

Response to request for information from the Research Directorate at the Immigration and Refugee Board (IRB) of Canada

September 11, 2026

Report authors:

Dr. Emile Dirks, Senior Research Associate, The Citizen Lab

Noura Aljizawi, Senior Researcher, The Citizen Lab

Maia Scott, Senior Researcher, The Citizen Lab

Rebekah Brown, Senior Researcher, The Citizen Lab

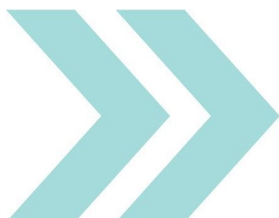
Dr. Marcus Michaelsen, Senior Researcher, The Citizen Lab

Siena Anstis, Senior Researcher, The Citizen Lab

Kristina Balaam, Senior Researcher, The Citizen Lab

For all inquiries related to this submission, please contact:

Dr. Ronald J. Deibert, Director, The Citizen Lab, Munk School of Global Affairs, Professor of Political Science, University of Toronto, r.deibert@utoronto.ca



At Trinity College
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

At the Observatory
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

munkschool.utoronto.ca

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

Table of Contents

Introduction

About the Citizen Lab

A Note On Terminology

A Note On Scope

Responses to Questions from the Research Directorate

Question 1

Chinese State Surveillance and Diaspora Governance

Targets of Chinese State Transnational Surveillance

Chinese State Surveillance Under Xi Jinping

Forms of Chinese State Surveillance: On- and Offline Activities

A. Online techniques

B. Offline techniques

Chinese State Surveillance Actors: State Agencies and Proxies

Question 2

Coercion-by-Proxy

Appendix: List Of Cited Citizen Lab Reports

Introduction

As senior researchers at the Citizen Lab, the authors of this submission welcome the opportunity to provide your office with information on the important issue of the monitoring of Chinese citizens and diaspora members in Canada by Chinese authorities and their proxies. In response to the questions provided by the Research Directorate at the Immigration and Refugee Board of Canada, this submission will:

1. Situate the Chinese government's monitoring activities in Canada within context of the Chinese government's broader diaspora governance agenda;
2. Present an overview of the profiles of Chinese citizens and diaspora members targeted for overseas monitoring;
3. Clarify the connection between overseas monitoring activities in Canada and state surveillance and repression in the People's Republic of China, specifically under the administration of China's current leader Xi Jinping;

4. Identify the online and offline monitoring techniques used by Chinese authorities and their proxies against individuals in Canada and other countries;
5. Identify which Chinese government offices and their proxies are involved in overseas monitoring activities; and
6. Explain how threats against the China-based family members of overseas Chinese citizens and diaspora members are a specific feature of the Chinese government's overseas monitoring activities.

The views expressed in this submission are those of the authors and do not necessarily reflect the views of other Citizen Lab researchers or the Citizen Lab as a whole.

About the Citizen Lab

Founded in 2001 by Professor Ronald J. Deibert, the Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, which focuses on novel threats to democracy, human rights, and global security in the digital ecosystem. The Citizen Lab uses a “mixed methods” approach to research, combining methods from political science, law, computer science, and area studies. Our research focus areas include app security and privacy; artificial intelligence; censorship; digital transnational repression; disinformation; law and policy; mass surveillance; and targeted surveillance. As an academic research unit at the University of Toronto, the Citizen Lab operates independent of government and corporate interests and evaluates the ethical and legal implications of all its projects.

Over the last 25 years, the Citizen Lab has studied state-sponsored surveillance, censorship, and targeted threats against journalists, human rights defenders, and civil society, either in their home countries or in exile and the diaspora. Since 2018, the Citizen Lab has led dedicated research on digital transnational repression, on a global scale, investigating the experiences of activists, journalists and human rights defenders from a variety of countries, including (but not limited to) China, Iran, Rwanda, Syria, Saudi Arabia, Azerbaijan, Myanmar, and Venezuela, residing in countries like Canada, the U.S., the U.K., and several European states. Applying mixed methods, including (but not limited to) semi-structured interviews, technical analysis, and open source intelligence, the Citizen Lab seeks to understand how origin states employ digital technologies to reach beyond borders to silence and repress diasporic and exiled activists, human rights defenders, journalists, and regime critics, and the impacts of these threats on targeted individuals and their transnational activism.

This submission concludes with an appendix of the Citizen Lab reports on transnational repression and Chinese state surveillance which are cited in this submission.

A Note On Terminology

For the purpose of this report, we use the term “Chinese citizens” to refer to individuals who are citizens of the People’s Republic of China (China), including permanent residents of the Hong Kong Special Administrative Region (Hong Kong) and the Macau Special Administrative Region (Macau), while the term “diaspora members” refers to individuals who are not Chinese citizens but who by birth or family ancestry are connected to people living in China.

We use the terms “overseas Chinese citizens” and “diaspora members” to refer to individuals who are Han Chinese (China’s majority ethnic group) or members of other non-Han ethnic communities (including, but not limited to, Uyghurs, Tibetans, and Mongolians).

We use the term “exiles” to refer to individuals who have been compelled to leave their country of origin and who are involved in activities in relation to their country of origin and/or causes of interest to their communities, such as human rights, advocacy, research, journalism, artistic expression, and community mobilization.

We use the term “targets” or “targeted individuals” to refer to individuals who Chinese authorities monitor due to their membership in a persecuted ethnic or religious community, or due to their political activities. These activities may include (but are not limited to) demonstrations of support for democratic values; human rights; digital rights; freedom of speech; gender equality; and creative expression.

We define “transnational repression” as actions undertaken by states or their proxies intended to silence, deter, or punish dissent outside of that state’s borders,¹ and the term “digital transnational repression” as the use of digital technologies to execute cross-border tactics to control, silence, and punish dissent.²

¹ ORCHR (2025), “Transnational Repression,” *ORCHR* (June 18, 2025)

<<https://www.ohchr.org/sites/default/files/documents/publications/transnational-repression-1-en.pdf>>.

² Marcus Michaelsen (2020), “The Digital Transnational Repression Toolkit, and Its Silencing Effects,” *Freedom House* (2020)

<<https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects>>

A Note On Scope

This submission focuses on how Chinese authorities and their proxies practice transnational repression by monitoring Chinese citizens and diaspora members in Canada. Most of the cases of overseas monitoring referred to in this report concern activities which occurred in Canada or involved individuals living in Canada. However, this submission also cites a small number of cases of the Chinese government's monitoring activities in other countries.

We believe that selective reference to a few non-Canadian cases, in addition to a larger number of Canada-specific cases, will provide a fuller picture of the Chinese government's overseas monitoring activities and their impacts on overseas Chinese citizens and diaspora members. Chinese authorities and their proxies use a range of on- and offline surveillance techniques as part of campaigns of transnational repression. Our research reveals that Chinese authorities' use of on- and offline surveillance is not confined to a single country or region. Instead, techniques used to monitor targets outside Canada could be used against Chinese citizens or diaspora members in Canada, or may have already been used against targets in Canada but remain undocumented. We therefore reference selected non-Canadian cases to provide a more comprehensive understanding of the scope and character of this problem.

Finally, in keeping with the questions provided by the Research Directorate, we have largely confined our analysis to examining the Chinese government's on- and offline monitoring activities abroad. This submission is therefore not an exhaustive examination of all the tactics of transnational repression, digital transnational repression, and gender-based digital transnational repression Chinese authorities use against exiles and diaspora members. For example, this submission does not explore in depth Chinese state-sponsored online attacks (e.g. deepfakes, doxxing, defamation, disinformation) to harass exiled activists.³ Nor does this submission examine how Chinese authorities and other authoritarian or illiberal states have

³ Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022). <<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>; Noura Aljizawi, Siena Anstis, Marcus Michaelson, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybullayeva, Muetter Iliq, Nicola Lawford, Émilie LaFlèche, Gabrielle Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *The Citizen Lab* (December 2, 2024) <<https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>>

attempted to intimidate, kidnap, or secure the unlawful deportation of migrants and asylum seekers in third countries⁴, including individuals who Canadian authorities have offered to resettle in Canada.⁵ Finally, this submission does not discuss the “overseas police service stations” established in Canada and other countries by the Public Security Bureaus of particular localities in China, and their purported involvement in monitoring overseas Chinese citizens and diaspora members.⁶ These and other forms of transnational repression are beyond the scope of this submission but are worth the attention of the Research Directorate.

Responses to Questions from the Research Directorate

Question 1

Do Chinese authorities monitor Chinese citizens in Canada?

If so, can you describe the profiles of such individuals who Chinese authorities are typically motivated to monitor in Canada?

⁴ Emile Dirks, Sarah McKune, Nate Schenckan, Sydney Smythe, and Yaqiu Wang (2026), “Submission to the Committee on Enforced Disappearances and the Working Group on Enforced and Involuntary Disappearances on the enforced disappearance of migrants in the context of transnational repression,” *The Citizen Lab* (January 31, 2026)

<https://citizenlab.ca/wp-content/uploads/2026/02/Submission_The-Citizen-Lab_31-January-2026_Call-for-inputs-on-Enforced-Disappearances-in-the-context-of-transnational-repression.pdf>

⁵ Nick Logan (2015), “UN told Thai government deported Chinese activists were poised to come to Canada,” *Global News* (November 30, 2015)

<<https://globalnews.ca/news/2371066/un-told-thai-government-deported-chinese-activists-were-poised-to-come-to-canada/>>; CBC (2025), “Canada, U.S. offered Uyghurs in Thailand asylum before their deportation to China: sources,” *CBC* (March 5, 2025) <<https://www.cbc.ca/news/uyghurs-deportation-china-1.7474958>>; Kanis Leung (2026), “A Chinese dissident recounts his perilous dinghy escape to South Korea and how he got to Canada,” *AP News* (June 29, 2026)

<<https://apnews.com/article/china-dissident-dong-guangping-south-korea-canada-8e50cfb73064865363322a37008cad5>>; Holmes Chan (2026), “Chinese activist held in Bangkok finds Canada refuge,” *CTV News* (August 7, 2026) <<https://www.ctvnews.ca/canada/article/chinese-activist-held-in-bangkok-finds-canada-refuge/>>

⁶ Emile Dirks and Diana Fu (2024), “China’s overseas police stations: An imminent security threat?,” *Brookings* (February 16, 2024)

<<https://www.brookings.edu/articles/chinas-overseas-police-stations-an-imminent-security-threat/>>; Safeguard Defenders (2024), “Patrol and Persuade: A Follow Up On 110 Overseas Investigation,” *Safeguard Defenders* (May 2, 2024) <<https://safeguarddefenders.com/en/blog/patrol-and-persuade-follow-110-overseas-investigation>>; The Guardian (2026), “New York man found guilty of acting as unregistered agent of China,” *The Guardian* (May 14, 2026)

<<https://www.theguardian.com/us-news/2026/may/13/new-york-man-guilty-unregistered-agent-china>>

If so, can you describe the nature of this monitoring in practice, including how and where it takes place within Canada?

If so, can you describe the various state agencies involved in such monitoring, including any potential presence of Chinese authorities in Canada?

Chinese State Surveillance and Diaspora Governance

Chinese authorities and their proxies routinely monitor the political activities of select overseas Chinese citizens living in Canada, as well as members of diaspora communities who are Canadian citizens. The goal of this on- and offline surveillance, along with more coercive forms of transnational repression, is to silence overseas opposition to the Chinese government and any critical voices that challenge the Chinese government's preferred political narratives. These chilling effects extend beyond targeted individuals and impact other Chinese citizens and diaspora members in Canada. The looming threat of state repression, referred to by some scholars of contemporary China as the "anaconda in the chandelier," can encourage a culture of political self-censorship among Chinese citizens and diaspora members.⁷

The Chinese government's overseas monitoring activities are part of its larger efforts to exert influence over Chinese citizens and diaspora members around the world. This political project dates back decades and has continued under Xi Jinping (2012-present), China's current paramount leader. The Chinese government's diaspora governance playbook consists of two broad approaches. First, consent-building activities intended to cultivate support for the Communist Party within key overseas constituencies, and, second, coercive measures intended to silence dissent among select overseas Chinese citizens and diaspora members.

Consent-building and coercion are two strategies that Chinese authorities and their proxies use to increase the Chinese government's influence across national borders. These activities range from lawful and benign forms of foreign influence (e.g. Chinese government-sponsored cultural and language exchange programs), to unlawful and malign forms of foreign

⁷ "In sum, the Chinese government's censorial authority in recent times has resembled not so much a man-eating tiger or fire-snorting dragon as a giant anaconda coiled in an overhead chandelier. Normally the great snake doesn't move. It doesn't have to. It feels no need to be clear about its prohibitions. Its constant silent message is "You yourself decide," after which, more often than not, everyone in its shadow makes his or her large and small adjustments—all quite "naturally." See: Perry Link. "China: The Anaconda in the Chandelier," *ChinaFile* (April 11, 2002) <<https://www.chinafile.com/library/nyrb-china-archive/china-anaconda-chandelier>>

interference (e.g. disinformation campaigns and electoral interference).⁸ Collectively these activities serve the common goal of buttressing the Communist Party's power and prestige at home and abroad.⁹

At the outermost edge of this spectrum are coercive activities commonly known as transnational repression. The monitoring of Chinese citizens and diaspora members in Canada and elsewhere constitutes a specific form of transnational repression, one which has profound implications for the rights of targeted individuals.

Targets of Chinese State Transnational Surveillance

Surveillance operations targeting overseas Chinese citizens and diaspora members reflect the authoritarian character of the Chinese government itself. While the Chinese government has described its form of government as a “whole-process people's democracy,”¹⁰ China is in fact a single-party autocracy dominated by the Communist Party of China. Civil and political rights are highly restricted, and Chinese authorities use a variety of legal and extralegal measures to control civil society and repress dissent. Targets of Chinese state surveillance and repression are people who Chinese authorities view as direct opponents of the Communist Party, or are individuals viewed as threats to the Communist Party's authority, either by virtue of the person's political beliefs, their ethnic or religious identity, or their link to someone who falls within one of these categories.

Those who Chinese authorities monitor in Canada therefore tend to resemble the groups Chinese authorities monitor inside China. Targeted overseas Chinese and diaspora members in Canada include (but are not limited to):

⁸ Diana Fu and Emile Dirks, “The TikTok debacle: Distinguishing between foreign influence and interference,” *Brookings* (June 24, 2024)

<<https://www.brookings.edu/articles/the-tiktok-debacle-distinguishing-between-foreign-influence-and-interference/>>; Diana Fu, “Distinguish Foreign Influence from Foreign Interference,” *Johns Hopkins School of Advanced International Studies* (2025)
<<https://mediahost.sais-jhu.edu/saismedia/media/web/reports/distinguish-foreign-influence-foreign-interference.html>>

⁹ Emile Dirks and Diana Fu (forthcoming), “Governing Global China's Diaspora,” *Cambridge Elements Global China*; Emile Dirks and Diana Fu (2024), “China's overseas police stations: An imminent security threat?,” *Brookings* (February 16, 2024)

<<https://www.brookings.edu/articles/chinas-overseas-police-stations-an-imminent-security-threat/>>

¹⁰ “What to know about whole-process people's democracy in China,” *The State Council of the People's Republic of China* (March 6, 2025)

<https://english.www.gov.cn/news/202503/06/content_WS67c8f0a0c6d0868f4e8f0784.html>

- pro-democracy and human rights campaigners, exiled political dissidents, and civil society activists;
- students, scholars, writers, journalists, artists, social media influencers, and new media professionals who express anti-Communist Party views or opinions at odds with the Chinese government's preferred narratives;
- members of ethnic or religious communities, including (but not limited to) Tibetans, Uyghurs, Mongolians, and Falun Gong practitioners;
- supporters of, or participants in, Hong Kong's pro-democracy protest movement;
- individuals, including current or former Communist Party members and state employees, who are accused of corruption, financial crimes, and/or official malfeasance; and
- the family members of any of the above individuals.

Targets of Chinese state surveillance in Canada are not always highly public figures. Some may use various forms of public advocacy to openly criticize the Chinese government, and may do so as an individual or as a member of civil society organizations. Others may express their political views on social media under their real name or pseudonymously, or may privately communicate their political opinions with fellow Chinese citizens or diaspora members via text message, email, or direct messages on (un)encrypted messaging apps. Others may have faced state persecution in China, and now in Canada refrain from any on- or offline activities abroad which they believe would expose them or their China-based family members to reprisals from Chinese authorities.

Whether or not these individuals chose to publicly express their views on the Chinese government, they may still be targeted for Chinese state surveillance simply by virtue of belonging to one of the aforementioned groups. Particular digital tools and techniques, described in detail later in this submission, are making it easier for Chinese authorities to track the location and activities of people overseas, often without the person's knowledge. On- or offline surveillance can in turn place an individual at greater risk of state persecution. For example, should an individual who was surveilled be compelled to return to China, information collected on that individual's political activities in Canada could be used by Chinese authorities to justify their detention and/or prosecution.

Chinese State Surveillance Under Xi Jinping

Monitoring Chinese citizens in Canada is not a new phenomenon. As far back as the 1980s, particularly in the aftermath of the 1989 Tiananmen Square protest movement and

subsequent massacre, Chinese authorities associated with diplomatic offices began surveilling Chinese post-secondary students in North America for evidence of pro-democracy, human rights advocacy, or anti-Communist Party sentiment. As former Chinese student activists and other exiles in Canada and the United States continued to agitate for political change in China in the wake of the 1989 killings,¹¹ the Chinese government's overseas surveillance activities increased. Under the administrations of Jiang Zemin (1989-2002) and Hu Jintao (2002-2012), Chinese authorities expanded the scope of these overseas monitoring activities to encompass a wider assortment of Chinese citizens and diaspora members, including Tibetans, Uyghurs, and Falun Gong practitioners. State surveillance was soon accompanied by other kinds of targeted coercion now commonly referred to as transnational repression.

While the Chinese government's monitoring of overseas Chinese citizens and diaspora members in Canada dates back decades, these operations have grown in scope and intensity under the administration of Xi Jinping.¹² The Chinese government under Xi is not the only illiberal or authoritarian government currently engaged in transnational repression. However, it is currently the most prolific perpetrator of transnational repression, according to the think tank Freedom House.¹³ One of the chief causes for the Chinese government's heightened attempts to monitor and harass overseas citizens is tightening state repression in China under Xi's rule. Experts on Chinese politics characterize Xi's government as more authoritarian and repressive than previous administrations.¹⁴ The Xi administration's intolerance of dissent was signalled early on through a leaked 2013 Communist Party communiqué which listed seven foreign and domestic ideological threats to the Party's power.¹⁵

¹¹ Rowena He (2014), *Tiananmen Exiles: Voices of the Struggle for Democracy in China*, New York: Palgrave Macmillan; Stefano Chessa Altieri (2026), "The Best and Loudest: The Rise (and Fall) of the Independent Federation of Chinese Students and Scholars (1989–1992)," *Diplomatic History* 50(1): 50-77.

¹² Yana Gorokhovskaia and Grady Vaughan (2025), "Engaging the Community: Combating Transnational Repression in Canada," *Freedom House*

<<https://freedomhouse.org/report/transnational-repression/canada/2025>>.

¹³ Grady Vaughan, Yana Gorokhovskaia, and Nate Schenkkan (2025), "Ten Findings from Ten Years of Data on Transnational Repression," *Freedom House* (February 6, 2025)

<<https://freedomhouse.org/article/ten-findings-ten-years-data-transnational-repression>>

¹⁴ Carl Minzer (2018), *End of an Era: How China's Authoritarian Revival is Undermining Its Rise*, New York: Oxford University Press; Minxin Pei (2026), *The Broken China Dream: How Reform Revived Totalitarianism*, Princeton: Princeton University Press; Elizabeth C. Economy (2018), *The Third Revolution: Xi Jinping and the New Chinese State*, New York: Oxford University Press; Diana Fu and Emile Dirks (2022), "The People's Leader: The Xi Jinping Era of Chinese Politics," in *The Oxford History of Modern China*, ed. Jeffery N. Wasserstrom, Oxford: Oxford University Press.

¹⁵ These seven threats included: 1) constitutional democracy; 2) universal values; 3) civil society; 4) neoliberalism; 5) freedom of the press; 6) "historical nihilism;" and 7) questioning "socialism with Chinese characteristics." See: ChinaFile (2013), "Document 9: A ChinaFile Translation," *ChinaFile* (November 8, 2013) <<https://www.chinafile.com/document-9-chinafile-translation>>

As part of Xi's broader attempts to deepen the Communist Party's control over Chinese society, Chinese authorities have launched crackdowns in key sectors and specific subnational regions, including (but not limited to):

- a campaign against human rights lawyers and other legal professionals begun on July 9, 2015, known as the “709 crackdown”;¹⁶
- a program of mass detainment, surveillance, and cultural destruction targeting Uyghurs and other non-Han people in the Xinjiang Uyghur Autonomous Region beginning in the mid-2010s;¹⁷
- the evisceration of civil liberties in the Hong Kong Special Administrative Region following the suppression of the 2019-2020 pro-democracy protest movement;¹⁸
- mass biometric data collection and restrictions on local languages and cultural practices in the Tibet Autonomous Region and the Inner Mongolia Autonomous Region;¹⁹
- a national anti-corruption campaign against Communist Party members and state employees begun in 2012, which has doubled as a political purge of Xi's internal opponents;²⁰

¹⁶Human Rights Watch (2025), “China: 10 Years Since ‘709 Crackdown,’ Lawyers Still Under Fire,” *Human Rights Watch* (July 6, 2025)

<<https://www.hrw.org/news/2025/07/06/china-10-years-since-709-crackdown-lawyers-still-under-fire>>.

¹⁷ Australian Strategic Policy Institute (2020), “The Xinjiang Data Project,” *Australian Strategic Policy Institute* (ASPI) <<https://xjdp.aspi.org.au/>>; Human Rights Watch (2021), ““Break Their Lineage, Break Their Roots”: China’s Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims,” *Human Rights Watch* (April 19, 2021)

<<https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting>>.

¹⁸ The Committee for Freedom in Hong Kong Foundation (2025), “The Hong Kong National Security Law at 5: Unhappy Birthday,” *The CFHK Foundation* (June 30, 2025)

<<https://thecfhk.org/the-hong-kong-national-security-law-at-5-unhappy-birthday/>>.

¹⁹Emile Dirks (2022), “Mass DNA Collection in the Tibet Autonomous Region from 2016–2022,” *The Citizen Lab* (September 13, 2022) <<https://citizenlab.ca/research/mass-dna-collection-in-the-tibet-autonomous-region/>>; The Action Institute (2025), “When They Came to Take Our Children: China’s Colonial Boarding Schools and the Future of Tibet,” *The Action Institute* (May 2025) <<https://tibetaction.net/when-they-came-to-take-our-children/>>; Erika Nguyen (2026), “Save Our Mother Tongue: Online Repression and Erasure of Mongolian Culture in China,” *Pen America* (January 20, 2026) <<https://pen.org/report/inner-mongolia-china-repression/>>.

²⁰ Minxin Pei (2025), “From Purge to Control: A Recent Pivot in Xi Jinping’s Anti-Corruption Crackdown,” *China Leadership Monitor* (February 27, 2025) <<https://www.prcleader.org/post/from-purge-to-control-a-recent-pivot-in-xi-jinping-s-anti-corruption-crackdown>>.

- routine campaigns led by the Cyberspace Administration of China against illegal and “harmful” online content, which frequently target politically-prohibited speech;²¹ and
- tightening restrictions on the operations of registered and unregistered civil society organizations.²²

The effects of these campaigns, coupled with state repression of other forms of political dissent, have reverberated far beyond China’s borders and impacted Chinese citizens and diaspora members around the world. Individuals persecuted in China have fled to Canada or other countries, either directly or via third countries, in search of asylum. Chinese citizens who are already living abroad have become targets of Chinese government intimidation and other forms of transnational repression. Other individuals have found that merely belonging to a particular ethnic or religious community puts them at risk of Chinese state surveillance activities overseas.²³

Compounding the threat to exiles and diaspora members posed by these campaigns of state repression are Chinese laws which criminalize political dissent, including activities conducted outside China. The Law of the People’s Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (also known as the National Security Law) asserts jurisdiction over individuals both in Hong Kong and around the world and criminalizes a range of offenses, including secession, subversion, terrorism, and collusion with foreign forces.²⁴ Hong Kong authorities have already used this law, and Article 23 of Hong Kong’s Basic Law,²⁵ to charge exiled supporters of the city’s pro-democracy protest movement,²⁶

²¹Shijie Wang (2025), “Beijing’s War on ‘Negative Energy,’” *Jamestown* (October 31, 2025) <<https://jamestown.org/beijings-war-on-negative-energy/>>.

²² Emile Dirks and Diana Fu (2022), “Governing ‘Untrustworthy’ Civil Society in China,” *The China Journal* 89: 101-122.

²³Scilla Alecci (2025), “Inside China’s machinery of repression — and how it crushes dissent around the world,” *International Consortium of Investigative Journalists (ICIJ)* (April 28, 2025) <<https://www.icij.org/investigations/china-targets/china-transnational-repression-dissent-around-world/>>.

²⁴Donald Clarke (2020), “Hong Kong’s National Security Law: An Assessment,” *China Leadership Monitor* (July 13, 2020) <<https://www.prcleader.org/post/hong-kong-s-national-security-law-an-assessment>>.

²⁵ Amnesty International (2024), “What is Hong Kong’s Article 23 law? 10 things you need to know,” *Amnesty International* (March 22, 2024) <<https://www.amnesty.org/en/latest/news/2024/03/what-is-hong-kongs-article-23-law-10-things-you-need-to-know/>>.

²⁶ Amnesty International (2023), “Hong Kong: Absurd Cash Bounties on Overseas Activists Designed to Sow Fear Worldwide,” *Amnesty International* (December 14, 2023) <<https://amnesty.ca/human-rights-news/hong-kong-absurd-cash-bounties-on-overseas-activists-designed-to-sow-fear-worldwide/>>; Farah Master and Jessie Pang (2024), “Hong Kong uses new national security law against exiled activists,” *Reuters* (June 12, 2024) <<https://www.reuters.com/world/asia-pacific/hong-kong-uses-new-national-security-law-against-exiled-activists-2024-06-12/>>.

including individuals in Canada.²⁷ The Chinese government has also claimed the right to prosecute individuals outside China who violate the country's Law on Promoting Ethnic Unity and Progress (also known as the Ethnic Unity Law),²⁸ recent legislation which codifies the Xi administration's efforts to forcibly assimilate non-Han Chinese ethnic communities and criminalize opposition to China's ethnic policies.²⁹

Exiles and diaspora members engaged in overseas activism therefore face the credible risk of detention and criminal prosecution should they return to China. These risks are not merely speculative. In recent years, Chinese citizens have been detained and convicted on the basis of their peaceful political activism overseas. In 2024, a Chinese artist who had returned to China from the United States was detained and in 2026 was sentenced to three years in prison for "slandering China's heroes and martyrs," an offense under China's Law on the Protection of Heroes and Martyrs,³⁰ in response to his artworks which criticized China's former leader Mao Zedong.³¹ In a similar case in 2025, a Chinese citizen studying in the United Kingdom was arrested after returning to China and charged with "inciting others to split the country and undermine national unity," an offense under China's Criminal Law, in response to her overseas activism in defense of human rights in Tibet.³²

These prosecutions and convictions highlight the Xi administration's intolerance of dissent, including among Chinese citizens living abroad. State repression remains a core feature of

²⁷ CBC (2025), "Hong Kong announces arrest warrants, rewards for exiles who formed political committee in Canada," *CBC News* (July 25, 2025)

<<https://www.cbc.ca/news/world/hong-kong-rewards-exiles-canada-1.7594040>>.

²⁸ Reuters (2026), "China says it has a right to target people overseas with new ethnic unity law," *Reuters* (June 24, 2026)

<<https://www.reuters.com/world/china/china-says-it-has-right-target-people-overseas-with-new-ethnic-unity-law-2026-06-24/>>.

²⁹ James Leibold and Tenzin Dorjee (2026), "The Next Phase of China's Minority Crackdown," *Foreign Affairs* (July 30, 2026)

<<https://www.foreignaffairs.com/china/next-phase-chinas-minority-crackdown#>>.

³⁰ Deutsche Welle (2018), "China criminalizes defamation of revolutionary heroes," *Deutsche Welle* (April 27, 2018) <<https://www.dw.com/en/china-criminalizes-defamation-of-revolutionary-heroes/a-4356346>>.

³¹ Amnesty International (2026), "China: Maximum sentence for artist Gao Zhen is an assault on artistic freedom," *Amnesty International* (August 25, 2026)

<<https://www.amnesty.org/en/latest/news/2026/08/china-maximum-sentence-for-artist-gao-zhen-is-an-assault-on-artistic-freedom/>>.

³² Human Rights Watch (2025), "China: Free Student Advocate for Tibetan Rights," *Human Rights Watch* (September 23, 2025) <<https://www.hrw.org/news/2025/09/23/china-free-student-advocate-for-tibetan-rights>>;

Jessie Lau (2025), "'She didn't realise how dangerous it was': London-bound student held in China over Tibet support," *The Guardian* (September 30, 2025)

<<https://www.theguardian.com/global-development/2025/sep/30/china-tibet-student-zhang-yadi-dalai-lama-university-soas-london-transnational-repression>>.

political life in China³³, as well as a core component of the Chinese government's diaspora governance strategies.³⁴ The Xi administration's continuing efforts to strengthen the Communist Party's hold on power at home, and its attempts to exert influence and control over Chinese citizens abroad, makes it highly unlikely that Chinese authorities will cease monitoring overseas Chinese citizens and diaspora members in Canada and elsewhere for signs of political dissent.

Forms of Chinese State Surveillance: On- and Offline Activities

Chinese authorities use various surveillance tactics to identify members of overseas communities viewed as threats, including both on- and offline techniques. Here, the term "online" techniques refers to the remote monitoring of a target via digital means (e.g., phishing campaigns, account hacking, the use of malware/spyware, or the monitoring of public social media accounts), which can be carried out from anywhere with an internet connection. The term "offline" techniques refers to non-digital forms of observation and surveillance (e.g., in-person monitoring of peaceful protests and assemblies, stalking, daily physical surveillance) which require physical presence in proximity to the targeted person.

On- and offline monitoring are not mutually exclusive categories and the line separating the two can be blurry. Online monitoring is complementary to offline monitoring and can facilitate it. In other words, information gathered about a person online can be used for the purpose of offline/physical surveillance and intimidation.³⁵ For example, tracking someone's social media account can be used to determine the person's location, the places they visit, their daily patterns, and their behaviours, all of which can in turn facilitate in-person

³³ Human Rights Watch (2026), "China Events of 2025," *Genocide Watch* (February 16, 2026) <<https://www.genocidewatch.com/single-post/china-events-of-2025>>.

³⁴ Emile Dirks and Diana Fu (forthcoming), "Governing Global China's Diaspora," Cambridge Elements Global China series; Emile Dirks and Diana Fu (2024), "China's overseas police stations: An imminent security threat?," *Brookings* (February 16, 2024) <<https://www.brookings.edu/articles/chinas-overseas-police-stations-an-imminent-security-threat/>>

³⁵ Siena Anstis, Tristan Surman, Noura Aljizawi, Marcus Michaelson, and Ron Deibert (2026), "Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the Committee on Enforced Disappearances and the Working Group on Enforced or Involuntary Disappearances," *The Citizen Lab* (January 31, 2026) <https://citizenlab.ca/wp-content/uploads/2026/02/Submission_The-Citizen-Lab_30-January-2026_Call-for-inputs-on-Enforced-Disappearances-in-the-context-of-transnational-repression.pdf>; Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022) <<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>.

surveillance. Online surveillance can also be paired with offline attacks or the threat of offline attacks.³⁶

The techniques used by the Chinese government in their campaigns of transnational repression are not unique to China. Other repressive states have used similar measures to surveil and intimidate their own overseas citizens and other members of other diaspora communities.³⁷ Spyware and malware have been used to monitor individuals' activities in real-time and facilitate offline attacks, while phishing and account takeovers have enabled state-actors to gain access to the private messages and communications of targeted people, including information on flight or hotel bookings. Nor do the on- and offline techniques discussed below constitute an exhaustive list of the tactics of transnational repression used by Chinese authorities and their proxies. As the Chinese government continues to invest in its domestic security apparatus and pursue its perceived opponents and critics abroad, it is possible that Chinese authorities will innovate new methods of overseas surveillance.

Regardless of how Chinese authorities practice overseas surveillance, both on- and offline techniques exact a heavy price on a person's sense of safety and well-being. Those targeted by Chinese authorities and their proxies can suffer intense emotional, psychological, professional, and reputational harm, as can a target's family members or intimate partners. Overseas surveillance and other forms of transnational repression also impact the ability of victims to exercise core civil and political rights, including freedom of expression, movement, and association.³⁸

³⁶ Siena Anstis, Tristan Surman, Noura Aljizawi, Marcus Michaelsen, and Ron Deibert, "Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the Committee on Enforced Disappearances and the Working Group on Enforced or Involuntary Disappearances," *The Citizen Lab* (January 31, 2026)

<https://citizenlab.ca/wp-content/uploads/2026/02/Submission_The-Citizen-Lab_30-January-2026_Call-for-inputs-on-Enforced-Disappearances-in-the-context-of-transnational-repression.pdf>.

³⁷ Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022).

<<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>; Noura Aljizawi, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybullu, Muetter Iliqut, Nicola Lawford, Émilie LaFlèche, Gabrielle Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *The Citizen Lab* (December 2, 2024)

<<https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>>; Freedom House, "Transnational Repression," *Freedom House*

<<https://freedomhouse.org/report/transnational-repression>>.

³⁸ Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022).

<<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>;

Psychological and Emotional War; Noura Aljizawi, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila

A. Online techniques

Online surveillance techniques fall within a wider category of coercive measures referred to as digital transnational repression. As a specific form of digital transnational repression, digital surveillance can be invisible and pervasive, occurring directly on a targeted individuals' devices regardless of where they live. This capacity to digitally monitor targets in Canada and other countries reflects the Chinese government's long-standing investment in its internal security apparatus, which has provided Chinese authorities at the national and sub-national levels with an increasingly wide array of tools to surveil individuals and communities in and outside China.³⁹

There are four major techniques of overseas online surveillance used by Chinese authorities:

- A. social media monitoring;
- B. impersonation and account takeover;
- C. malware and spyware; and
- D. social engineering and phishing.

These four techniques are not mutually exclusive, and targeted overseas Chinese citizens and diaspora members may be subjected to multiple forms of online surveillance.

A) Social media monitoring: This is among the most common forms of Chinese state digital surveillance. Social media monitoring occurs across different social media platforms, including Western platforms (e.g., Facebook, Instagram, YouTube, X) and China-based platforms (e.g., WeChat, RedNote). Overseas Chinese citizens and diaspora members often use China-based social media platforms like WeChat to communicate. However, WeChat

Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybulla, Muetter Iliqut, Nicola Lawford, Émilie LaFlèche, Gabrielle Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *The Citizen Lab* (December 2, 2024)

<<https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>>; Gina Romero (2026), "Digital Surveillance is Breaking Activist Mental Health," *Global Voices* (June 23, 2026) <<https://globalvoices.org/2026/06/23/digital-surveillance-is-breaking-activist-mental-health/>>; Yaqiu Wang, "Why Some Chinese Immigrants Living in Canada Live in Silent Fear," *The Globe and Mail* (February 25, 2019) <<https://www.theglobeandmail.com/opinion/article-why-some-chinese-immigrants-living-in-canada-live-in-silent-fear/>>.

³⁹ Sheena Greitens (2026), "China's Internal Security Spending: An Assessment of New Data," *The China Quarterly* 266.

surveillance extends directly to non-China-registered accounts (e.g., accounts registered to users in Canada), gathering users' information, public and private communications, and monitoring their activities and interactions.⁴⁰ Through open-source intelligence and content filtering tactics, Chinese authorities scan user content published on these platforms, identify social media accounts of interest, and monitor the activities of these accounts and the accounts interacting with them.

B) Impersonation and account takeover: This tactic involves gaining access to private social media chat groups to gather information about the chat group's members. In order to gain access to these closed groups and gain the trust of group members, Chinese authorities or their proxies may either create fake online identities, impersonate a member of the group, or gain control of an existing group member's account. Having gained access to the closed group, the Chinese state or state-backed actor will attempt to collect information on group members' on- and offline activities. Chinese authorities can in turn leverage this information to orchestrate other on- or offline threats, including targeted harassment, maliciously sharing of an individual's personal details online (known as "doxxing"), and other forms of coercion.⁴¹

In addition to infiltrating private social media chat groups, state-affiliated threat actors have also infiltrated public social media groups.⁴² Within public Telegram channels, for example, threat actors regularly create long-standing identities, masquerading as members of a particular community in order to distribute spyware directly to other users⁴³ or to guide channel members toward malicious websites, including fake app stores controlled by the threat actor.⁴⁴

⁴⁰ Jeffrey Knockel, Christopher Parsons, Lotus Ruannon-Chinese-registered, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert. "We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus," *The Citizen Lab* (May 7, 2020) <<https://citizenlab.ca/research/we-chat-they-watch/>>; Miles Kenyon, "WeChat Surveillance Explained, FAQ," *The Citizen Lab* (May 7, 2020). <<https://citizenlab.ca/research/we-chat-they-watch/wechat-surveillance-explained/>>.

⁴¹ Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022). <<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>

⁴² Katrina Manson (2022), "Spyware Tied to China Targets Apps Used by Uyghurs, Cybersecurity Firm Says," *Bloomberg* (November 10, 2022) <<https://www.bloomberg.com/news/articles/2022-11-10/lookout-researchers-say-spyware-tied-to-china-is-targeting-apps-used-by-uyghurs>>.

⁴³ Callum Roxan, Paul Rascagneres, and Tom Lancaster (2023), "EvilBamboo Targets Mobile Devices in Multi-year Campaign," *Volexity* (September 22, 2023) <<https://www.volexity.com/blog/2023/09/22/evilbamboo-targets-mobile-devices-in-multi-year-campaign/>>

⁴⁴ Mike Dvilyanski and Nathaniel Gleicher (2021), "Taking Action Against Hackers in China," *Meta* (March 24, 2021) <<https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/>>.

Social media monitoring can also lead to account takeover and impersonation. In 2024, leaked data from the Chinese contracting company Shanghai Anxun (also known as I-Soon) revealed the Ministry of Public Security's use of a tool to monitor social media activity on X (formerly Twitter).⁴⁵ This tool supported monitoring of specific X (formerly Twitter) accounts, which could also be phished to gain access to a user's direct messages and allow the attackers to post messages on the user's behalf.⁴⁶ Hijacked accounts could then be grouped together to post similar content or interact with specific users.

C) Malware and spyware: This kind of sophisticated category of surveillance software is capable of gaining full control over a compromised device following the installation of malicious software. Such capabilities include obtaining full access to sensitive personal and professional data on the device, such as text messages, chats, photos, emails, drives, cloud storage, calendars, and real-time location tracking. This software can also turn on the device's camera and microphone without user interaction.⁴⁷

Malware and spyware infections are often paired with targeted social engineering tactics to lure targets into clicking malicious links, opening infected files, or even installing the compromised application. In a 2020 report, the cybersecurity company Lookout documented a long-running mobile surveillance campaign primarily targeting Uyghurs in China and abroad, as well as Tibetans and other Muslim communities. The report identified a form of Android malware that steals personal data and provides extensive surveillance capabilities, which was linked to a wider network of cyberespionage operations associated with Chinese threat actors dating back to at least 2013.⁴⁸

⁴⁵ Paul Mozur, Keith Bradsher, John Liu and Aaron Krolik (2024), "Leaked Files Show the Secret World of China's Hackers for Hire," *The New York Times* (February 24, 2024)

<<https://www.nytimes.com/2024/02/22/business/china-leaked-files.html>>

⁴⁶ Brandon Karpf (2024) "The I-Soon data leak unveils China's cyber espionage tactics, techniques, procedures, and capabilities." *The CyberWire* (Feb 22, 2024)

<<https://thecyberwire.com/stories/05ba5c2ff18f4af5abc30ebe28c968bf/the-i-soon-data-leak-unveils-chinas-cyber-espionage-tactics-techniques-procedures-and-capabilities>>.

⁴⁷ Mohammed Al-Maskati, Bill Marczak, Siena Anstis, and Ron Deibert. "Peace through Pegasus: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware," *The Citizen Lab* (April 5, 2022)

<<https://citizenlab.ca/research/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/>>.

⁴⁸ Lookout Threat Intelligence Lab (2020), "Mobile APT Surveillance Campaigns Targeting Uyghurs," Lookout (June 2020) <<https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf>>.

Members of at-risk communities have also reported the forced installation of lawful intercept surveillanceware⁴⁹ at border crossings, checkpoints, after interactions with law enforcement⁵⁰ and even through WeChat-distributed directives.⁵¹ While lawful intercept surveillanceware is often described as non-persistent forensics tools, reports indicate that these products are not necessarily removed from the user's device after their interaction with law enforcement, and can continue to exfiltrate sensitive data even after the individual has been released and has left mainland China.⁵²

Numerous technical reports have documented these Chinese government-sponsored surveillance campaigns, and have highlighted malware and spyware families such as BadBazaar⁵³ and Moonshine,⁵⁴ alongside the distribution of trojanized applications like UyghurEditPP which provide attackers with a backdoor into the devices of targeted exiled and diaspora activists.⁵⁵ Reports also indicate that data collected from compromised devices have been cited by Chinese authorities as indicators of so-called "pre-criminal activity"⁵⁶, and have been used to justify criminal charges⁵⁷, arrests, and detentions inside China.⁵⁸

⁴⁹ Morgan Marquis-Boire (2014), "Schrodinger's Cat Video and the Death of Clear-Text," The Citizen Lab (August 15, 2014) <<https://citizenlab.ca/research/cat-video-and-the-death-of-clear-text/>>.

⁵⁰ Christian Shepherd and Yuan Yang (2019), "Chinese police use app to spy on citizens' smartphones," Financial Times (July 4, 2019) <<https://www.ft.com/content/73aebaaa-98a9-11e9-8cfb-30c211dcd229?syn-25a6b1a6=1>>.

⁵¹ Darren Byler (2018), *Spirit Breaking: Uyghur Dispossession, Culture Work and Terror Capitalism in a Chinese Global City*, PhD dissertation, University of Washington. <https://digital.lib.washington.edu/server/api/core/bitstreams/16459f8d-7dda-4e4c-bd08-05f35ba01600/content> >.

⁵² Lookout Threat Intelligence Lab (2024), "Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus," *Lookout* (December 11, 2024) <<https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware/>>.

⁵³ Lookout Threat Intelligence Lab, "Lookout Discovers Surveillance Campaigns Targeting Uyghurs," *Lookout* (January 22, 2024) <<https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15>>

⁵⁴ Canadian Centre for Cyber Security, "Joint guidance on BADBAZAAR and MOONSHINE," *Government of Canada* (April 9, 2025) <<https://www.ncsc.gov.uk/files/NCSC-Advisory-BADBAZAAR-and-MOONSHINE-guidance.pdf>>; Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits," *The Citizen Lab* (September 24, 2019) <<https://citizenlab.ca/research/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/>>

⁵⁵ Rebekah Brown, Marcus Michaelson, Matt Brooks, and Siena Anstis. "Weaponized Words: Uyghur Language Software Hijacked to Deliver Malware," *The Citizen Lab* (April 28, 2025) <<https://citizenlab.ca/research/uyghur-language-software-hijacked-to-deliver-malware/>>

⁵⁶ Uyghur Human Rights Project (2020), "Kashgar Coerced: Forced Reconstruction, Exploitation, and Surveillance in the Cradle of Uyghur Culture," *UHRP* (June 3, 2020) <<https://uhrp.org/report/kashgar-coerced/>>.

⁵⁷ Oiwan Lam (2016), "Leaked Xinjiang Police Report Describes Circumvention Tools as 'Terrorist Software'," *Global Voices Advox* (October 26, 2016) <<https://advox.globalvoices.org/2016/10/26/leaked-xinjiang-police-report-describes-circumvention-tools-as-terrorist-software/>>

⁵⁸ Darren Byler (2019), "Ghost World," *Logic(s)* (May 1, 2019) <<https://logicmag.io/china/ghost-world/>>.

D) Social Engineering and Phishing: Social engineering is the process of manipulating individuals into taking actions that result in the disclosure of sensitive information, break security procedures, or result in the installation of malware or spyware onto a device. Phishing is a specific type of social engineering commonly leveraged in China-sponsored campaigns. With phishing, an email or direct message is sent to a targeted individual that contains a malicious link. Clicking on the link will take a recipient to an often benign looking site that can profile the individual, steal credentials, or install additional malicious programs. Phishing emails and messages often feature a personalized hook designed to be of interest to the targeted individual. Information for these “lures” is often obtained through social media monitoring or information gathering conducted via account takeovers. When targeting members of civil society, lures can include fake human rights reports, invitations to a conference, leaked documents exposing human rights violations, or community events.

To trick recipients into clicking on malicious links, attackers may claim to be journalists, fellow activists, or high profile individuals. The social engineering preparations for such attacks can extend over an exchange of several messages or a shift between different channels of communication (e.g., from email to Signal messenger) before the attackers include a compromised file or link. This intersection of phishing and impersonation is documented in a recent report highlighting the targeting of a senior member of a Canada-based Uyghur non-profit organization.⁵⁹

B. Offline techniques

In addition to online techniques, Chinese authorities and their proxies also use a variety of offline techniques to surveil Chinese citizens and diaspora members in Canada and around the world, including by stalking targeted individuals.⁶⁰ Online and offline monitoring can work hand in hand. Information gathered about a person online, or through digital means like phishing attacks, can be used for the purpose of intimidating that individual offline, and vice

⁵⁹ Rebekah Brown, Maia Scott, Marcus Michaelsen, Emile Dirks, and Francesca Thaler (pseudonym). “Tall Tales: How Chinese Actors Use Impersonation and Stolen Narratives to Perpetuate Digital Transnational Repression,” *The Citizen Lab* (April 27, 2026)

<<https://citizenlab.ca/research/how-chinese-actors-use-impersonation-and-stolen-narratives-to-perpetuate-digital-transnational-repression/>>

⁶⁰ Elizabeth Thompson and Aloysius Wong (2025), “Followed, threatened and smeared — attacks by China against its critics in Canada are on the rise,” *CBC News* (May 29, 2025)

<<https://www.cbc.ca/news/politics/china-targets-dissidents-canada-1.7543745>>.

versa. Chinese authorities or their proxies may also use digital platforms to threaten targeted individuals with offline physical and sexual violence.⁶¹

Offline monitoring can take the form of documenting participants in public gatherings. Many Chinese citizens and diaspora members in Canada exercise their rights to speech and assembly by joining protests against the Chinese government, including demonstrations held outside Chinese diplomatic offices. During demonstrations Chinese authorities associated with diplomatic offices or their proxies have reportedly attempted to photograph and identify protest participants.⁶² State-backed actors have in turn used this information to threaten targeted individuals online. For example, exiled activists in Canada who were photographed at pro-democracy protests for Hong Kong were later subjected to doxxing campaigns, in which their photographs, names, email addresses, and phone numbers were shared widely in WeChat groups alongside inciting messages.⁶³ Consequently, these campaigns resulted in strangers approaching targets in the streets, photographing them, or tailing them in the streets.⁶⁴ In other cases, the home addresses of Uyghur and Chinese activists in Canada were published online as part of wider campaigns of digital harassment.⁶⁵ Doxxing of this kind can in turn encourage further waves of on- or offline harassment.

⁶¹ Noura Aljizawi, Siena Anstis, Marcus Michaelson, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybullu, Muetter Iliq, Nicola Lawford, Émilie LaFlèche, Gabrielle Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), “No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression,” *The Citizen Lab* (December 2, 2024)

<<https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>>

⁶² Amnesty International (2024), “Students at Canadian Universities Face Surveillance, Harassment,” *Amnesty International* (May 12, 2024)

<<https://amnesty.ca/human-rights-news/students-canadian-universities-surveillance-harassment-chinese-state-authorities/>>.

⁶³ Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). “Psychological and Emotional War: Digital Transnational Repression in Canada,” *The Citizen Lab* (March 1, 2022).

<<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>

⁶⁴ Global News, “Cherie Wong describes threats she’s faced while advocating for Hong Kong, intimidation from Chinese government,” *Global News* (March 31, 2021)

<<https://globalnews.ca/video/7732233/cherie-wong-describes-threats-shes-faced-while-advocating-for-hong-kong-intimidation-from-chinese-government/>>.

⁶⁵ Noura Aljizawi, Siena Anstis, Marcus Michaelson, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybullu, Muetter Iliq, Nicola Lawford, Émilie LaFlèche, Gabrielle Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), “No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression,” *The Citizen Lab* (December 2, 2024)

<<https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>>

Offline monitoring can also occur outside protest events. Chinese citizens and diaspora members in Canada who participate in public events about Chinese politics, human rights, or other similar issues are also vulnerable to surveillance. Those behind offline surveillance activities are not only Chinese authorities but also supporters of the Chinese government. Proxies on university campuses in Canada and the U.S. have reported Chinese students and diaspora activists to Chinese diplomatic offices or authorities inside China.⁶⁶ These individuals may not work under direct orders from Chinese authorities. Instead, these people may have self-selected to report on the activities of overseas Chinese citizens or diaspora members. Whether or not proxies operate directly at the behest of Chinese authorities, their monitoring of fellow Chinese citizens or diaspora members can have a profoundly chilling effect on both targets and other overseas Chinese citizens and diaspora members.⁶⁷

In other cases, offline surveillance and state repression inside China can fuel on- and offline monitoring in Canada. Information gathered by authorities inside China can in turn be used to initiate digital threats against targets overseas. For example, the arrest of activists in Hong Kong and the confiscation by police of their devices has allowed Hong Kong authorities to access online activist coordination groups and gather information about activists in Hong Kong and abroad, including people in Canada.⁶⁸ Human Rights Watch has documented how police in Xinjiang have used the application known as the Integrated Joint Operations Platform (IJOP) to collect information from Uyghurs and other non-Han people in Xinjiang,

⁶⁶ Justin Mowat (2019), “McMaster student government bans Chinese students' group from campus,” *CBC News* (September 26, 2019)

<<https://www.cbc.ca/news/canada/hamilton/mcmaster-china-student-association-ban-1.5298882>>; Sebastian Rotella (2021), “Even on U.S. Campuses, China Cracks Down on Students Who Speak Out,” *Propublica* (November 30, 2021)

<https://www.propublica.org/article/even-on-us-campus-china-cracks-down-on-students-who-speak-out>;

U.S. Attorney’s Office District of Massachusetts (2024), “Berklee College of Music Student Convicted of Stalking, Threatening Individual Promoting Democracy in China,” *U.S. Department of Justice* (January 25, 2024)

<<https://www.justice.gov/usao-ma/pr/berklee-college-music-student-convicted-stalking-threatening-individual-promoting>>; CBC (2019), “Toronto police investigating online abuse of student leader at U of T,”

CBC News (February 28, 2019)

<<https://www.cbc.ca/news/canada/toronto/toronto-police-investigating-online-abuse-tibetan-canadian-student-chemi-lhamo-1.5038517>>.

⁶⁷ Amnesty International (2024), “Students at Canadian Universities Face Surveillance, Harassment,” *Amnesty International* (May 12, 2024)

<<https://amnesty.ca/human-rights-news/students-canadian-universities-surveillance-harassment-chinese-state-authorities/>>

⁶⁸ Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). “Psychological and Emotional War: Digital Transnational Repression in Canada,” *The Citizen Lab* (March 1, 2022).

<<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>

including information about relatives and family members abroad, such as how they communicate and what phone numbers their overseas relatives use.⁶⁹

The rapid spread of artificial intelligence (AI) will likely make digital transnational repression worse, including in Canada.⁷⁰ Large language models (LLMs) and other AI-enabled tools can rapidly deanonymize social media users, speeding the synthesis of large amounts of data, and enable AI-driven surveillance.⁷¹ Although there are no documented cases yet of AI-powered China-sponsored digital surveillance against exiled activists in Canada, Anthropic's latest threat report provides examples of how China is using AI to enhance its campaigns of transnational surveillance.⁷²

Chinese State Surveillance Actors: State Agencies and Proxies

Numerous Chinese government agencies and state-backed proxies take part in monitoring Chinese citizens and diaspora members in Canada. This multi-actor approach to overseas surveillance is indicative of the high priority the Chinese government places on silencing dissent abroad. It also reflects the Chinese government's tactics of domestic political control, which combine the use of police and other security officers⁷³, hired thugs⁷⁴, neighbourhood informants⁷⁵, and diverse forms of digital surveillance.⁷⁶

⁶⁹ Human Rights Watch (2019), "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," *Human Rights Watch* (May 1, 2019) <<https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mas>>

⁷⁰ Emile Dirks, Shaila Baran, Emma Dickinson, and Andre Fajardo (2026), "Transnational Repression in the Age of Upheaval: Global Policy Changes for Canada," *The Citizen Lab* (March 11, 2026) <<https://citizenlab.ca/research/transnational-repression-in-the-age-of-upheaval-global-policy-changes-for-canada/>>

⁷¹ Ron Deibert (2026), "The Coming Tsunami of Transnational Repression," *The Citizen Lab* (March 12, 2026) <<https://citizenlab.ca/canadians-face-tsunami-of-transnational-repression-in-coming-years/>>.

⁷² Anthropic (2026), "Detecting and countering misuse of AI: September 2026," *Anthropic* (September 10, 2026) <<https://www.anthropic.com/threat-intelligence-report-september-2026#surveillance-operations-sep-26>>.

⁷³ Suzanne Scoggins (2021), *Policing China: Street-level Cops in the Shadow of Protest*, New York: Cornell University Press

⁷⁴ Lynette Ong (2022), *Outsourcing Repression: Everyday State Power in Contemporary China*, Oxford: Oxford University Press

⁷⁵ Minxin Pei (2024), *The Sentinel State: Surveillance and the Survival of Dictatorship in China*, Cambridge: Harvard University Press

⁷⁶ Josh Chin and Liza Lin (2023), *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*, New York: St. Martin's Publishing Group.

Chief among the state agencies involved in overseas surveillance and transnational repression are China's national police force the Ministry of Public Security (MPS) and China's intelligence agency the Ministry of State Security (MSS), as well as their respective local- and provincial-level offices. Multiple party-state offices have also participated in Operation Fox Hunt and Operation Sky Net, the overseas extensions of the Communist Party's domestic anti-corruption campaign, including the MPS, the Supreme People's Court, the Supreme People's Procuratorate, the People's Bank of China, and the Organization Department of the Communist Party.

Particular campaigns of overseas surveillance and transnational repression can involve specific government agencies. For example, since the 2019-2020 Hong Kong protest movement, the Hong Kong Police Force has played a central role in monitoring overseas Hong Kong activists, including individuals who the Hong Kong government accuses of violating the National Security Law or Article 23 of the Basic Law. Hong Kong police officers, like their counterparts in the MPS, have threatened Hong Kong activists in Canada and other countries via phone or video calls.⁷⁷ Social media campaigns, directed at overseas Chinese-speaking audiences and likely conducted with state backing, have used disinformation and the promise of monetary rewards to encourage users to provide information on exiled Hong Kong activists and diaspora members living in Canada.⁷⁸

Chinese authorities have also recruited people in North America and Europe, including both diaspora and non-diaspora members, to monitor and even threaten targeted Chinese citizens and diaspora members. As part of Operation Fox Hunt, Chinese authorities have tasked proxies in the United States—including a former U.S. law enforcement officer—with monitoring and threatening specific individuals.⁷⁹ Such threats against overseas Chinese citizens accused

⁷⁷ Robert Fife (2024), "Hong Kong police make threatening phone call to pro-democracy supporter living in Canada," *The Global and Mail* (May 27, 2024)

<<https://www.theglobeandmail.com/politics/article-hong-kong-police-intimidation-canada/>>.

⁷⁸ Global Affairs Canada (2026), "G7 members and others targeted in PRC-linked information operation," *Government of Canada* (May 11, 2026).

<<https://international.canada.ca/en/global-affairs/corporate/reports/rapid-response-mechanism/news/2025-china-operation>>.

⁷⁹ United States Attorney's Office Eastern District of New York (2023), "Federal Jury Convicts Three Defendants of Interstate Stalking of Chinese Nationals in the U.S. and Two of Those Defendants for Acting or Conspiring to Act on Behalf of the People's Republic of China," *U.S. Department of Justice* (June 20, 2023)

<<https://www.justice.gov/usao-edny/pr/federal-jury-convicts-three-defendants-interstate-stalking-chinese-nationals-us-and>>; Office of Public Affairs (2025), "Leader of Multi-Year 'Operation Fox Hunt' Repatriation Campaign Directed by the People's Republic of China Sentenced to 20 Months in Prison," *U.S. Department of Justice* (March 19, 2025)

<<https://www.justice.gov/opa/pr/leader-multi-year-operation-fox-hunt-repatriation-campaign-directed-peoples-republic-china>>.

of official malfeasance are intended to bypass formal bilateral extradition requests and instead use intimidation to compel the individual to return to China and surrender to local authorities.

In addition to the global anti-corruption campaign, Chinese authorities have also recruited members of overseas dissident organizations to act as informants. These proxies leverage their trusted credentials within activist circles to collect information on fellow community members, which is subsequently turned over to contacts in China's security services.⁸⁰ Chinese authorities have also attempted to enlist members of persecuted ethnic and religious communities to act as overseas informants. For example, police in Xinjiang have offered to provide Uyghurs with passports in exchange for promises that they would act as spies in Canada.⁸¹

Other proxies have included individuals affiliated with the Communist Party's united front system. The united front is a decades-old network of Chinese government offices and civil society organizations aimed at increasing support for the Communist Party among key non-Party individuals and constituencies inside and outside China.⁸² Most overseas united front-affiliated organizations in Canada and other countries are not involved in transnational repression and instead are focused on non-coercive influence operations within Chinese diaspora communities which aim to build consent for the Chinese government and its preferred political narratives. In notable cases, however, individuals affiliated with specific united front-linked organizations in North America have been implicated in efforts to monitor and harass overseas Chinese citizens and diaspora members. These operations have included organizing counter-demonstrations in response to local protests against the Communist Party

⁸⁰ Jake Offenhartz (2025), "Chinese dissident who led pro-democracy group in NYC pleads guilty to spying for Beijing," *AP News* (September 16, 2025) <https://apnews.com/article/chinese-dissident-nyc-spying-prodemocracy-9a19aeed01ce3dafc7bcfda2f91f8c2>; Scilla Alecci (2025), "Purported dissident who monitored Chinese activists in Germany convicted of espionage," *International Consortium of Investigative Journalists* (October 2, 2025) <https://www.icij.org/investigations/china-targets/purported-dissident-who-monitored-chinese-activists-in-germany-convicted-of-espionage/>.

⁸¹ Uyghur Human Rights Project (2021), "'Your Family Will Suffer': How China is Hacking, Surveilling, and Intimidating Uyghurs in Liberal Democracies," *Uyghur Human Rights Project* (November 10, 2021) <https://uhrp.org/report/your-family-will-suffer-how-china-is-hacking-surveilling-and-intimidating-uyghurs-in-liberal-democracies/>.

⁸² Alex Joske (2020), "The Party Speaks for You: Foreign Interference and the Chinese Communist Party's United Front System," *Australian Strategic Policy Institute* (June 9, 2020) <https://www.aspi.org.au/report/party-speaks-you/>.

and Xi Jinping, as well as providing Chinese diplomatic offices or Chinese security officials with information on overseas critics of the Chinese government.⁸³

In addition to overseas proxies, Chinese authorities have contracted private companies inside China to assist them with monitoring overseas opponents of the Communist Party. These companies may assist Chinese security offices with monitoring the online activities of overseas Chinese citizens and diaspora members for anti-Communist Party sentiment. Private actors are also suspected of assisting Chinese authorities in collecting information on select overseas Chinese citizens via targeted phishing campaigns.⁸⁴ These phishing campaigns can vary from imitating login security alerts from large tech companies, to impersonating a target's colleague. In these cases, private actors attempt to steal the target's login credentials and if successful, pass the login information on to other teams to use. Criminal investigations in Taiwan have found that contracting companies provided access to social media and messaging accounts for use in these social engineering attacks, and that these contracting companies were acting "under the direction of the Chinese Communist Party's cyber army unit."⁸⁵

Question 2

Are you aware of any adverse treatment perpetrated by Chinese authorities against the China-based families of Chinese citizens in Canada?

If so, can you describe the nature of this treatment, including how and where it takes place in China?

⁸³ Shibani Mahtani, Meg Kelly, Cate Brown, Cate Cadell, Ellen Nakashima, and Chris Dehghanpoor (2024), "How China Extends its Repression into an American City," *The Washington Post* (September 3, 2024) <https://www.washingtonpost.com/world/interactive/2024/chinese-communist-party-us-repression-xi-jinping-appeal/>; Office of Public Affairs (2026), "Bronx Man Convicted of Operating Police Station for the Chinese Government in New York City and Obstruction of Justice," *U.S. Department of Justice* (May 13, 2026) <https://www.justice.gov/opa/pr/bronx-man-convicted-operating-police-station-chinese-government-new-york-city-and-justice>.

⁸⁴ Rebekah Brown, Maia Scott, Marcus Michaelsen, Emile Dirks, and Francesca Thaler (pseudonym). "Tall Tales: How Chinese Actors Use Impersonation and Stolen Narratives to Perpetuate Digital Transnational Repression," *The Citizen Lab* (April 27, 2026). <https://citizenlab.ca/research/how-chinese-actors-use-impersonation-and-stolen-narratives-to-perpetuate-digital-transnational-repression/>.

⁸⁵ Scilla Alecci. "Taiwanese authorities charge executives who helped China's cyber spies target ICIJ network", *International Consortium of Investigative Journalists (ICIJ)* (July 7, 2026) <https://www.icij.org/investigations/china-targets/taiwanese-authorities-charge-executives-who-helped-chinas-cyber-spies-target-icij-network/>.

If so, can you describe the profile of individuals in Canada typically associated in such cases?

If so, can you describe the various Chinese state agencies involved in such treatment?

Coercion-by-Proxy

Chinese authorities are known to intimidate the China-based family members of Chinese citizens or diaspora members in Canada. This intimidation tactic is referred to as “coercion-by-proxy,” or the use of “domestic forms of repression as a means of punishing, threatening, or controlling those who reside overseas.”⁸⁶ The use of family intimidation to silence political dissent is not unique to the Chinese government’s campaigns of transnational repression, and inside China authorities have used similar forms of “relational repression” against Chinese citizens to dissuade their relatives from social or political activism.⁸⁷

As a tactic of transnational repression, coercion-by-proxy leverages China’s domestic political controls to undermine the ability of overseas Chinese citizens and diaspora members to freely exercise their civil and political rights, including their right to speech and assembly. Chinese authorities’ attempt to instill in exiles and diaspora members a sense of personal responsibility for the well-being of the family members in China, which in turn can have profoundly negative psychological and emotional impacts on targeted individuals.

Like other forms of overseas surveillance and transnational repression, numerous Chinese state offices and proxies participate in coercion-by-proxy. Chief among these offices are China’s domestic law enforcement and security agencies, including the MPS and the MSS and their respective provincial- or local-level offices, and the Hong Kong Police Force. In addition to these security offices, Chinese authorities have also enlisted proxies overseas, including Chinese citizens and diaspora members, as well as individuals outside of targeted diaspora communities, to communicate threats to overseas targets.

Coercion-by-proxy often takes the form of remote threats by China-based authorities to overseas targets, communicated via phone or video call, direct message, email, or other

⁸⁶ Fiona Adamson and Gerasimos Tsourapaas (2020), “At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression,” *Freedom House* (July 1, 2020) <<https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression>>.

⁸⁷ Yanhua Deng and Kevin J.O’Brien, “Relational Repression in China: Using Social Ties to Demobilize Protesters,” *The China Quarterly*, 215 (2013): 533-52.

digital communication platform. These threats are intended to demonstrate the Chinese government's control over a target's relatives in China, and to warn activists that continuing public advocacy against the Communist Party would further imperil the well-being of their family members. For example, prominent Uyghur activists in Canada have reported receiving phone calls from Chinese authorities, informing them of the health or even death of relatives detained in Xinjiang's complex of prisons and extrajudicial reeducation camps.⁸⁸ Social media monitoring can play a role in coercion-by-proxy, with Chinese authorities threatening family members in response to the online activities of their overseas relatives. Police in China are known to have contacted the family members of a Chinese citizen in Canada who used social media to post content critical of the Communist Party and Xi Jinping.⁸⁹

Coercion-by-proxy can also include legal threats against the family members of overseas targets. These threats leverage police investigations and criminal convictions to deter exiles and diaspora members from continuing to speak out against the Chinese government. Hong Kong police have questioned the family members of exiled Hong Kong activists living in Canada who are wanted on charges of violating national security legislation. These individuals include both Chinese citizens living in Canada applying for refugee status⁹⁰, and Canadian citizens with familial ties to Hong Kong who are journalists or Canadian federal election political candidates.⁹¹ Chinese authorities have also charged the relatives of exiles with seemingly non-political offenses. To silence a Canada-based critic of the Chinese

⁸⁸ Ashleigh Stewart, Jeff Semple and Stewart Bell (2023), "Canadians describe surveillance, intimidation and terror 'under China's shadow,'" *Global News* (April 5, 2023)

<<https://globalnews.ca/news/9601649/china-foreign-interference-spying/>>; House of Commons, Special Committee on Canada-China Relations, Evidence, 43rd Parl., 2nd Sess., Meeting 27 (May 31, 2021). <<https://www.ourcommons.ca/DocumentViewer/en/43-2/CACN/meeting-27/evidence>>.

⁸⁹ Joanna Chiu (2021), "A Chinese student in Canada had two followers on Twitter. He still didn't escape Beijing's threats over online activity," *Toronto Star* (Sept 18, 2021) <https://www.thestar.com/news/canada/a-chinese-student-in-canada-had-two-followers-on-twitter-he-still-didn-t-escape/article_6800d3f1-38e6-5c6f-a551-ea4d9f500997.html>.

⁹⁰ John Mackie (2025), "Scare tactic or dangerous threat? Hong Kong activists living in B.C. react to police bounties," *Vancouver Sun* (July 28, 2025) <<https://vancouver.sun.com/news/scare-tactic-or-dangerous-threat-hong-kong-activists-living-in-bc-react-to-police-bounties>>.

⁹¹ CBC (2025), "Hong Kong has issued a warrant for his arrest, but this Vancouverite isn't worried," *CBC News* (July 29, 2025) <<https://www.cbc.ca/news/canada/british-columbia/victor-ho-hong-kong-arrest-warrant-1.7596560>>; Hillary Leung (2025), "Hong Kong police take in relatives of wanted activist Joe Tay for questioning," *Hong Kong Free Press* (May 8, 2025) <<https://hongkongfp.com/2025/05/08/hong-kong-police-take-in-relatives-of-wanted-activist-joe-tay-for-questioning/>>.

government, Chinese authorities charged his son and sister with bribery.⁹² In this case, the detention of family members was combined with legal threats against the Canada-based target, with Chinese authorities requesting an Interpol red notice be issued for the individual on the grounds that he was under investigation for bribery.⁹³

For exiles and diaspora members, the emotional and psychological impact of coercion-by-proxy can be devastating. Chinese authorities use family separation as means of applying pressure to exiles and diaspora members.⁹⁴ In response, overseas Chinese citizens and diaspora members have cut off ties with family members in China, in an attempt to protect their relatives from the threat of coercion-by-proxy.⁹⁵ Despite facing these threats, some overseas Chinese citizens and diaspora members maintain contact with people in China. Social media platforms like Facebook and WhatsApp are inaccessible in China without the use of a virtual private network (VPN), so connections between exiles or diaspora members and relatives in China are often mediated through China-based platforms like WeChat, which are subject to strict content moderation and government-enforced censorship.⁹⁶ Overseas Chinese citizens may also be compelled by circumstance to maintain contact with Chinese diplomatic offices, for example in order to renew passports or other travel documents. Chinese authorities may continue to exploit these connections in order to put pressure on targeted individuals or their family members.

⁹² Nathan Vanderklippe (2018), “China admits to having agents in Canada as former judge harassed in Toronto,” *The Global and Mail* (January 15, 2018) <<https://www.theglobeandmail.com/news/world/china-admits-to-having-agents-in-canada-as-former-judge-harassed-in-toronto/article37616456/>>.

⁹³ Human Rights Watch (2018), “China: Families of Interpol Targets Harassed,” *Human Rights Watch* (January 31, 2018) <<https://www.hrw.org/news/2018/02/01/china-families-interpol-targets-harassed>>.

⁹⁴ Uyghur Human Rights Project (2026), “Fading Ties: Uyghur Family Separation as a Tool of Transnational Repression,” *UHRP* (February 23, 2026) <<https://uhrp.org/report/fading-ties-uyghur-family-separation-as-a-tool-of-transnational-repression/#KeyTakeaways>>.

⁹⁵ House of Commons, Special Committee on Canada-China Relations (2021), “Evidence, 43rd Parl., 2nd Sess., Meeting 27,” *House of Commons Canada* (May 31, 2021) <<https://www.ourcommons.ca/DocumentViewer/en/43-2/CACN/meeting-27/evidence>>; Amnesty International (2024), “China: Overseas students face harassment and surveillance in campaign of transnational repression,” *Amnesty International* (May 13, 2024) <<https://www.amnesty.org/en/latest/news/2024/05/china-overseas-students-face-harassment-and-surveillance-in-campaign-of-transnational-repression/>>.

⁹⁶ Jeffrey Knockel, Christopher Parsons, Lotus Ruannon-Chinese-registered, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert (2020), “We Chat, They Watch: How International Users Unwittingly Build up WeChat’s Chinese Censorship Apparatus,” *The Citizen Lab* (May 7, 2020) <<https://citizenlab.ca/research/we-chat-they-watch/>>; Emile Dirks (2024), “Citizen Lab submission to the Congressional-Executive Commission on China about the State of Human Rights in China,” *The Citizen Lab* (April 2, 2024) <<https://citizenlab.ca/citizen-lab-submission-to-the-congressional-executive-commission-on-china-about-the-state-of-human-rights-in-china/>>.

Appendix: List Of Cited Citizen Lab Reports

The following is a list of relevant Citizen Lab reports cited in this submission and brief summaries of their contents.

Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2020). “Psychological and Emotional War: Digital Transnational Repression in Canada,” *The Citizen Lab* (March 1, 2022)

<<https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>>

- Describes how activists and dissidents living in Canada are impacted by digital transnational repression.

Noura Aljizawi, Siena Anstis, Marcus Michaelson, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybullayeva, Muetter Iliquid, Nicola Lawford, Émilie LaFlèche, Gabrielle Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), “No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression,” *The Citizen Lab* (December 2, 2024)

<<https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>>

- Examines how gender and sexuality play a central role in digital transnational repression.

Mohammed Al-Maskati, Bill Marczak, Siena Anstis, and Ron Deibert (2022), “Peace through Pegasus: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware,” *The Citizen Lab* (April 5, 2022)

<<https://citizenlab.ca/research/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/>>

- Examines the use of Pegasus spyware against four Jordanian human rights defenders.

Siena Anstis, Tristan Surman, Noura Aljizawi, Marcus Michaelson, and Ron Deibert (2026), “Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the Committee on Enforced Disappearances and the Working Group on Enforced or Involuntary Disappearances,” *The Citizen Lab* (January 31, 2026)

<<https://citizenlab.ca/wp-content/uploads/2026/02/Submission-The-Citizen-Lab-30-January-2026-Call-for-inputs-on-Enforced-Disappearances-in-the-context-of-transnational-repression.pdf>>

Examines how digital transnational repression facilitates transnational enforced disappearances.
Rebekah Brown, Marcus Michaelson, Matt Brooks, and Siena Anstis (2025), “Weaponized Words: Uyghur Language Software Hijacked to Deliver Malware,” <i>The Citizen Lab</i> (April 28, 2025) <https://citizenlab.ca/research/uyghur-language-software-hijacked-to-deliver-malware/> Examines a spearphishing campaign that targeted senior members of the World Uyghur Congress in March 2025.
Rebekah Brown, Maia Scott, Marcus Michaelson, Emile Dirks, and Francesca Thaler (2026), “Tall Tales: How Chinese Actors Use Impersonation and Stolen Narratives to Perpetuate Digital Transnational Repression,” <i>The Citizen Lab</i> (April 27, 2026) <https://citizenlab.ca/research/how-chinese-actors-use-impersonation-and-stolen-narratives-to-perpetuate-digital-transnational-repression/> Examines two distinct actors aligned with the People’s Republic of China that targeted and impersonated journalists and civil society members.
Ron Deibert (2026), “Canadians Will Face ‘Tsunami’ of Transnational Repression in Coming Years,” <i>The Citizen Lab</i> (March 23, 2026) <https://citizenlab.ca/canadians-face-tsunami-of-transnational-repression-in-coming-years/> Highlights digital transnational repression and its impacts on targets and civil society, and warns about how AI will be deployed to increase the volume and sophistication of digital transnational repression.
Emile Dirks (2024), “Citizen Lab submission to the Congressional-Executive Commission on China about the State of Human Rights in China,” <i>The Citizen Lab</i> (April 2, 2024) <https://citizenlab.ca/citizen-lab-submission-to-the-congressional-executive-commission-on-china-about-the-state-of-human-rights-in-china/> Examines Chinese government-backed online censorship and its impact on the freedom of expression and opinion of people accessing the internet from within China or using China accessible online platforms
Emile Dirks (2022), “Mass DNA Collection in the Tibet Autonomous Region from 2016–2022,” <i>The Citizen Lab</i> (September 13, 2022) <https://citizenlab.ca/research/mass-dna-collection-in-the-tibet-autonomous-region/>

Examines mass DNA collection in the Tibet Autonomous Region.
Emile Dirks, Shaila Baran, Emma Dickinson, and Andre Fajardo (2026), “Transnational Repression in the Age of Upheaval: Global Policy Changes for Canada,” <i>The Citizen Lab</i> (March 11, 2026) https://citizenlab.ca/research/transnational-repression-in-the-age-of-upheaval-global-policy-changes-for-canada/ Argues that the Canadian government must do more to protect diaspora members from transnational repression.
Emile Dirks, Sarah McKune, Nate Schenkkan, Sydney Smythe, and Yaqiu Wang (2026), “Submission to the Committee on Enforced Disappearances and the Working Group on Enforced and Involuntary Disappearances on the enforced disappearance of migrants in the context of transnational repression,” <i>The Citizen Lab</i> (January 31, 2026) https://citizenlab.ca/wp-content/uploads/2026/02/Submission The-Citizen-Lab 31-January-2026 Call-for-inputs-on-Enforced-Disappearances-in-the-context-of-transnational-repression.pdf Examines the vulnerability of migrants to enforced disappearances via unlawful deportations and forced renditions in the context of transnational repression.
Miles Kenyon (2020), “WeChat Surveillance Explained,” <i>The Citizen Lab</i> (May 7, 2020) https://citizenlab.ca/research/we-chat-they-watch/wechat-surveillance-explained/ Provides a summary of the research findings of the “We Chat, They Watch” report and questions and answers from the research team.
Jeffrey Knockel, Christopher Parsons, Lotus Ruannon-Chinese-registered, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert (2020), “We Chat, They Watch: How International Users Unwittingly Build up WeChat’s Chinese Censorship Apparatus,” <i>The Citizen Lab</i> (May 7, 2020) https://citizenlab.ca/research/we-chat-they-watch/ Examines how WeChat communications conducted among non-China-registered accounts are subject to pervasive content surveillance.
Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert (2019), “Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits,” <i>The Citizen Lab</i> (September 24, 2019) https://citizenlab.ca/research/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/ Examines the use of one-click mobile exploits used to target Tibetan groups.

Morgan Marquis-Boire (2014), “Schrodinger’s Cat Video and the Death of Clear-Text,” *The Citizen Lab* (August 15, 2014)

<<https://citizenlab.ca/research/cat-video-and-the-death-of-clear-text/>>

- Examines two products sold for facilitating targeted surveillance known as network injection appliances.