhouse.org/report/transnational-repression/iran>.

[31] Dana M Moss (2018), "The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and 'Voice' in the Syrian Diaspora," *Globalizations* 15(2) at 276 [Moss, "Ties That Bind"].

Section 2: An Introduction to Digital Transnational Repression

Key Features of Digital Transnational Repression

Digital technologies are integrated into existing patterns of transnational repression, enhancing the mechanisms available to authoritarian states to undertake extraterritorial repressive activities.[32] Countries as wide-ranging as Bahrain,[33] Myanmar,[34] China,[35]

See our animated video explaination of digital transnational repression.

[32] See Marcus Michaelsen (2020), "The Digital Transnational Repression Toolkit, and Its Silencing Effects," Freedom House <https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects> [Michaelsen, "Toolkit"]. See also Moss, "Ties That Bind" at 269.

[33] Ben Knight, "UK Malware Used Against Bahraini Activists," *DW* (9 May 2012) <https://www.dw.com/en/uk-malware-used-against-bahraini-activists/a-16219440>.

[34] Geff Green and Eleanor Grace Lockley (2014), "Surveillance Without Borders: The Case of Karen Refugees in Sheffield," in *Emerging Trends in ICT Security*, Ed. Babak Akhgar and Hamid R. Arabnia (2014: Elsevier) <https://doi.org/10.1016/B978-0-12-411474-6.00032-3> [Green and Lockley, "Karen Refugees"].

[35] See e.g. Al Jazeera (2018), "China: Spies, Lies and Blackmail: How China Controls Its Citizens Inside and Outside the Country Where No Criticism or Dissent is Allowed," *Al Jazeera* (5 April 2018) <https://www.aljazeera.com/program/101-east/2018/4/5/china-spies-lies-and-blackmail> [Al Jazeera, "China Spies"]; Yaqiu Wang (2019), "Why Some Chinese Immigrants Living in Canada Live in Silent Fear," *The Globe and Mail* (25 February 2019) <https://www.theglobeandmail.com/opinion/article-why-some-chinese-immigrants-living-in-canada-live-in-silent-fear/>; Paul Mozur and Nicole Perlroth (2020), "China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn," *The New York Times* (1 July 2020) <https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html>; David Gilbert (2020), "Chinese Police Are Making Threatening Video Calls to Dissidents Abroad," *Vice News* (14 July 2020) <https://www.vice.com/en_us/article/jgxdv7/chinese-police-are-video-calling-citizens-abroad-with-threats-not-to-criticize-beijing> [Gilbert, "Chinese Police"]; Bradley Jardine, Edward Lemon, and Natalie Hall (2021), "No Space Left to Run: China's Transnational Repression of Uyghurs," Uyghur Human Rights Project <https://uhrp.org/wp-content/uploads/2021/06/Transnational-Repression_FINAL_2021-06-24-2.pdf>.

Egypt,[36] Ethiopia,[37] Iran,[38] Kazakhstan,[39] Rwanda,[40] Saudi Arabia,[41] Syria,[42] and Vietnam[43]—to name a few—are reported to have used various digital technologies to repress their nationals who live outside their borders. The spread of digital transnational repression is facilitated by the following key features that are unique to this phenomenon:

- *Low risk and scalable*: While digital technologies require some financial or human investment by the government of origin, many forms of digital transnational repression can be relatively inexpensive (for example, social media harassment campaigns, the use of Skype video calls to engage in coercion-by-proxy, or online smear campaigns) and achieved at a wide scale with a significant audience.[44]

[36] Michaelsen, "Silencing Across Borders."

[37] Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert (2017), "Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," Citizen Lab <https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/>; Bill Marczak, John Scott-Railton, and Sarah McKune (2015), "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware," Citizen Lab <https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/>; Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton (2014), "Hacking Team and the Targeting of Ethiopian Journalists," Citizen Lab <https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/>.

[38] Michaelsen, "Silencing Across Borders"; Michaelsen, "Exit and Voice"; Michaelsen, "Far Away, So Close"; Raphael Satter and Christopher Bing (2020), "Exclusive: Iran-Linked Hackers Pose as Journalists in Email Scam," *Reuters* (5 February 2020) <https://www.reuters.com/article/us-iran-hackers-exclusive-idUSKBN1ZZ1MS>; John Scott-Railton, Bahr Abdul Razzak, Adam Hulcoop, Matt Brooks, and Katie Kleemola (2016), "Group5: Syria and the Iranian Connection," Citizen Lab <https://citizenlab.ca/2016/08/group5-syria/> [Scott-Railton et al., "Group5"]; John Scott-Railton and Katie Kleemola (2015), "London Calling: Two-Factor Authentication Phishing From Iran," Citizen Lab <https://citizenlab.ca/2015/08/iran_two_factor_phishing/>.

[39] Eva Galperin, Cooper Quintin, Morgan Marquis-Boire, and Claudio Guarnieri (2016), "I Got a Letter From the Government the Other Day: Unveiling Campaign of Intimidation, Kidnapping, and Malware in Kazakhstan," The Electronic Frontier Foundation <https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf>.

[40] *Ibid*.

[41] Lizzie Dearden (2019), "Human Rights Activist Launches Legal Claim Against Saudi Arabia for 'Hacking Phone' in UK," *The Independent UK* (29 May 2019) <https://www.independent.co.uk/news/uk/home-news/saudi-arabia-spying-phones-ghanem-dosari-uk-spyware-pegasus-a8935331.html>; Eli Lake (2019), "The Dark Side of Israel's Cold Peace With Saudi Arabia: The Saudis Are Using Israeli-Made Cyberweapons to Monitor and Intimidate Dissidents Abroad," *Bloomberg* (3 June 2019) <https://www.bloomberg.com/opinion/articles/2019-06-03/israel-s-cold-peace-with-saudi-arabia-has-a-dark-side> [Lake, "The Dark Side"]; Ayman M Mohyeldin (2019), "No One Is Safe: How Saudi Arabia Makes Dissidents Disappear," *Vanity Fair* (29 July 2019) <https://www.vanityfair.com/news/2019/07/how-saudi-arabia-makes-dissidents-disappear>; Bill Marczak, John Scott-Railton, and Ron Deibert (2018), "NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident," Citizen Lab, <https://citizenlab.ca/2018/07/nso-spyware-tar>; Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert (2018), "The Kingdom Came to Canada," Citizen Lab <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>.

[42] Daniel Regalado, Nart Villeneuve, and John Scott-Railton (2015), "Behind the Syrian Conflict's Digital Frontlines," Fire Eye <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf>.

[43] BR24 (2020), "Lined Up in the Sights of Vietnamese Hackers," *BR24* (7 October 2020) <https://web.br.de/interaktiv/ocean-lotus/en/>.

[44] Ronald J Deibert (2020), *Reset: Reclaiming the Internet for Civil Society* (2020: House of Anansi Press)

- *Hard to detect*: Intrusion attempts with digital technologies can be difficult for impacted individuals to detect.[45] People struggle to trace the origins of a smear campaign or to discover the real identity of those who write harassing or threatening messages on social media or other online platforms. The availability of zero-click exploits provides a mechanism for infecting someone's phone without leaving an obvious trace (such as a malicious text) or needing the target to take a specific action (such as clicking on a link).[46] It can be challenging for law enforcement or other relevant groups, who often lack necessary technical expertise, to identify such activity and attribute it to a specific actor.
- *Adaptable*: Digital transnational repression is characterized by the ease with which states that engage in such activities can rapidly change tactics and strategies when using digital technologies.[47] Further, digital transnational repression does not necessarily require the same resource expenditure as physical surveillance activities.[48]
- *More widespread chilling effect*: The mere existence of digital technologies, such as spyware and malware, and the possibility that a country of origin would use them against a target creates a sense of insecurity and has chilling effects on the social and political activities of those targeted. Essentially, "having one's private life exposed after a malware attack, or learning that a family member was threatened, can prompt a person to scale back or halt rights activism or other undesired behaviour immediately."[49]
- *Lack of accountability for state actors and other perpetrators*: As researchers observe, the "normative cost" of transnational repression may be "low" as such threats may not be perceived as "breaching the sovereignty of the host country."[50] This impunity is coupled with the reality that the "normative cost of using transnational repression has gone down, particularly due to the erosion of norms against states using extraterritorial violence in the absence of war."[51] Indeed, the international law framework for digital attacks that fall below the threshold of the use of force remains debated.[52]

at chap. 3; Erica Frantz, Andrea Kendall-Taylor, and Joseph Wright (2020), "Digital Repression in Autocracies" Varieties of Democracy Institute at 2 <https://www.v-dem.net/media/publications/digital-repression17mar.pdf> [Frantz et al., "Autocracies"].

[45] Moss, "Ties That Bind" at 278. See also Dalmasso et al., "Intervention" at 3; Schenkkan and Linzer, Freedom House Report at 4.

[46] See e.g. Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert (2021), "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild," Citizen Lab <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>.

[47] Moss, "Ties That Bind" at 278.

[48] Frantz et al., "Autocracies" at 2.

[49] Schenkkan and Linzer, Freedom House Report at 13.

[50] *Ibid*.

[51] *Ibid* at 7.

[52] See e.g. Chatham House (2019), "The Application of International Law to Cyber Attacks" Chatham

Impacts of Digital Transnational Repression

Self-Censorship and the Silencing of Transnational Networks

Digital transnational repression serves as a constraint on the ability of emigrants to engage in home-country politics both in person and online and has a "dampening" effect on the voice of the pro-revolution diaspora living abroad through self-censorship.[53] Digital technologies "increase the intensity, outreach, and immediacy of potential contacts and conflicts between the state actors and political exiles."[54] The mere possibility of being subject to digital surveillance by state or state-related actors and uncertainty around the scope and purpose of such surveillance activities pushes activists towards self-censorship.[55] Even where established dissidents in exile may not stop using digital technologies, digital "threats deter the wider diaspora who wish to avoid being caught in the blacklisting dragnet from expressing their views."[56] Self-censorship can also lead victims to avoid speaking to law enforcement about threats to personal safety.[57] Moreover, this silencing effect may serve to further cement the power of the ruling regime in the country of origin.[58]

Psychological Harm and Behaviour Modification

Victims of digital transnational repression have explained that this threat has generated concerns about their privacy[59] and feelings of insecurity,[60] guilt,[61] fear,[62] uncertainty,[63] mental and emotional distress,[64] and burnout.[65] An Ethiopian refugee in the UK, for

House <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/7-conclusions-and-recommendations>.

[53] Moss, "Case of the Arab Spring" at 486; Moss, "Ties That Bind" at 274–275.

[54] Michaelsen, "Exit and Voice" at 261.

[55] Michaelsen, "Toolkit"; Moss, "Defending Diaspora Activism."

[56] Dalmasso et al., "Intervention" at 4.

[57] Moss, "Defending Diaspora Activism."

[58] Frantz. et al., "Autocracies" at 13.

[59] Lake, "The Dark Side."

[60] Raphael Satter (2016), "Experts See Iranian Link in Attempt to Hack Syrian Dissident," *Associated Press* (2 August 2016) <https://www.apnews.com/6ab1ab75e89e480a9d12befd3fea4115>.

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

[62] Scott-Railton et al., "Group5"; Leigh Day, "Legal Case Launched Against Kingdom of Saudi Arabia for Alleged Use of Spyware to Target Dissident," *Leigh Day* (28 May 2019) <https://www.leighday.co.uk/News/2019/May-2019/%E2%80%8BLegal-case-launched-against-the-Kingdom-of-Saudi> [Leigh Day, "Legal Case"]; Al Jazeera, "China Spies."

[63] Danna Ingleton, "Amnesty International Affidavit in Support of Israeli Petition" *Amnesty International* (13 May 2019) <https://www.amnesty.org/en/documents/act10/0332/2019/en/>.

[64] *Ibid*.

[65] Michaelsen, "Toolkit."

instance, reported that the Ethiopian government's surveillance of his online activism through the use of FinFisher spyware "made him feel insecure and very uncomfortable, as if he was constantly being watched."[66] A Syrian activist in Canada (who was not a part of our study) described the feeling as "a surge of excitement and dread, not knowing what will follow, when a new [malicious] email pings its arrival."[67] Victims have also expressed concerns regarding the safety and security of their immediate and extended community, such as family members, friends, or other dissidents.[68]

Other victims report that digital transnational repression pushed them to adopt different patterns of behaviour, such as keeping a low profile online, posting pictures of specific locations only after leaving them, and asking that conference biographies be kept offline.[69] One article regarding a Burmese Karen refugee community in the UK described the profound impact that an intrusion incident had on its members, particularly in terms of community trust.[70] The incident also involved an online smear campaign, which community members saw as "part of the psychological and physical warfare that extended from the ethnic cleansing of Karen communities in Burma, now extended to a newer, 'virtual' location."[71] Similarly, for the Rwandan diaspora, the Rwandan regime's assassinations, physical harassment, and forcible renditions of nationals outside its borders have been combined with digital threats, such as the use of spyware and online harassment.[72] The consequence of these and other tactics is a community-wide lack of trust on two levels: both between individuals and towards diaspora organizations.[73]

[66] Privacy International (2014), "Surveillance Follows Ethiopian Political Refugee to the Uk," *Privacy International* (16 February 2014) <https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk>.

[67] Naheed Mustafa (2016), "Life in the Digital Life of the Syrian War," *Open Canada* (18 October 2016) <https://www.opencanada.org/features/life-digital-shadow-syrian-war/>.

[68] Ari Shapiro (2019), "Human Rights Activist Iyad El-Baghdadi Says U.S. Warned Of Saudi Arabia Threat," *NPR* (15 May 2019) <https://www.npr.org/2019/05/15/723686069/human-rights-activist-iyad-el-baghdadi-says-u-s-warned-of-saudi-arabia-threat?utm_source=dlvr.it&utm_medium=twitter>; Dalmasso et al., "Intervention" at 4; Andrea Peterson (2015), "Spyware Vendor May Have Helped Ethiopia Target Journalists—Even after It Was Aware of Abuses, Researchers Say," *Washington Post* (9 March 2015) <https://www.washingtonpost.com/news/the-switch/wp/2015/03/09/spyware-vendor-may-have-helped-ethiopia-spy-on-journalists-even-after-it-was-aware-of-abuses-researchers-say/?noredirect=on&utm_term=.e0d9e60ce12b>; Leigh Day, "Legal Case"; Michaelsen, "Exit and Voice" at 256–257.

[69] Michaelsen, "Exit and Voice" at 257–258 (see interviews on 26 August 2015 and 10 September 2015); Moss, "Ties That Bind" at 274.

[70] Green and Lockley, "Karen Refugees."

[71] *Ibid* at 525.

[72] Schenkkan and Linzer, Freedom House Report at 22.

[73] *Ibid* at 26.

Repression of Family Members and Friends in the Country of Origin

Digital technologies also facilitate coercion-by-proxy through the intimidation of family members who remain in the country of origin.[74] In particular, "the transnationalization of politics has been accompanied by the transnationalization of family ties, social relations, and social networks, which perversely has provided an additional source of leverage for states to engage in transnational repression."[75] In other words, digital surveillance provides a mechanism by which authoritarian states can identify relationships between family members and colleagues in the country of origin and dissidents and activists outside.[76]

An example of this coercion-by-proxy activity emerges from China, where a Chinese activist abroad reported that the Chinese government used Skype to call him while the authorities were in the same room as their family members back in China.[77] Similarly, in an attempt to have an Iranian engineer based in the United States spy for them, Iranian authorities in Tehran threatened the engineer's sister, who also received a summons for her brother to report to the Iranian courts for questioning.[78] Moreover, when an Iranian man who was living in Canada refused the Iranian Aircraft Accident Investigation Bureau's request to delete Instagram posts condemning the shooting down of Ukrainian International Airlines Flight 752, his family in Iran received a call from Iranian intelligence services.[79] Iranian authorities' questioning of family in Iran is also proving a popular mechanism to target Iranian journalists in exile. In a survey, 69 of 102 participants who were Iranian journalists living abroad reported that the Iranian government had questioned, harassed, or threatened one or more of their relatives in Iran.[80]

Another example relates to digital threats that Uyghurs living abroad faced when, using WeChat, their relatives were employed as proxies by the Chinese authorities.[81] Syrian dissidents living abroad have also reported that their families have been detained and tortured because of the dissident's activities outside the country.[82] Similarly, in the

[74] Adamson and Tsourapas, "Coercion-by-Proxy."

[75] *Ibid*.

[76] *Ibid*.

[77] Gilbert, "Chinese Police."

[78] Wallis Snowdon (2020), "Edmonton Software Engineer Says Iranian Regime Attempted to Make Him Their Spy," *CBC News* (27 August 2020) <https://www.cbc.ca/news/canada/edmonton/edmonton-software-engineer-arrest-iranian-regime-informant-1.5700744>.

[79] Steven Chase (2020), "Victims of Foreign-State-Sponsored Harassment in Canada Recount Threats of Rape, Murder and Harm to Families," *The Globe and Mail* (26 November 2020) <https://www.theglobeandmail.com/politics/article-victims-of-foreign-state-sponsored-harassment-in-canada-recount/>.

[80] Sirwan Kajjo, "Secondary Targets: When You Can't Punish a Journalist, Family Will Do Just Fine," *VOA News* [undated] <https://projects.voanews.com/press-freedom/secondary-targets/>.

[81] Schenkkan and Linzer, Freedom House Report at 18.

[82] Amnesty International (2011), "The Long Reach of the Mukhabarat: Violence and Harassment Against

Chechen Republic, the Russian government uses digital platforms to collect information on its critics and then arrests or tortures family members who remain in the country to silence dissent abroad.[83] One member of the Rwandan diaspora described their concern for their loved ones back home as "psychological torture."[84]

Syrians Abroad and Their Relatives Back Home," *Amnesty International* <https://www.amnesty.org/en/documents/MDE24/057/2011/en/>. See also Emma Lundgren Jorum (2015), "Repression Across Borders: Homeland Response to Anti-Regime Mobilization Among Syrians in Sweden," *Diaspora Studies* 8(2) <https://doi.org/10.1080/09739572.2015.1029711>.

[83] Schenkkan and Linzer, Freedom House report at 29.

[84] *Ibid* at 25.

Section 3: Digital Transnational Repression in Canada

Between 2020 and 2021, we conducted exploratory interviews to better understand how digital transnational repression impacts activists and dissidents living in Canada, which is generally not studied enough. We interviewed 18 individuals, all of whom resided in Canada and had moved or fled to Canada from another country (their country of origin), and self-reported being or having been politically or socially engaged in relation to their country of origin.

Six participants self-identified as female, 11 self-identified as male, and one participant did not provide their gender. Participants self-identified as coming from a range of geographical regions and countries, including Syria, Saudi Arabia, Yemen, Tibet, Hong Kong, China, Rwanda, Iran, Afghanistan, East Turkestan, and Balochistan.[85] The average age of participants was 37 years old.[86] All participants were college- or university-educated or were enrolled in a college or university study program. Participants who were not students reported working in areas that included journalism, the private and non-profit sectors, and the civil society sector. Participants left their countries of origin for various reasons, including family reasons (for example, leaving as a young child), the inability to make a life in their country of origin, and/or flight from persecution. In most cases, the participants' departure (or that of their family if they left as a young child) was linked to persecution or fear of persecution by authorities in their countries of origin.

Interviews explored a range of issues, such as the participants' activism in their country of origin and in Canada, their use of digital technologies in both locations, their feelings about whether they had been digitally targeted in Canada or before arriving in Canada, and how this targeting impacted them. Transnational digital repression tactics against participants ranged broadly but included hacking and phishing, account takeovers, troll and bot campaigns on social media, online threats, and disinformation campaigns. Participants stated that they adopted some digital practices in an attempt to protect themselves.[87]

[85] We have referred to the participants' country of origin based on what they self-reported this to be. For example, a participant who has self-reported as being from Balochistan will be described as a "participant from Balochistan" even though the region of Balochistan is not internationally recognized as its own country and is considered part of Pakistan. In some cases, we have omitted the participant's country of origin to protect their identity.

[86] One participant did not want to provide their age and has been omitted from this number.

[87] Such digital security practices included using separate personal and work email accounts, using several devices and phone numbers, using encrypted platforms and VPNs, employing code language when communicating online, not opening links in direct messages, regularly changing passwords and activating 2FA, turning off location-tracking in applications, and deleting applications that they believed their country of origin could potentially use against them.

In the following sections, we describe the experiences of those targeted with digital transnational repression in more detail. Participants described important mental, social, and physical impacts, such as feeling paranoid and anxious, being more cautious and self-isolating, having their professional and student life negatively affected, feeling responsible for the safety of others, and limiting communications with friends and family in Canada and the country of origin. They also drew links between their digital and physical security, and they highlighted the lack of resources that were available to them to respond to digital transnational repression. These findings build on prior research that underscores the serious psychosocial impacts of digital transnational repression and how it leads to self-censorship and the erosion of community networks. While we did not conduct a technical examination of the digital threats described by participants, participants linked these digital activities to their country of origin and presumed that they were related to their work in political or social activism.

The Impact of Digital Transnational Repression on Psychosocial Health

Participants corroborated existing research that digital transnational repression impacts their psychosocial health, including their mental health. For example, a Saudi activist explained that being digitally targeted was a form of "psychological and emotional war" and described themselves as experiencing "endless fear and anxiety" about being digitally targeted.

Similar observations were made by other study participants. A Tibetan human rights activist had their Instagram account used as a platform to harass and bully them and received phishing emails and violent threats through direct messages on Facebook and Instagram. They explained that they experienced physical burnout and that balancing their regular life with an influx of digital threats was "mentally [...] excruciating," and they became prone to mental illness and found the experience traumatic. Female participants reported receiving online rape threats as well as other misogynist threats, and they were left with a deep sense of digital and physical insecurity.

Yemeni participants—one of whom worked in journalism (identified as Ahmad later in this report) and another in human rights advocacy—suffered repeated successful and failed intrusion attempts on their social media and email accounts and online smear campaigns. They observed that the potential of digital threats made them feel "paranoid all the time" and "emotionally numb." A Syrian political activist explained that the digital targeting—which included repeated page takedowns by Facebook and the hacking of their social media and email accounts—negatively impacted their physical and mental health, and they developed "severe anxiety."

Another Syrian political activist whose social media accounts were also hacked noted that being digitally targeted had "psychological effects" that caused them "permanent paranoia and constant anxiety." This state affected their "emotional relationships" and "created a state of psychological instability." A social and political activist from Afghanistan explained that they felt a deep level of insecurity after their SIM was purportedly taken over and worried that they might be physically attacked in Canada.

In some cases, participants expressly stated that despite any negative impacts they experienced, digital targeting did not stop them from engaging in advocacy. For example, a Tibetan human rights activist reiterated that even though the digital targeting had impacted how they engaged in advocacy work related to Tibet, this experience was not going to stop their advocacy work. A Syrian participant who had quit engaging in political activism once in Canada still noted that the digital targeting they experienced (which had occurred primarily when they were in Syria) actually made them "fiercer."

Ali: A Human Rights Activist from Saudi Arabia[88]

Ali moved to Canada from Saudi Arabia to study in 2017. Before moving to Canada, Ali did not consider himself an activist, although some family members were engaged in such work in Saudi Arabia. After arriving in Canada, Ali's sibling was detained in Saudi Arabia, and Ali began to advocate from Canada for their release. Technology has been a crucial tool in Ali's work, enabling him to connect with people and family in Saudi Arabia and elsewhere. At the same time, Ali recognizes that authoritarian regimes have the resources to circumvent digital security measures like encryption in order to target activists and dissidents.

Ali has personally experienced digital targeting in reaction to his advocacy work. For example, he was repeatedly targeted by what he believes to be Saudi state-backed trolls on Twitter. When Ali posted something activism-related on Twitter that received a lot of positive attention, he was "just shower[ed] [...] with insults." When he first experienced these trolls, Ali explained: "I was shocked and I couldn't think properly, I couldn't sleep properly, I couldn't eat properly, I couldn't make decisions properly." Ali was also targeted through phishing attempts and online slander campaigns, and he received suspicious text messages. After reading that Saudi Arabia was targeting activists with NSO Group's Pegasus spyware, Ali suspected that his devices might be targeted with the same spyware.

[88] The participant has been assigned a pseudonym to protect their identity.

This digital targeting has impacted Ali's physical and mental health and his online and in-person social life. For example, he now engages in self-censorship and limits the personal information he shares on social media. Ali has "started to think about everything" he could say a "million times" and explains that he is "being more careful" in what words he uses. Ali also limits his online communications with people in Saudi Arabia to protect those individuals and his social engagements with the Saudi community in Canada.

Li: A Pro-democracy Activist from Hong Kong[89]

Li was raised in Hong Kong and moved to Canada as a teenager. Li's childhood participation in large protests in Hong Kong taught her that people can create change; however, she also learned that some subjects are taboo and those who are too outspoken can be labelled as troublemakers. In Canada, Li works with an organization that does Hong Kong-related advocacy work. Technology is a key part of this work, whether it is promoting the cause on social media or using digital tools to organize. But this technology comes with risks. Members of Li's network who are based in Hong Kong have been arrested and have had their phones confiscated and used to access private group chats. Their group has had their pro-democracy social media posts taken down after coordinated efforts by authorities to mass report their posts to the social media company.

After engaging in media interviews, Li faced waves of coordinated misogynistic messages and death threats. Li explained that when she posted on social media, she received a "wave of bot accounts" attacking her with "insults mixed with death threats and rape threats." The rape threats were "very descriptive" and "founded on misogyny." In advance of an advocacy-related trip, Li received threatening messages that identified the number of the hotel room she planned to stay in. She also regularly receives suspicious emails and text messages that discuss her advocacy work and encourage her to click on a link. Li's organization's website has faced DDoS attacks timed to its release of new reports. Li has been photographed at protests and has had those photos distributed alongside her name, email address, and phone number in WeChat groups.

Li explained that her physical health has been affected by these threats, and she is in "constant pain." Li recounted:

> “
>
> It puts a mental strain on you and it feels very isolating in many ways because [...] who do you talk to about this stuff? You can't change anything because nothing I do would be able to change how my family could be treated in Hong Kong. It's just so crushing in so many ways: it does not stop me from doing the work I do, I get called brave all the time, but it's not bravery, it's stupidity, really, putting myself at risk and

[89] The participant has been assigned a pseudonym to protect their identity.

> I fully acknowledge that and grappl[e] with how I could keep myself and my family and my loved ones safe and continu[e] the work that I do and I have no answers yet.

Although Li is in Canada, her digital life is highly intertwined with activists and family members based in Hong Kong and China. She fears that if her online accounts are compromised, the safety of these people could be put at risk. This fear leads her to self-censor her online activity. As Li explained:

> [I am] self-censoring in a sense where I'm telling my friends not to do something as basic as mention me publicly on their social media accounts. [...] Posting a photo of your lunch seems perfectly normal in Canadian standard, but if I post a picture of my lunch my thought goes to okay [...] where I have lunch, now they know where I am. It changes such little, and such big, aspects of my life. [...] I am keeping a distance from my friends, so they could be safe, to the point that I can't post a picture of my lunch and tag where I had lunch.

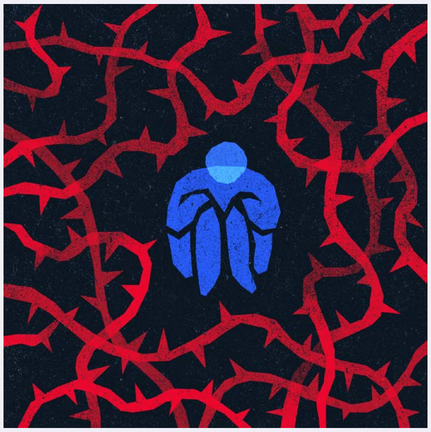
Li feels like it is not just a few people who are digitally targeting her; it is a global superpower. Li knows this reality is true for many dissidents who have fled to Canada and wishes the government would do more to acknowledge it. She has reported her experiences of being harassed to the police in Canada, but the police have said there is nothing they can do. Li also thinks that social media companies need to do more to protect their users and the data that users have entrusted to them.

Digital Transnational Repression and Self-Censorship

Participants adopted practices of self-censorship, such as using extra caution in online posts, in the face of digital transnational repression. A political and human rights activist from Balochistan noted that they were "very careful and afraid of doing things that might be leaked or monitored or used against [them]." A Yemeni journalist (identified as Ahmad later in this report) explained that repeated targeting affected him on a "personal level," so he refrained from political expression unless "necessary" on Facebook.

A Syrian activist described that they felt unsafe and did not want to publish personal information online. They expressed that they could not "speak openly," "connect with people openly," or "post whatever" they felt like online. For another Syrian participant, the fear of digital targeting led them to withhold information from family in Syria. For example, they did not feel comfortable telling their parents that they had resettled in Canada as a refugee.

Arash: An Activist from Iran[90]



Arash's early childhood memories of Iran are dominated by fear and political repression. In 1990, Arash's family fled Iran and came to Canada to find a safe home. Despite growing up in Canada, this social and political activist works closely with communities in Iran, advocating for democracy, and he has been the subject of various online threats, such as attempts to compromise his email accounts, online impersonation attempts, and phishing attacks. Arash has also been subject to offline threats. For example, an Iranian pro-regime group reached out to Arash's employer in Canada to try and get him dismissed from his job. Arash expressed being deeply concerned about the security and privacy of his personal information and his physical safety. Arash is also concerned with the safety of friends and family because the threats affect anyone he is in contact with in Canada or Iran.

Arash feels that the situation impacts his mental health. He "constantly worr[ies]" about being digitally targeted and characterizes the experience as "deeply threatening." Arash explains that "psychologically, it has an impact on you, [you] worry about your employment, worry about your safety, your security, and so on." Arash is increasingly concerned about his online posts and communications with individuals living in Iran. This concern has led Arash to engage in self-censorship, such as limiting political conversations with family and assuming that anyone who reaches out to him is affiliated with the regime. Arash is also wary about socializing with other Iranians in Canada.

In addition to these concerns, Arish worries about the potential of being kidnapped by the Iranian regime and does not feel like he can travel freely. Arash reported some of the threats he faced to the police and the Canadian Security Intelligence Service (CSIS); however, no action was taken by these bodies.

Digital Transnational Repression and the Erosion of Community Networks

Participants expressed that digital transnational repression impacted how they socialized and interacted with others, both within Canada and abroad. Participants explained that they restricted digital communications with people in their country of origin, and they avoided socializing with others from the same country of origin. Participants noted that their concern in communicating with people back home was related to the potential harm that those people might suffer if their communications were intercepted by authorities in their country of origin.

[90] The participant has been assigned a pseudonym in order to protect their identity.

For example, a Syrian business owner and political activist (identified as Amir later in this report) noted that after being the target of a digital attack he started “choosing friends wisely.” A Tibetan human rights activist similarly recounted that the stress of dealing with digital targeting in Canada, among other factors, led them to cut personal ties with friends and family, in part for safety reasons. They explained that they felt guilty and responsible for the safety of persons who might be punished for being linked to them. They also noted that other individuals on their campus in Canada were scared of speaking with them in public because they were concerned that they would not be able to go back home or their parents might get in trouble.

A Syrian participant noted that their family life and relationships with friends were “very heavily” impacted by their activism and that the experience of being digitally targeted meant that they had “to be very careful” with who they befriended on social media. Another Syrian political and social activist explained that they felt “afraid of communicating” with other Syrians and that they were still afraid of “espionage, assassination attempts, or revenge” on their family. They noted that digital targeting “greatly affected” their social involvement with the Syrian community because they felt “afraid of them” and “did not feel comfortable communicating with them.” Their fear of being hacked led them to cut off direct contact with relatives and friends, and they “became very introverted,” “concerned about people,” and had “constant doubts about people and exaggerated questions about their intentions to communicate and their motives.”

Another Syrian activist noted that they made a conscious decision to stay away from the Syrian community when they arrived in Canada. Their concerns regarding online discourse on Facebook and other social media led them to be “more careful” whenever they engaged with anyone they did not really know and in relation to Syrian issues. A social and political activist from Afghanistan explained that the experience of being digitally targeted made it difficult for them to “trust people”; they became “suspicious” of people from their country of origin, and they restricted communications with others.

A social and political activist from East Turkestan[91] explained that it was very difficult to communicate with individuals in their country of origin because the authorities monitor communications on such platforms as WeChat and other applications. Thus, they did not communicate with friends and family back home. They also noted that part of their concern regarding digital attacks and surveillance was related to the fact that other people in their country of origin might face serious consequences such as death or torture. A Chinese pro-democracy activist explained that they “lost contact” with most of their friends and relatives because they “don’t want to get [them in] trouble.”

[91] East Turkestan is also known as the Xinjiang Uyghur Autonomous Region of China.

A Saudi activist explained that their key concern was the safety of others, saying "if my phone gets hacked, all these persons will be exposed to serious problems just because my mobile is hacked. The danger is not only to the person who has been targeted, but also to everyone who communicates with this person." Similarly, an Iranian participant (previously identified as Arash) noted that one of his concerns with a lack of digital security was the safety of others. An activist from Balochistan noted that they were not worried about being tracked or monitored by the Pakistani government while in Canada, but they were "worried about people back home" when they contacted them. They noted that, while they came to Canada to have a free space to advocate for their people, they could not safely communicate with people back home.

Ahmad: A Journalist from Yemen[92]

Ahmad was born and raised in Yemen and fled to Canada in 2014. Before leaving Yemen, Ahmad worked as a journalist and played a crucial role in the 2011 uprising and during the transitional period. Ahmad fled to Canada as it was no longer safe for journalists to stay in Yemen after Houthi militias took over Sana'a and a Saudi-led coalition subsequently intervened in the country. In Yemen, journalists were subjected to various forms of violence due to their work.

Despite this situation, Ahmad was not dissuaded from doing these journalistic activities from Canada and continued to receive numerous online and offline threats. Numerous unauthorized attempts to access Ahmad's email and social media accounts have been made, and he was targeted on WhatsApp with a suspicious message. He explained that the digital targeting he experienced means that "you [are] always thinking about what is going to happen next, what kinds of pictures you are taking, what kind of information you are keeping in your phone." Further, he noted that he does not "trust anyone anymore online" and that:

> I used to be very open, very active, but now [...] I limit [my] social life [...] even not only online [...] I mean in real life. [I am] usually very suspicious of what [...] people [I am] meeting, especially if they have [a] certain background that could somehow put you [in] a difficult position politically with them or you expect that they might not be or they are not in the same way of thinking politically as you do.

The digital targeting has led Ahmad to engage in self-censorship on social media, where he is cautious about every word he writes. Ahmad observes that:

[92] The participant has been assigned a pseudonym to protect their identity.

> “You are very careful, more careful than what you used to be [...] [You] don’t usually write everything you want to post or you want to; all your thoughts are not written or posted whenever you want anymore. You are more careful, [...] you calculate things differently—what’s going to happen, are you going to piss somebody [off] personally or are you going to affect your family, affect your friends, affect your opportunity.

Despite being in Canada, Ahmad is still concerned for his family and colleagues’ safety in Yemen due to his work. In particular, he is concerned that the information of people he is in contact with in Yemen will be exposed and used to harm them or to blackmail him. This fear is particularly acute because Houthi militias arrested some of the journalist’s family members to pressure him and forced his family to disavow him in a statement. Ahmad remains worried, stressed, and fearful in Canada. Ahmad’s work and studies in Canada have suffered, and his social life has been impacted both online and offline as it is very difficult for him to trust anyone.

The Relationship between Digital Transnational Repression and Physical Security

Participants noted that in addition to digital targeting they were subjected to other means of transnational repression, such as physical threats. Thus, participants’ departure from their country of origin did not necessarily resolve their concerns regarding their physical safety, and participants continued to feel unsafe in Canada.

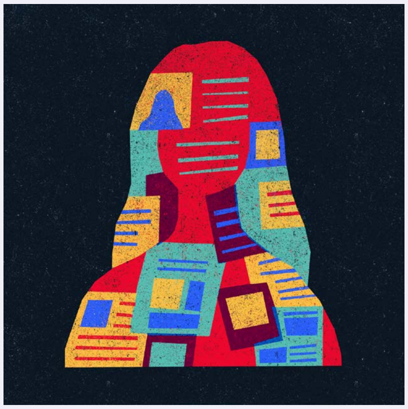
For example, a Saudi activist (previously identified as Ali) explained that he was approached by individuals in Canada who attempted to lure him back to his country of origin. A Syrian activist recounted that they were threatened by individuals in Canada not to participate in political activities. A Yemeni journalist (previously identified as Ahmad) noted with relief that he felt safe enough to go for coffee in Canada, but he then explained that his family members were arrested because of his activities and that they still get threats if he posts on Facebook, which highlights how the physical safety of family members in the country of origin may continue to be at risk even when an activist has left the country of origin.

A social and political activist from East Turkestan explained that, during a presentation at a university, someone who appeared to be a university student attempted to disrupt the participant’s presentation. The participant believed that the student may have been acting on the direction of individuals at the Chinese consulate in Canada. The participant also recounted that they received repeated phone calls telling them to come to the consulate of their country of origin in Canada to pick up a document.

An activist from Balochistan noted that they did not feel physically safe in Canada and were advised by police and CSIS to take certain precautionary measures. A pro-democracy activist from Hong Kong (previously identified as Li) recounted that, two days after a report came out regarding the harassment of anti-CCP activists in Canada, she was chased on the street to her apartment building. She also recounted that, while at a protest, she was approached by someone who got up in her face and said that they were going to kill her.

A Rwandan social and political activist noted that several of their friends were assassinated in exile or had been subject to assassination attempts. The participant recounted how the government of their country of origin had nearly kidnapped them from Kenya, but they escaped. To deter future attempts while they were working in Kenya, they had to take a series of precautions. An Iranian activist (previously identified as Arash) also noted that he had taken certain measures to protect his physical safety, such as changing his "patterns of movement," not announcing his travel plans, and not travelling to countries where Iran has a strong presence.

Liu: A Pro-democracy Activist from China[93]



Liu was born in China and fled to Canada in 1989 due to political repression. While she is no longer living in China, she continues her pro-democracy work from Canada. Liu writes and organizes activities around the struggle for democracy in China and challenges the Chinese Communist Party (CCP)'s attempts to manipulate the overseas narrative about China.

Due to this work, Liu has been subjected to numerous forms of offline and online threats—she has had her devices compromised, been targeted with socially engineered phishing attempts, and been the subject of unauthorized attempts to access her email and social media accounts. The activist was also subjected to gender-based threats online. For example, in 2013, while preparing for an international conference in Toronto, Liu discovered that conference attendees received fabricated nude photos of her. Further, Liu was subjected to doxxing and her personal information was posted in online ads soliciting sex services.

For offline threats, Liu believes that the Chinese government attempted to stop the publication of her book as she received threatening calls asking her to stop publication. Liu was also targeted with offline disinformation campaigns. For example, an individual distributed printed fliers with defamatory content about Liu to members of Parliament in Ottawa and pasted Liu's photo on lampposts in the city. On one occasion, Liu was invited to speak about the Tiananmen

[93] The participant has been assigned a pseudonym to protect their identity.

Square Massacre and a person approached her and handed over legal documents informing her that she had been sued for 10 million Canadian dollars.

Liu observes that while she felt safe when she first arrived in Canada, which was shortly after the Tiananmen Square Massacre, this feeling has since dissipated. While she feels like she has escaped repression in China, she also feels in constant danger in Canada. For example, Liu described herself as "really scared" and explains that "sometimes I laugh at myself, I escaped from China, from the killing, from the persecution [...] from the horrible danger, to Canada and the danger is getting more and more. The pressure is getting more and more here."

This fear of digital and physical targeting has impacted many aspects of Liu's life, such as her social life. Other members of the Chinese diaspora in Canada who fear the CCP try to stay away from Liu, both online and offline. Liu reported various offline and online threats that she experienced to the police, but the police said there was nothing they could do. In the face of such repression, Liu is concerned not only about her own safety, but that of all dissidents in Canada.

The Availability of Resources to Address Digital Transnational Repression

Participants noted a lack of formal resources from non-governmental organizations and the private sector for addressing digital targeting. For example, one Syrian activist explained that they were able to respond to hacking attempts by relying on a friend, a digital security expert, who could then reopen their account. However, they then observed that "[o]ther than that, I have nothing."

One participant (subsequently identified as Amir) coordinated with established organizations in civil society and in the private sector to address digital threats against Syrian activists and presented at an industry-led conference. This same participant observed that the Canadian government did not provide a course or seminar to raise awareness regarding digital security risks for small businesses. An Iranian activist (previously identified as Arash) spoke with his employer and asked for his devices to be checked. One Tibetan human rights activist spoke to the Canadian and Tibetan media about the digital targeting they were suffering. However, they noted that it was a "challenge" to receive appropriate "emotional support and personal support."

A Syrian activist attempted to speak directly with Facebook regarding their community pages being shut down on the social media site. They also attempted to speak to the US Department of State regarding the issue. However, neither intervention yielded any results. Participants reached out to external organizations with experience in digital security, but these outreach attempts were not always successful.

Law Enforcement and Intelligence Services' Response to Digital Transnational Repression

Participants reached out to Canadian law enforcement bodies or the Canadian Security Intelligence Agency (CSIS) for assistance and had mixed reactions to these interactions.[94] Participants appeared frustrated with the lack of governmental assistance and felt like they were forced to deal with digital transnational repression alone. They sometimes decided not to approach law enforcement because they thought doing so might make the situation worse, or they assumed law enforcement would simply be ineffective.

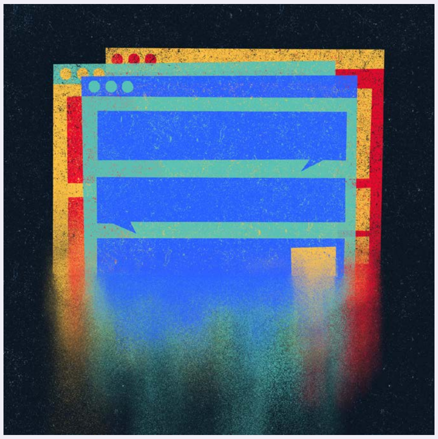
For example, a Yemeni activist reported the swapping of their Canadian SIM card and the hacking of their bank account to the police, but they never received a reply. One participant from Hong Kong (previously identified as Li) raised the issue of digital transnational repression with high-level officials in the Canadian government, but she felt that there was no recognition or support for Canadians who faced such concerns.

An activist from Balochistan spoke to both the police and CSIS but was left with the feeling that they had to address the issue alone. An activist from East Turkestan told the police that they were being harassed through repeated phone calls, but the police said they could not do anything because the calls were from an international number. Further, in response to the participant's concerns regarding digital security issues on their advocacy blog, the police said the participant could hire a private detective.

Participants simply avoided dealing with the police, fearing that it might make the situation worse or that they could not be of assistance. For example, after his business was the subject of extensive DDoS attacks, a Syrian business owner and activist (identified as Amir, below) stated that he did not reach out to the police because he assumed that the police would not be able to assist. A social and political activist from Afghanistan explained that they did not approach the police after being digitally targeted because they did not trust Canadian authorities. A pro-democracy activist from Hong Kong (previously identified as Li) said that she avoided approaching the police because it would have been "useless."

[94] The participant has been assigned a pseudonym to protect their identity.

Amir: An Activist from Syria[95]



Amir was born in Syria and associates his early childhood in the country with fear and political repression. Amir's family moved to Canada in 1992 and has remained there since. They became involved in political advocacy in relation to Syria after the 2011 Syrian uprising.

Since then, Amir has been subjected to multiple means of digital threats. For example, in 2011, Amir started supporting and hosting media websites that promoted democracy in Syria. In 2012, his personal Gmail account was taken over. In mid-2013, his Canadian web-hosting business experienced extensive DDoS attacks from Russia. One of these attacks affected the company's entire data centre. That attack caused severe damage to his business and had a significant financial impact. These attacks have affected Amir on a professional, financial, and social level. Amir explained that he "started to be more careful" and select friends "more carefully." He did not want to interact with "anyone with ties to the dictatorship" or to inform anyone of what he was doing. He wanted to avoid being intimidated or have a business relationship with anyone linked to the Syrian regime. He also noted that after being the target of a digital attack, he started "choosing friends wisely, even choosing who to do business with wisely" and that he does not want to "support someone [or] give business to someone who supports the dictator [...] [because] basically, I'd be giving the price of the bullets to the dictator indirectly to kill people."

Amir is concerned with family members' and fellow activists' online security. Many of them have been subjected to various attempts to take over their accounts and leak documents, and Amir feels responsible for their digital security. Amir reported the DDoS attack on his business to the Canadian Security Intelligence Service (CSIS). However, Amir observed that CSIS was primarily concerned with understanding whether there were members of the Syrian community in Canada with ties to terrorist groups. Amir believes that the Canadian government needs to do more to protect and support dissidents and activists in Canada who face the same challenges as he does.

[95] The participant has been assigned a pseudonym to protect their identity.

Section 4: Policy Recommendations to the Canadian Government for Addressing Digital Transnational Repression in Canada

The interviews detailed in Section 3 show the serious impact that digital transnational repression has on Canadian communities. While the Canadian government has begun to address the threat of "foreign interference" in Canada, a term broad enough to capture digital transnational repression, the response has reflected a dominant concern for threats related to Canadian democratic institutions, economic interests, and critical infrastructure.[96] Our review of existing government reports and statements suggests there has been limited effort to understand and document impacts of foreign interference on activists and dissidents who moved or fled to Canada. A focus on the specific concept of digital transnational repression (as well as transnational repression more broadly) could bring into greater focus the profound impacts that such authoritarian activities are having on the rights and freedoms of these communities. With these impacts in mind, we make the following initial recommendations to the Canadian government, which complement recommendations made by other organizations in Canada.[97]

[96] For example, the *Canadian Security Intelligence Service Act* defines foreign influenced activities (considered to be "another term for foreign interference" by CSIS) as "activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person." This definition of "foreign interference" is broad enough to capture activities that take place under digital transnational repression as defined at the outset of this report since such activities threaten Canadian values and interests such as human rights. See Canadian Security Intelligence Service (2021), "Foreign Interference Threats to Canada's Democratic Process" <https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html#toc2>; Public Safety Canada (2020), "Foreign Interference" <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210325/027/index-en.aspx?wbdisable=true>; Public Safety Canada (2021), "Foreign Interference" <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210722/015/index-en.aspx>; Public Safety Canada (2020), "Response to the December 18, 2021 Motion on Foreign Interference" <https://www.passengerprotect-protectiondespassagers.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/27-en.aspx>; Canadian Security Intelligence Service (2020), "Espionage and Foreign Interference" <https://www.canada.ca/en/security-intelligence-service/corporate/espionage-and-foreign-interference.html>.

[97] In particular, see recommendations by Alliance Canada HK (2021), "In Plain Sight. Beijing's Unrestricted Network of Foreign Influence in Canada," Alliance Canada HK <https://alliancecanadahk.com/wp-content/uploads/2021/05/ACHK_InPlainSight.pdf> [Alliance Canada HK, "In Plain Sight"]; Canadian Coalition on Human Rights in China and Amnesty International Canada (2020), "Harassment & Intimidation of Individuals in Canada Working on China-Related Human Rights Concerns," Canadian Coalition on Human Rights in China & Amnesty International <https://www.amnesty.ca/sites/default/files/Canadian%20Coalition%20on%20Human%20Rights%20in%20China%20-%20Harassment%20Report%20Update%20-%20Final%20Version.pdf> [Canadian Coalition on Human Rights in China, "Harassment & Intimidation"]. For a list of detailed policy recommendations in the US context

Hold the Perpetrators of Digital Transnational Repression to Account

- *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.*[98] The Canadian government needs to emphasize the importance of protecting the rights and freedoms of activist and dissident communities in Canada and understand that this problem is not confined to, for example, threats to business or Canada's economic interests.[99] For example, the United States Department of Commerce recently expressly noted the role of companies in facilitating transnational repression when it added a notorious spyware vendor, NSO Group, to the Department's Entity List and restricted US exports to that company.[100] This type of government activity sends an important message to the market that the sale of surveillance technologies to authoritarian regimes will not be tolerated.
- *Examine the possible use of targeted sanctions against foreign states, individuals, and entities that are responsible for, or complicit in, violations of international human rights law.* This recommendation has also been made in the context of addressing transnational repression in the United States.[101]
- *Review foreign state immunity law in Canada and implement the changes necessary to ensure that individuals subjected to digital transnational repression by foreign state actors are able to pursue a legal remedy in Canada.* For example, in the United States context, foreign state immunity is a potential obstacle when a victim seeks to sue a foreign state actor for acts of digital transnational repression.[102]
- *Examine how existing Canadian criminal law could be used to pursue the perpetrators and facilitators of digital transnational repression in Canada and educate the public and law enforcement on these provisions in the context of digital transnational repression.*[103] Further, consider whether a new crime specific to acts of transnational

regarding how the US should address transnational repression, see Schenkkan and Linzer, Freedom House Report.

[98] See Alliance Canada HK, "In Plain Sight" at 12.

[99] See also Canadian Coalition on Human Rights in China, "Harassment & Intimidation" at 51.

[100] United States Department of Commerce (2021), "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," *US Department of Commerce* (3 November 2021) <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>.

[101] Schenkkan and Linzer, Freedom House Report at 55.

[102] Harvard Law Review (2018), "Doe v. Federal Democratic Republic of Ethiopia," *Harvard Law Review* 131 at 1179–1186 <https://harvardlawreview.org/2018/02/doe-v-federal-democratic-republic-of-ethiopia/>.

[103] Digital transnational repression (and transnational repression) may fall within the scope of general

repression might be appropriate. For example, in some jurisdictions, a specific crime of "refugee espionage" has been enacted to address the surveillance and harassment of refugee communities.[104] Additionally, the Canadian government should investigate the possibility of criminal prosecutions that may help to limit the export or abuse of surveillance technologies by other states.[105]

- *Ensure greater transparency in Canada's dual-use export rules by publishing detailed information such as the names of exporting companies, the types of technology being exported, the destination of exported technology, and reasons for decisions to approve (or deny) export permits.* The European Union recently increased transparency requirements on EU states in the context of dual-use exports.[106] Doing so enables ongoing monitoring by civil society of the surveillance capacity of countries of export and the proliferation of dual-use surveillance technologies globally.
- *Strengthen and expand existing export rules by ensuring that new surveillance technologies are subject to dual-use controls, that there is a robust assessment of the human rights impacts of potential dual-use exports, that companies have to comply with due diligence requirements before export, and that export rules are robustly implemented.* Mandating a human rights assessment before granting export licences may reduce the surveillance technologies that are available to authoritarian regimes. The European

criminal law provisions such as national computer crime laws, although there are few examples of states undertaking such prosecutions specifically in relation to digital transnational repression. See Ron Deibert and Sarah McKune (2017), "Who's Watching Little Brother?: A Checklist for Accountability in the Industry Behind Government Hacking," Citizen Lab at 10–13 <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf>. As the authors note: "[l]acking, however, are coordinated campaigns against malicious actors specifically targeting civil society. Indeed, the frequent extraterritorial application of spyware technology against diaspora groups and other 'hostile' civil society actors beyond the physical reach of the state—some of which even incorporate ICT infrastructure in the jurisdiction of the target—raises serious questions about the resolve of governments to protect citizens from foreign espionage and information operations, and what sovereignty means in such a context."

[104] UN High Commissioner for Refugees (2014), "Comments from the UNHCR on the Memorandum of 6 December 2013, Proposing Criminalization of Refugee Espionage" <https://www.refworld.org/country,,UNHCR,,FIN,,5829ad6c4,0.html>; Säkerhetspolisen (2017), "Man gripen för flyktingspionage," Säkerhetspolisen (27 February 2017) <https://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2017-02-27-man-gripen-for-flyktingspionage.html>. See also Swedish Security Service (2019), "Individual Charged on Suspicion of Refugee Espionage," *Swedish Security Service* (6 October 2019) <https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2019-11-06-individual-charged-on-suspicion-of-refugee-espionage.html>; However, the use of criminal law to pursue individuals who undertake surveillance against refugee communities needs to be done with extreme caution so it does not become a mechanism by which to deport refugee claimants.

[105] For example, the United States Department of Justice has also pursued American ex-intelligence officials for facilitating the digital espionage capabilities of foreign states and noted that the prosecution was intended to dissuade the use of "hackers-for-hire." See United States Department of Justice(2021), "Three Former US Intelligence Community and Military Personnel Agree to Pay More than 1.68 Million to Reserve Criminal Charges Arising from their Provision of Hacking-Related Services to a Foreign Government" *United States Department of Justice* (14 September 2021) <https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million>.

[106] Beatrix Immenkamp (2021), "Review of Dual-Use Export Controls. European Parliamentary Research Service," European Parliament at 3 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf>.

Union has taken steps towards ensuring such a strengthened and expanded export review system.[107]

- *Ensure that the use of any surveillance technologies by Canadian intelligence and law enforcement bodies in Canada complies with the Canadian Charter of Rights and Freedoms and international human rights law.* Ensure that procurement of such technology is transparent and subject to public consultation and that government agencies and institutions do not import or use surveillance technology from companies associated with human rights abuses. In leading by example, the Canadian government—as well as other democratic states—have an opportunity to begin to articulate clear norms regarding when and how surveillance technology is going to be used by state actors, which detracts from authoritarian states' ability to argue that such technologies can be used by any state in any manner.

Support the Victims of Digital Transnational Repression

- *Create a dedicated government agency that is independent from CBSA, CSIS, or law enforcement to provide support for victims of transnational repression and to conduct research to better understand the scale and impact of these activities on the exercise of human rights in Canada.*[108] Ensure that government institutions coordinate how they address transnational repression and focus on the protection of the rights and freedoms of communities in Canada. These reforms could help address concerns raised in the National Security and Intelligence Committee of Parliamentarians' 2019 report, which highlights that security and intelligence organizations do not share a common understanding of the threat, including its gravity and most common manifestations.[109] As a result, Canada has been slow to react.[110] Further, the report notes that government responses have been "piecemeal, responding to specific instances of foreign interference but leaving unaddressed the many other areas where Canadian

[107] *Ibid*. On due diligence rules, see Siena Anstis and RJ Reid (2021), "The Adverse Human Rights Impacts of Canadian Technology Companies: Reforming Export Control with the Introduction of Mandatory Human Rights Due Diligence," *Canadian Journal of Law and Technology*.

[108] See also Canadian Coalition on Human Rights in China, "Harassment & Intimidation" at 50–51. For example, Public Safety Canada "has established a Federal, Provincial and Territorial Community of Practice on Economic-based national security threats to bring together key officials at the working level from across these jurisdictions to discuss national security threats that arise through economic activities. This includes, for example, threats arising from foreign direct investment, trade and exports, and the transfer or acquisition of Canadian intellectual property, knowledge, rights and licenses." A similar effort in relation to digital transnational repression has not been undertaken, despite the fact that such activity threatens and impairs the fundamental rights of Canadians and, more broadly, may facilitate understanding and responding to economic-based national security threats. National Security and Intelligence Committee of Parliamentarians (2019), "Annual Report," at 109 <https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf> [NSICOP 2019 Annual Report].

[109] NSICOP 2019 Annual Report.

[110] *Ibid* at 102.

institutions and fundamental rights and freedoms continue to be undermined by hostile states."[111] There is also a concern that investigations into foreign interference (often done by local police) will be "one-off" or "ad hoc" and "will not inform a broader understanding of the threat to national security, domestic sovereignty and the rights of Canadians."[112] These concerns have also been reflected in research by civil society organizations in Canada.[113]

- *Institute a dedicated hotline and/or reporting mechanism for individuals to confidentially report instances of digital and other forms of transnational repression and undertake outreach efforts to better understand what other services and support are required.* Engage in active community education efforts, in partnership with Canadian community organizations that work with refugees and immigrants, to share information regarding where individuals can receive support from government bodies.[114]
- *Ensure that existing government institutions that have mandates that overlap with transnational repression have staff who are trained to understand, investigate, and respond to digital and other forms of transnational repression and are sensitive to its impacts in communities in Canada.* Address existing distrust between government agencies such as CSIS and local communities by ensuring diversity within these institutions, undertaking public consultations, and implementing strong safeguards over CSIS' activities.
- *Provide resources (such as financial support) to Canadian community organizations that work closely with refugees and immigrants in Canada to help address transnational repression*. Government funding could be used by organizations to investigate the impact of transnational repression on their clients, offer digital security resources (e.g., Security Planner)[115] and educational resources related to transnational repression, and increase the availability of psychosocial and mental health support services for high-risk individuals.

[111] *Ibid* at 104.

[112] *Ibid* at 105.

[113] Alliance Canada HK, "In Plain Sight"; Canadian Coalition on Human Rights in China, "Harassment & Intimidation."

[114] See also Canadian Coalition on Human Rights in China, "Harassment & Intimidation" at 50–51; Alliance Canada HK, "In Plain Sight" at 12.

[115] Consumer Reports (2022), "Security Planner" <https://securityplanner.consumerreports.org/>.

Engage with Companies Implicated in the Infrastructure of Digital Transnational Repression

- *Legislate transparency into how social media companies respond to government requests to remove online content from their platforms or requests for user information.* Social media companies may end up facilitating acts of digital transnational repression by, for example, closing activists' social media pages pursuant to a request from state or state-related actors. Ensuring greater transparency into how such decisions are made and what their outcomes are provides a potential mechanism for accountability.
- *Engage with social media companies to understand how they currently identify and address digital transnational repression on their platforms and evaluate what mechanisms (for example, regulatory) might be suitable to ensure that social media companies act appropriately in response to this threat.*[116] In particular, there are concrete measures that social media companies can take to invest in the account security of their users and mitigate the threat of digital transnational repression, such as:
  - Facilitate and support the use of two-factor authentication and implement it as default for new accounts.
  - Undertake research on threats to activists and dissidents on their platforms and ensure sufficient resources and skills to understand and track these threats (e.g., sufficient language skills and awareness of political contexts).
  - Publicly report on the number of estimated cases of digital transnational repression on the platforms, along with how cases have been addressed and outcomes.
  - Provide warnings/notifications to users identified by platforms as being targeted by digital transnational repression and provide understandable and easily actionable advice. Such work should be done in partnership with community organizations to ensure that individuals receive the follow-up support they need.
  - Ensure language-localized security resources and guides for high-risk individuals in how to secure their accounts and engage with community and resettlement support organizations to make it easy for these organizations to refer urgent cases of digital transnational repression to platforms so that they can be assessed and addressed.

[116] In assessing the potential regulation of social media companies, caution must be exercised not to make the problem worse. Such regulatory measures should only be taken after careful, public, and exhaustive consultation with civil society and human rights organizations. See Cynthia Koo, Lex Gill, and Christopher Parsons (2021), "Comments on the Federal Government's Proposed Approach to Address Harmful Content Online," Citizen Lab <https://citizenlab.ca/2021/09/comments-on-the-federal-governments-proposed-approach-to-address-harmful-content-online/>.

- *Examine the role of other business actors in facilitating digital transnational repression and assess how such businesses should respond.* Entities to examine could include domain registrars, web-hosting companies, and companies whose services and products are used by other actors in developing and deploying digital surveillance technologies.

Conclusion

This report highlights how digital transnational repression impacts Canadian communities of dissidents and activists who are living in exile. In particular, such digital targeting has a serious impact on the well-being of victims, undermines their ability to engage in transnational advocacy work, violates fundamental rights such as the right to privacy, freedom of expression, and peaceful assembly, and increases the dangers faced by their family members and friends who remain within the country of origin.

At the same time, the growth of the surveillance market and the continued spread of digital technologies around the globe mean that the phenomenon of digital transnational repression is likely going to grow in scale and impact. We have argued in this report that the Canadian government has to take action to help prevent these abuses and to protect targeted Canadian communities. As we outlined, a number of gaps exist in policy and law on these issues, which the Canadian government must begin to address.

Areas for Further Research

There are several areas of research to pursue to better understand digital transnational repression and to craft additional recommendations targeted at government, civil society, and business entities. These include:

- Engaging with victims of digital transnational repression to understand how they define accountability in response to these threats, what remedies may be appropriate, and what their expectations are for how host states and companies implicated in digital transnational repression, such as social media companies, should respond.
- Investigating how the practices of social media companies may enable digital transnational repression (for example, by taking down user pages or blocking accounts); examining how digital transnational repression may be different from other types of online harms; and identifying what gaps exist in how social media companies respond to digital transnational repression and what further recommendations should be made to these companies to address it.

- Broadening research on digital transnational repression to include other countries beyond the United States and Canada; comparing how other host states have begun to address this issue; and identifying if a global framework or agreement could help facilitate a coordinated response to these activities across multiple countries and what the substantive content should be.

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF
TORONTO

THE CITIZEN LAB