PRC Foreign Interference and Transnational Repression in Canada:

Insights from Vulnerable Diaspora Communities

Marcus Kolga, Sze-Fung Lee, and Sarah Teich

Foreign Interference Resilience & Education
An initiative by Digital Public Square

disinfowatch

DIGITAL PUBLIC SQUARE

About

Digital Public Square is a Toronto-based not-for-profit whose objective is to rethink and redesign the way technology is used to support communities worldwide. We find ways for communities to engage in healthy debate, share knowledge, and co-create solutions to their most pressing challenges. Over the past decade, Digital Public Square has created space for tens of millions of people around the world to interact with our platforms. Our products have been deployed in a wide range of contexts, from countering misinformation in North America to increasing knowledge of labor rights in Asia and strengthening election integrity in Africa.

Marcus Kolga is the founder and director of DisinfoWatch, a leading Canadian platform dedicated to monitoring and debunking foreign disinformation. As an expert in digital communications, global human rights, sanctions, disinformation, and cybersecurity, Marcus leverages his expertise to combat foreign influence operations. DisinfoWatch relies on open-source data, contributions from an international network of journalists, civil society organizations, analysts, and some automated tools. This information is analyzed and exposed to raise awareness about foreign operations and to build long-term resilience against foreign information and influence campaigns. The platform's core mission is to enhance public understanding of foreign information operations by uncovering who produces it, who amplifies it, why it is created, how to recognize it, and how to prevent its spread.

Sze-Fung Lee is an independent researcher specializing in Chinese hybrid warfare, including Foreign information manipulation and interference (FIMI), grand strategy, nuclear proliferation, gray zone tactics, and cognitive warfare. Zir research also focuses on Indo-Pacific security policy, challenges posed by emerging technologies, and the politics of Hong Kong.

Sarah Teich is an award-winning international human rights lawyer based in Toronto. She advises various organizations including Tamil Rights Group, the Association of Victims of Flight PS752 Families, United Tegaru Canada, Secure Canada, and Uyghur Rights Advocacy Project, helping them utilize domestic, foreign, and international mechanisms to seek justice and accountability for atrocity crimes and human rights abuses committed by state and non-state actors around the world.

Research for this report was supported by Heritage Canada's Digital Citizen Contribution Program.

This project has been made possible in part by the Government of Canada. Ce projet a été rendu possible en partie grâce au gouvernement du Canada.

Canada

Executive Summary

This report examines the People's Republic of China's (PRC) interference in Canada, focusing on its efforts to disrupt democratic processes, violate sovereign information spaces, and carry out transnational repression (TNR) in Canada against communities, groups, and individuals who are critical of PRC policies. Drawing on insights from leaders of Canadian Uyghur, Tibetan, Hong Kong, Taiwanese, and Falun Gong communities, it highlights Beijing's use of intimidation, disinformation, and diaspora manipulation to advance its authoritarian agenda and silence critics.

The PRC's transnational repression and foreign information manipulation and interference (FIMI) campaigns are a significant threat to Canada. Through TNR, the PRC targets activists, diaspora leaders, and critics of its regime with harassment, intimidation, and surveillance. These tactics often involve threats against family members in China, online harassment, and the use of platforms like WeChat to monitor and coerce individuals in Canada. The pervasive nature of these operations creates an atmosphere of fear, undermining the freedom and security of targeted communities.

Beijing's FIMI operations aim to influence public opinion, discredit critics, and promote favorable narratives about China. By leveraging state-controlled media and social media applications, diaspora-targeted propaganda, and coordinated disinformation campaigns, the PRC seeks to undermine Canadian democratic values and violate our cognitive sovereignty by manipulating our collective understanding of PRC efforts to suppress ethnic minority rights, cultures, and basic human rights.

Central to the PRC's strategy is the United Front Work Department (UFWD), a powerful agency tasked with influencing overseas Chinese communities and advancing the Chinese Communist Party's (CCP) objectives. Through cultural associations, media collaborations, and grassroots infiltration, the UFWD amplifies pro-China narratives, suppresses dissent, and aligns diaspora groups with the CCP's agenda. This sophisticated network enables Beijing to carry out influence operations while masking its role behind ostensibly independent organizations.

Despite efforts to address these challenges, significant gaps remain in Canada's policy and enforcement responses. While measures like Bill C-70 and the Foreign Influence Transparency and Accountability

Act (FITAA) represent progress, they are limited by a lack of clear definitions for foreign interference and TNR. In addition, enforcement challenges and fragmented response frameworks hinder Canada's ability to effectively counter these covert operations.

To address these threats, the report makes recommendations to strengthen legislation and community resilience. Clear definitions of foreign interference and TNR are essential for creating effective legal tools to identify and disrupt these activities. A comprehensive kill chain framework is proposed to systematically counter PRC operations, enabling government, law enforcement, civil society, and Canada's democratic allies to both individually and collaboratively address threats at every stage of their development and execution.

Support for vulnerable communities is equally critical. Enhancing digital security training, providing accessible law enforcement reporting mechanisms, and establishing networks to support victims of TNR are necessary steps to empower and defend those targeted by Beijing's tactics. Coordination and partnerships with civil society organizations and community groups are critically important to helping prevent, disrupt, and deter TNR and FIMI operations targeting Canadians.

Introduction

PRC information and influence operations represent one of the most significant foreign interference threats to Canada today, according to the National Security and Intelligence Committee of Parliamentarians (NSICOP).

As the latest NSICOP Special Report on Foreign Interference in Canada's Democratic Processes and Institutions has revealed, some elected officials, including parliamentary members, have been wittingly assisting foreign state actors on Canadian soil.

Foreign interference is defined in the NSICOP report as foreign-influenced activities "within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."[1] This includes foreign states' or proxies' attempts to influence policies, intimidate officials, and/or steer public opinion toward their favoured conditions while undermining Canada's interests and national security. These operations have also been broadly defined as foreign information manipulation and interference (FIMI) by the European External Action Service.[2]

Another component of foreign interference is transnational repression (TNR). TNR refers to the actions of foreign governments reaching beyond their borders to intimidate, silence, coerce, harass, or harm members of their diaspora communities, to control them and silence critics—whether they be activists, journalists, or officials.[3] Although not a new tactic, TNR has been intensified by technology and increasingly aggressive authoritarian regimes like China, posing a growing threat globally, including in Canada.

Foreign interference, including FIMI and TNR, is a daily assault on civilians everywhere — including in democracies like the United States, United Kingdom, Canada, Germany, Australia, and South Africa.

The People's Republic of China's (PRC) FIMI operations in Canada range from short-term tactical objectives to long-term strategic goals.

Tactically, the PRC seeks to sway ethnocultural groups, impede parliamentary processes, and block criticism of its domestic policies, including human rights abuses.[4]

Strategically, Beijing aims to cultivate a positive or neutral image of itself within Canada while discouraging criticism of its authoritarian regime. This approach often leverages

[1] National Security and Intelligence Committee of Parliamentarians (NSICOP). 2024. 'Special Report on Foreign Interference in Canada's Democratic Processes and Institutions'. June 3, 2024. Available at: https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/intro-en.html

[2] European External Action Service, FIMI - Foreign Information Manipulation and Interference: Threat Report 2023, (Brussels: European External Action Service, 2023), https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

[3] Freedom House, Transnational Repression: A Global Problem, accessed November 26, 2024, https://freedomhouse.org/report/transnational-repression.

[4] Ibid

Canada's significant Chinese diaspora—1.71 million Canadians of Chinese origin as of the 2021 census[5]—viewing them both as an opportunity to exert influence within Canada and as a potential threat to the regime's stability.

Among the targets of PRC influence operations and TNR are Uyghur, Tibetan, Hong Kong, Taiwanese, and Falun Gong communities[6]; and elected officials and activists in Canada who support and advocate for them[7]. Many members of these groups are critical of the PRC's actions, and face intense pressure through surveillance, intimidation, and disinformation campaigns as part of Beijing's broader strategy of TNR.

Drawing on interviews with 25 leaders from communities that are vulnerable to PRC TNR in Canada—many of whom have been targeted for their community leadership and activism for years—we explore the PRC's foreign interference tactics targeting Canadian minority ethnocultural communities. Their experiences highlight the sophisticated and wide-reaching nature of Beijing's influence operations, as well as significant gaps in Canada's policy responses.

The recommendations in this report outline a framework and targeted kill chain[8], which details the tactics, techniques, and procedures employed by the PRC, its proxies, and enablers to carry out TNR against vulnerable communities in Canada. Each tactic and step includes proposed countermeasures aimed at preventing, disrupting, and deterring foreign interference, including FIMI and TNR.

PRC Foreign Information Manipulation and Interference (FIMI) in Canada

The PRC conducts extensive foreign interference operations in Canada through a range of PRC bodies, including the Ministry of State Security (MSS), Ministry of Public Security (MPS), and the Cyber Administration of China (CAC). The United Front Work Department (UFWD), the primary entity responsible for these operations, targets the overseas Chinese diaspora and other communities to advance Beijing's political goals. The UFWD, which reports directly to the Chinese Communist Party (CCP), focuses on suppressing groups deemed as threats to the PRC, including Uyghurs, Tibetans, Falun Gong practitioners, pro-democracy activists (including in Hong Kong), and Taiwanese independence advocates.[9]

[5] Statistics Canada. 2021. 'Census Profile, 2021 Census of Population'. Available at: https://www12.statcan.gc.ca/census-recensement/2021/dp-pd/prof/details/page.cfm

[6] Countering China's Global Transnational Repression Campaign: https://www.cecc.gov/events/hearings/countering-chinas-global-transnational-repression-campaign

[7] "Meet the Canadian lawmaker targeted by China" https://www.politico.com/news/2023/09/12/canadian-lawmaker-targeted-by-china-00115085

[8] A "kill-chain" is a phase-based model that identifies the stages of any kind of attack by an adversary

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

The United Front Work Department

The UFWD is a high-level governmental body that reports directly to the Central Committee of the CCP. It is composed of twelve specialized bureaus, each dealing with a "prioritized" target group that "threatens" PRC national security. These include residents of Hong Kong, Macau, and Taiwan, Chinese students studying abroad, ethnic and regional minorities (such as Uyghurs and Tibetans), as well as overseas Han Chinese communities.[10] The CCP labels Uyghurs, Tibetans, adherents of Falun Gong spiritual practices, pro-democracy activists, and those who advocate for the independence of Hong Kong and Taiwan as the "Five Poisons".

Chinese president Xi Jinping has described the UFWD as a "magic weapon" for safeguarding China's national security and interests, and for accomplishing the "great rejuvenation of the Chinese nation".[11] The UFWD operates through a network of front organizations, including Chinese student groups, cultural associations, media outlets, and business leaders, often concealing their ties to the CCP.[12]

These entities engage in lobbying, espionage, and/or political contributions, amplifying CCP narratives while undermining Canadian democratic processes. The PRC's influence is particularly visible in its infiltration of political parties[13] and coordination with local Canadian politicians. Some Canadian politicians have allegedly unknowingly or knowingly participated in activities that align with Beijing's interests, such as accepting disguised funds[14] or collaborating on electoral mobilization efforts.[15]

According to the Canadian Security Intelligence Service (CSIS), the UFWD has "established community organizations to facilitate influence operations against specific members of Parliament and infiltrated existing community associations to reorient them towards supporting CCP policies and narratives".[16]

A leaked CSIS report revealed that PRC operations have employed cyberattacks, bribery,

[10] Charon, Paul. and Jeangene Vilmer, Jean-Baptiste. 2021. Chinese Influence Operations—A Machiavellian Moment. The Institute for Strategic Research. Available at: https://www.irsem.fr/report.html

[11] People's Daily. 2024. 'Xi Jinping emphasized that this work is not outdated; it has become even more important!'. January 17, 2024. Available at: http://politics.people.com.cn/BIG5/n1/2024/0117/c1001-40160714.html

[12] Joske, "The Party Speaks for You"

[13] https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20200930/015/index-en.aspx

[14] Sam Cooper, "Canadian Intelligence Warned PM Trudeau That China Covertly Funded 2019 Election Candidates: Sources," Global News, November 7, 2022, https://globalnews.ca/news/9253386/canadian-intelligence-warned-pm-trudeau-that-china-covertly-funded-2019-election-candidates-sources/.

[15] National Security and Intelligence Committee of Parliamentarians (NSICOP), Special Report on Foreign Interference, June 3, 2024, sec. 164, https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf

[16] National Security and Intelligence Committee of Parliamentarians (NSICOP). 2024. 'Special Report on Foreign Interference in Canada's Democratic Processes and Institutions'. June 3, 2024. Available at: https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/intro-en.html

and "honey pot" schemes to compromise officials.[17] Some targeted individuals, including Canadian Members of Parliament, have been manipulated into providing privileged information or altering their political stances to align with PRC interests.[18] This cooperation undermines Canada's national security and democracy while bolstering the PRC's global influence.

PRC FIMI Objectives in Canada

In addition to these covert operations, PRC FIMI operations on social media aim to achieve two major objectives:

1. to promote a positive image of the PRC while rebuking Western allegations of human rights abuses; and

2. to steer public opinion, especially during critical events such as elections.

These efforts align with President Xi Jinping's strategy of "Telling China's story well," which seeks to enhance China's "international discourse power" by amplifying PRC-aligned narratives.[19]

For example, Chinese propaganda frequently depicts "happy Uyghurs" living peacefully in Xinjiang[20] to counter allegations of genocide. Other campaigns aim to confront foreign policy issues by spreading narratives such as "the U.S. and its allies provoked war in Ukraine,"[21] or "Taiwan is part of China."[22] These information operations not only aim to distort facts and spread disinformation but also seek to undermine support for oppressed communities. By saturating the information space with PRC-aligned messages, these operations create confusion, division, and doubt in Canadian society, thereby weakening support for democratic values and human rights.

[17] Fife, Robert and Chase, Steven. 2023. 'CSIS reports outline how China targets Canadian politicians, business leaders'. The Globe and Mail, February 20, 2023. Available at: https://www.theglobeandmail.com/politics/article-secret-csis-reports-paint-picture-of-chinas-efforts-to-entrap-canadian/

[18] These and other examples are detailed in the 2024 NSICOP report above.

[19] Lim, Louisa and Bergen, Julia "Inside China's audacious global propaganda campaign"https://www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping

[20] Hoja, Gulchehra. 2023 'China pumps up narrative of happy Uyghurs in Xinjiang among Pakistanis'. Radio Free Asia, August 23, 2023. Available at:

[21] Hoa, Zhang "Ukraine crisis instigator: US-led NATO reneges on 'Not one inch eastward' promise to compress Russia's space to the extreme" 2022 https://www.globaltimes.cn/page/202203/1256665.shtml

[22] Global Times 2024,'Taiwan is an integral part of China…' https://www.globaltimes.cn/page/202406/1313970.shtml

PRC Tactics, Techniques and Procedures (TTPs) & Platforms

The PRC's information and influence operations in Canada are extensive, targeting Uyghur, Tibetan, Hong Kong, Taiwanese, and Falun Gong communities with a multi-platform strategy that leverages social media, state media, influencers, and community events. This approach aims to shape perceptions, suppress dissent, and maintain control over Chinese Canadians, targeted communities, and the broader Canadian public.

Chinese social media platforms like WeChat and Weibo are central to these operations and are used to disseminate propaganda and conduct surveillance.

The PRC conducts influence operations across diverse social media platforms, employing evolving tactics to micro-target audiences. By tailoring disinformation to specific groups and leveraging multiple languages and platforms, Beijing promotes its narratives and political agenda. Chinese regime-controlled platforms like WeChat, Weibo, and Douyin primarily target Chinese-language speakers, as Chinese is the major language used on these platforms. Given that these platforms are also subject to heavy PRC censorship and regulations, they remain an ideal channel to amplify Beijing's disinformation and propaganda.

On the other hand, Western platforms like Facebook and X are censored and blocked inside China. As such, the PRC's FIMI operations on platforms such as these tend to target broader audiences in Canada.

Videos on platforms like YouTube present misleadingly positive depictions of life in Tibet and in East Turkistan (Xinjiang), portraying happiness that does not reflect reality. Half of the community leaders interviewed have observed disinformation spread on Facebook as well.

State media plays a significant role, with Chinese Canadian audiences consuming content from multiple PRC-controlled channels available on Canadian public airwaves, cable and satellite systems, and the internet. These mediums offer the PRC a steady and open stream through which to communicate and impose their official narratives, overshadowing and marginalizing alternative viewpoints and manipulating facts.

Content-sharing agreements between Chinese state media and domestic Canadian Chinese-language media further integrate Beijing's messaging into the daily lives of Chinese Canadians. These arrangements are often driven by financial dependencies and the fear of losing advertising revenue tied to China and Chinese communities in Canada.

At least 14 Canada-based media platforms are listed as Global Chinese Media Cooperation Union (GCMCU) members. The GCMCU portrays itself as a global cooperative organization, but is operated by UFWD through Chinese state media China News Service (CNS)[23]. The

GCMCU's role is to seek out, identify, and connect with foreign platforms that amplify state narratives. The GCMCU should be considered an important foreign-facing component of the PRC's FIMI operations.

Both open and covert community engagement are crucial tactics. The PRC sponsors events and gatherings in Canada, leveraging the prestige of these occasions to influence business owners, media figures, and opinion leaders. By inviting select individuals to lavish events, Chinese diplomats foster an atmosphere of exclusivity, luring and pressuring attendees to align with the PRC's positions and discouraging dissent to preserve social status.

Influencers and key opinion leaders, including former officials and prominent community figures, play a crucial role in amplifying pro-PRC messages. These individuals, whose status and large followings on platforms like YouTube and WeChat are strategically leveraged, subtly promote PRC narratives while discrediting activists. By exploiting seemingly respected voices, the PRC ensures its perspectives dominate, making dissenting opinions appear marginal and less credible.

Overall, the PRC's sophisticated use of media, community influence, and targeted intimidation shapes a narrative that marginalizes critics and reinforces control over the Chinese diaspora in Canada. This strategy seeks to silence opposition and impose a favourable image of PRC within these communities.

[23] Bandurski, David. 2023. "Global Chinese Media Cooperation Union (GCMCU)." China Media Project, May 12, 2023. Available at: https://chinamediaproject.org/the_ccp_dictionary/global-chinese-media-cooperative-union/

Case Studies

Below we highlight some of the highest profile examples of PRC information and influence operations, along with descriptions of the tactics, techniques, and procedures (TTPs) used by the PRC to execute them.

Electoral Interference in Canada's Federal Elections (Kenny Chiu)

TTP Connection: Cyber Espionage, Disinformation Campaigns, Political Interference, Transnational Repression

During the 2021 Canadian federal election, a PRC disinformation campaign targeted Conservative MP Kenny Chiu over his proposed Foreign Influence Registry Act.[24] The campaign falsely portrayed the bill as an "anti-China bill that discriminates against all Chinese and threatens their freedom, cultural and economic development"[25] and as a threat to the cultural and economic freedoms of the Chinese community. This disinformation was spread primarily on Chinese social media platforms like WeChat, targeting audiences in Canada. The attack on Chiu also represents an example of PRC TNR, targeting Chiu as a critic of PRC policies, and an effort to silence him.

This operation is an example of direct political interference, as it aimed to weaken support for Chiu and the Conservative Party of Canada by manipulating the Chinese diaspora community's perception of him and his proposed legislation. The PRC leveraged micro-targeting on Chinese-language platforms like WeChat, showing how Beijing uses cyber influence tactics to disrupt political outcomes and align them with its interests.

Spamouflage Campaign Targeting Canadian MPs

TTP Connection: Cyber Espionage, Disinformation Campaigns, Political Interference, Transnational Repression

Spamouflage is a type of coordinated online influence operation that uses fake accounts and bots to amplify pro-China narratives, suppress dissent, and manipulate discourse. The PRC's Spamouflage[26] campaign targeted 47 Canadian MPs, including the Prime Minister and several Cabinet members, using spam and disinformation on platforms like YouTube, Twitter (X), and Facebook. The operation sought to discredit critics of the CCP by generating

[24] DisinfoWatch. 2021 "Influence Operation Targeting Canadian 2021 Federal Election" https://disinfowatch.org/influence-operation-targeting-canadian-2021-federal-election/

[25] Today Commercial News. 2021. 'Please spread the message: Conservative MP Kenny Chiu proposed <The Foreign Influence Registry Act> to suppress the Chinese community'. https://todaycommercialnews.com/canada/⁴9³07# (〈請廣傳！ 保守黨國會議員趙錦榮提「外國勢力註冊」法案打壓華人社區〉，加拿大商報，2021年09月09日)

[26] Martin, Alexander. 2023. 'Chinese law enforcement linked to largest covert influence operation ever discovered'. The Record Future, August 29, 2023. Available at: https://therecord.media/spamouflage-china-accused-largest-covert-influence-operation-meta

waves of content accusing MPs of criminal and ethical violations.

This illustrates disinformation and cyber manipulation, where large-scale social media spam is used to discredit public figures and erode their credibility. This operation aimed to intimidate MPs and reduce criticism of the CCP, connecting to Beijing's broader strategy of silencing dissent while operating through coordinated, inauthentic behaviour across multiple platforms.[27]

Operation Fox Hunt and Overseas Chinese "Police" Stations

TTP Connection: Cyber Espionage, Transnational Repression

"Operation Fox Hunt" is a PRC campaign that targets Chinese expatriates abroad, pressuring them to return to China by using intimidation and threats. In Canada, this is exemplified by the establishment of illegal overseas "police stations"[28] run by pro-China individuals with alleged ties to PRC state entities. While the PRC claimed that these "police stations" are established to provide services like the renewal of PRC driver's licenses, CSIS assessed that a key purpose of these stations was "to collect intelligence and monitor former PRC residents living in Canada as part of the PRC's broader transnational anti-corruption, repression, and repatriation campaign."[29]

This case directly aligns with TNR tactics, where PRC actors extend state control beyond their borders to suppress dissent. These police stations serve as hubs for surveillance and intimidation, particularly targeting those critical of the PRC and members of the so-called "Five Poisons". They are part of a broader espionage network operating under the guise of offering community services, thus extending the reach of the PRC's repression into Canadian territory.

Operation Targeting MP Michael Chong

TTP Connection: Cyber Espionage, Political Interference, Transnational Repression

In August 2023, Global Affairs Canada's Rapid Response Mechanism announced that it detected a PRC information operation on WeChat targeting MP Michael Chong.[30] The campaign coincided with diplomatic tensions between Canada and China, including the

[27] Rapid Response Mechanism (RRM Canada). 2023. 'Probable PRC "Spamouflage" campaign targets dozens of Canadian Members of Parliament in disinformation campaign'. Government of Canada, October 23, 2023. Available at: https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2023-spamouflage.aspx?lang=eng

[28] Safeguard Defenders. 2022. 'Patrol and Persuade - A follow up on 110 Overseas investigation'. Available at: https://safeguarddefenders.com/en/blog/patrol-and-persuade-follow-110-overseas-investigation

[29] Canadian Security Intelligence Service. 2022. 'CSIS Security Alert: "Police Stations" in Canada a Part of Ongoing PRC Interference'. December 5, 2022.

[30] Rapid Response Mechanism (RRM Canada). 2023. 'WeChat account activity targeting Canadian parliamentarian suggests likely foreign state involvement'. Government of Canada, August 9. 2023. Available at: https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/wechat.aspx?lang=eng

expulsion of a Chinese diplomat from Canada.[31] It spread false narratives about Chong's background and political views to discredit him among Chinese-speaking communities in Canada, aiming to undermine his influence due to his criticism of Beijing's human rights abuses and support for democracy in Hong Kong and Taiwan.

MP Michael Chong and his family were reportedly threatened[32] and monitored[33]; common tactics of TNR. Reports indicated that a Chinese diplomat in Canada targeted Chong and was seeking information about his relatives in Hong Kong, possibly to intimidate or exert pressure on him through his family, and was likely sending that information back to China's Ministry of State Security. In a recent testimony at Canada's Public Inquiry into Foreign Interference, Prime Minister Justin Trudeau said that "gathering information on Chong didn't qualify as foreign interference."[34] However, given the PRC's past targeting of Chong, it is reasonable to assume that the PRC's monitoring and surveillance activities were part of the regime's broader efforts to discredit and harass Chong, and therefore, should be considered foreign interference and TNR.

The PRC's tactics align with patterns of TNR, where authorities target the families of critics abroad in their efforts to stifle dissent. These threats aimed not only to undermine Chong's political influence but also to send a broader message to other potential critics of Beijing's policies, emphasizing that opposition to the CCP could have personal and familial repercussions, even when that opposition occurs outside China's borders.

The case highlights how the PRC combines disinformation, political interference, and TNR to intimidate and silence critics. By leveraging ethnocultural networks, the PRC aims to silence voices advocating for human rights and democracy, demonstrating its broader tactics of using reputational attacks and intimidation to deter opposition to its policies.

[31] Catharine Tunney, "Canada Expelling Chinese Diplomat After Allegations of Intimidation," CBC News, May 8, 2023, https://www.cbc.ca/news/politics/canada-expelling-chinese-diplomat-1.6836336.

[32] "MP Michael Chong Received Personal Threats: Report," National Post, accessed October 23, 2024, https://nationalpost.com/news/politics/mp-michael-chong-received-personal-threats.

[33] Michael Chong, "Testimony before the Standing Committee on Procedure and House Affairs, Meeting 74, 44th Parliament, 1st Session," Our Commons, May 16, 2023, https://www.ourcommons.ca/DocumentViewer/en/44-1/PROC/meeting-74/evidence.

[34] Elizabeth Thompson, "Trudeau Tells Inquiry Some Conservative Parliamentarians Are Involved in Foreign Interference," CBC News, October 16, 2024, https://www.cbc.ca/news/politics/trudeau-testify-foreign-interference-inquiry-1.7353342.

PRC TNR Targeting Vulnerable Canadian Ethno-Cultural Communities

The most vulnerable groups to PRC operations in Canada are the Uyghur, Tibetan, Hong Kong, Taiwanese, and Falun Gong communities, particularly the leaders within them.

In May-June 2024, we conducted interviews and surveys with 25 Chinese, Hong Kong, Taiwanese, Tibetan, Uyghur, and Falun Gong community leaders and activists in Canada to assess their experiences with PRC FIMI, TNR, and related information and influence operations. Five in-depth, in-person interviews were conducted, while the remaining participants responded to an online survey which solicited open answers about their observations and experiences. Participants were asked about narratives and threats they had experienced or witnessed, as well as their perspectives on the Canadian government's response to PRC information and influence operations. Most of those interviewed have been actively involved with their communities in Canada for at least five or more years, offering a depth of experience and insight into the ongoing repression and disinformation targeting their organizations and communities.

Our findings offer a community perspective on the threats, strategies, narratives, and methods of repression used by the PRC, and vulnerability to these tactics. This research has been applied to help develop a framework and a TNR kill chain (a model used to identify and disrupt various stages of a TNR operation) to help governments, law enforcement, and vulnerable communities prevent, disrupt, and deter TNR.

Almost all of the respondents to our survey reported experiencing or observing harassment or intimidation connected to PRC transnational repression objectives.

Types of Threats Reported	No. of responses
Harassment	19
Intimidation	18
Surveillance	12
Online Threats	10

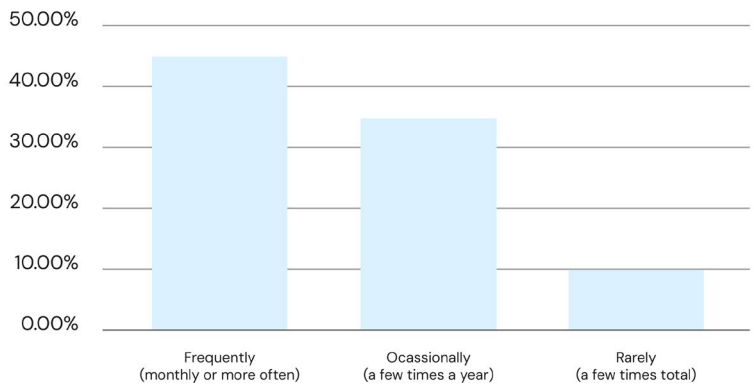
In our survey, we asked community leaders and activists about their experiences or observations of the PRC's attempts to exert control and influence over their members. 80% of respondents reported that threats to family members in China are a common method of coercion. Additionally, 85% noted that direct threats against Canadian activists are used to intimidate and control these communities, while 70% identified political pressure as a key tool for exerting influence. Furthermore, 75% indicated that financial incentives are often used to sway community members.

How does the PRC government control or influence community members in Canada?

1) Threats to activists in Canada (*85% of respondents*)
2) Threats to family members in China (*80% of respondents*)
3) Financial incentives (*75% of respondents)*
4) Political pressure (*70% of respondents*)

Most of the community leaders who responded to our survey reported personally experiencing or observing threats from PRC-linked entities. Among the most frequently deployed tactics were harassment and intimidation, with 45% of respondents reporting frequent occurrences (monthly or more often). Harassment includes repeated and threatening phone calls, as well as online harassment.

How often do these threats occur?



Key PRC FIMI and TNR Objectives and Tactics Deployed in Canadian Communities

The PRC has systematically used disinformation and propaganda to target and discredit the Uyghur, Tibetan, Hong Kong, Taiwanese, and Falun Gong communities, as well as the government of Canada.

These narratives aim to suppress criticism and dissent, justify repressive policies, and promote a favourable image of China, while attacking critics, including those in Canada. The PRC's foreign information and influence efforts seek to shape Canadian policy to align with PRC interests and undermine legislation designed to counter its harmful activities, such as the Uyghur Genocide Motion or the Foreign Influence Transparency Registry (FITR). The FITR has been mischaracterized by the PRC and its domestic proxies as an anti-Chinese Canadian law.

Based on interviews with leaders and activists from vulnerable Canadian communities, we examine the narratives the PRC deploys against them, and the TNR tactics used to intimidate, coerce, and silence dissent within these groups.

Uyghur Community

The PRC's objective when promoting narratives about the Uyghur community and the situation in East Turkistan (Xinjiang) is to suppress reports of genocide and forced labour, while promoting positive narratives of economic development, cultural and religious tolerance, and progress in the region. The PRC denies any human rights abuses and uses economic threats to silence critics, ensuring that countries like Canada remain hesitant to implement sanctions or speak out forcefully against Chinese policies. A common tactic is the use of "whataboutism", which shifts attention away from Chinese atrocities by pointing out social or political issues in other countries.

Uyghur activists in Canada have been targets of PRC TNR and are aware of the regime's ability to exert pressure on exiled Uyghur communities, largely through threats directed at family members who remain in East Turkistan which are used to coerce and intimidate the diaspora and suppress activism or criticism. Many activists have been harassed through phone calls, online threats, and surveillance, creating an environment of fear and intimidation.

Uyghur Canadian leaders told us that they are extremely concerned about the PRC's disinformation campaigns aimed at undermining reports of human rights abuses,

particularly with regard to the genocide and PRC-backed forced labour practices. These narratives are often promoted through influencers,[35] news-focused websites, and social media platforms, where the PRC attempts to paint a picture of progress and prosperity in the region, directly countering reports from human rights organizations, scholars, activists, and journalists.

Tibetan Community

Beijing's influence operations surrounding Tibet focus on creating the illusion of cultural tolerance and support for Tibetan Buddhism. By showcasing religious sites and model villages to foreign journalists and diplomats, the PRC attempts to paint a positive image of its policies in Tibet. However, these orchestrated visits conceal the reality of widespread repression and human rights abuses.

The PRC also uses economic leverage to prevent criticism of its actions in Tibet. Respondents to our survey noted that by emphasizing the economic benefits of maintaining positive relations with the PRC, the PRC government discourages Canadian politicians and business leaders from speaking out. This economic pressure is a key factor in the continued apathy towards Tibet among many international human rights organizations and governments. The PRC's economic

influence allows it to leverage its trade relationships to dissuade countries like Canada from speaking out about its actions in Tibet.

Tibetan Canadian leaders told us that they and members of their community face both subtle and overt coercion. For example, PRC exit visa applications are manipulated to pressure visitors into acting as informants for the PRC government. Conversely, Canadians of Tibetan heritage may be denied PRC entry visas if they speak out in Canada, preventing them from visiting family members. Additionally, Tibetan activists have received direct threats, including threats of sexual violence, for their outspoken stances on Chinese policies.

Community leaders told us that the PRC's disinformation against the Tibetan community is rooted in racist stereotypes, portraying Tibetans as "lazy", "dirty", or "violent". These narratives, which have been spread both in China and abroad, serve to further marginalize the community. Tibetans are often depicted as benefiting from Chinese control, an image actively promoted by state-run media and PRC-controlled cultural exchanges.

[35] U.S. Department of State, PRC Efforts to Manipulate Global Public Opinion on Xinjiang, accessed November 22, 2024, https://www.state.gov/prc-efforts-to-manipulate-global-public-opinion-on-xinjiang/.

Hong Kong Community

In Canada, Beijing has worked to portray itself as a defender of the global Chinese-speaking community. This narrative is intended to foster loyalty among Chinese Canadians and create a division between those who support the PRC and those who support democracy in Hong Kong. By polarizing the community, the PRC seeks to weaken opposition to its policies and diminish the influence of pro-democracy Hong Kong activists.

The PRC's messaging also emphasizes national pride and loyalty to the CCP, with the goal of promoting a sense of belonging to China rather than Canada. Through this strategy, the PRC attempts to undermine Canadian identity among Chinese-speaking citizens, further isolating dissenters within the community.

Leaders in the Canadian Hong Kong community, particularly pro-democracy activists, are concerned about the influence and social manipulation deployed by the PRC in Canada. The PRC strategically uses platforms like WeChat to spread propaganda that promotes PRC narratives, while also enforcing ethno-nationalism and conformity among Chinese Canadians and discrediting and marginalizing critics within the community.

These techniques create divisions within the Chinese Canadian community, polarizing it into "Blue" (pro-PRC) and "Yellow" (pro-Hong Kong) factions. The deliberate marginalization of critics, both online and in person, serves as a warning to those who might consider speaking out against the PRC. Activists in Canada have also faced direct threats and harassment aimed at silencing their pro-democracy efforts.

Falun Gong

The PRC has systematically attempted to discredit Falun Gong practitioners' beliefs, frequently using international media campaigns to spread false information about their practices. As a result, Falun Gong members have become frequent targets of propaganda designed to erode their legitimacy.

The campaign against Falun Gong practitioners relies heavily on disinformation and conspiracy theories, aiming to depict the group as a dangerous "cult" to undermine its credibility and justify the persecution of its followers. This disinformation includes fabricated stories about illegal activities and extreme practices, fostering a climate of fear and mistrust around Falun Gong practitioners.

A report published by Falun Dafa Association of Canada in July 2024[36] highlights efforts to intimidate and harass members of this community. In March 2024, a bomb threat was

[36] Falun Dafa Association of Canada. Foreign Interference & Repression of Falun Gong in Canada: Key Development & Case Studies 1999-2024. October 2023, updated July 2024. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/HRC0000123.pdf.

sent to a Vancouver theatre where a community cultural event was being held. The report highlights an intensification of surveillance and other threats and intimidation against community members.

Taiwanese Communities

While our outreach to Taiwanese community groups was more limited than with other community groups, we heard that the Taiwanese Canadian community has observed ongoing PRC attempts to delegitimize Taiwan's sovereignty, both through diplomatic pressure and media manipulation. Some pro-sovereignty Taiwanese groups have been excluded from public Chinese Canadian community events, further isolating them from the broader Chinese-speaking population in Canada.

New Canadian Measures to Combat TNR & Bill C70

Bill C-70 and Its Impact on Combating TNR

In June 2024, Parliament passed Bill C-70, which updated Canada's national security laws and enacted the Foreign Influence Transparency and Accountability Act (FITAA) to combat foreign influence operations and TNR. Below, we outline the potential impact of Bill C-70.

Expanding Information Disclosure under the CSIS Act

Bill C-70 introduces significant amendments to the CSIS Act, notably expanding the agency's ability to disclose information to non-governmental entities when it is considered "essential in the public interest." This amendment, implemented through section 19(2)(d), allows such disclosures if the public interest clearly outweighs any potential invasion of privacy. Additionally, the new subsection 19(2.1) permits CSIS to share information "to any person or entity" to build resilience against threats to Canada's security, provided that:

- The information has already been shared with a relevant federal department or agency.
- It does not include any personal information of a Canadian citizen, permanent resident, or individual in Canada.
- It does not contain the name of any Canadian corporation or entity.

While these conditions are designed to protect privacy, they may limit CSIS's ability to identify specific threat actors, particularly in cases involving foreign influence operations.

Strengthening CSIS's Operational Capabilities

Bill C-70 also enhances CSIS's ability to conduct operations beyond Canada's borders. A new section added to the CSIS Act, 16(1.1), authorizes CSIS to collect, from within Canada, information or intelligence located outside the country if the assistance is directed at a person or entity in Canada or at an individual who was in Canada and is temporarily outside Canada. New sections 20.3 and 20.4 empower the CSIS Director or designated employees to seek judicial orders for preserving and producing information or documents located outside of Canada. Updated warrant provisions under section 22.21(1) now enable judges to authorize activities outside of Canada to enable CSIS to investigate threats to the security of Canada.

The bill also mandates a parliamentary review of the CSIS Act every five years, ensuring that the legislation remains up-to-date with evolving security threats. Despite these substantial changes, the CSIS Act does not define critical terms such as "foreign interference," "foreign

influence," or "TNR," which could impact how these issues are addressed.

Broader Offences under the Security of Information Act (SOIA)

Bill C-70 significantly expands the scope of offences under the Security of Information Act (SOIA). Section 20(1) now criminalizes actions taken at the direction of, for the benefit of, or in association with foreign entities or terrorist groups that use intimidation, threats, or violence to coerce individuals to do anything or to cause anything to be done. In many instances, such actions would still constitute an offence if committed outside of Canada.[37]

Further, the new sections 20.2, 20.3, and 20.4 broaden the behaviours that are prohibited. Section 20.2 prohibits the commission of an indictable offence at the direction of, for the benefit of, or in association with, a foreign entity. Section 20.3 prohibits knowingly engaging in surreptitious or deceptive conduct if it is for a purpose that is prejudicial to the safety or interests of Canada, or if the person is reckless as to whether it is likely to harm Canada's interests. Section 20.4 prohibits engaging in surreptitious or deceptive conduct intending to influence Canada's political, governmental, or educational processes. Given the vulnerability of political nomination processes to foreign interference, this last change is particularly important in countering tactics used by state actors like the PRC.

Expansion of Preparatory Offences

Bill C-70 also amends section 22 of SOIA to widen the list of preparatory offences, increasing the legal tools available to counter threats to national security. Further, the maximum penalty for a preparatory offence under subsection 22(1) has increased from two to five years, while the offences contained in sections 20(1), 20.1(1), 20.2(1), 20.3(1), and 20.4(1) all carry maximum sentences of life imprisonment.

Criminal Code Amendments on Sabotage

Amendments to the Criminal Code under Bill C-70 focus on the offence of sabotage, specifically targeting acts against essential infrastructure and devices. While these changes are aimed at enhancing Canada's defences, the bill does not introduce a specific offence in the Criminal Code for foreign interference, refugee espionage, or online harassment and digital violence. These gaps may limit the effectiveness of countermeasures against influence tactics that target vulnerable communities in Canada.

[37] The particulars of the jurisdictional requirements are complex and outlined in Human Rights Action Group's submission to the Standing Senate Committee on National Security and Defence: Bill C-70, https://rightsactiongroup.org/wp-content/uploads/2024/07/HRAG-Written-Brief-Final-Jun-2024-SECD-version.pdf, pgs. 4-5. In brief, if one of the criteria in section 20(2) is met, and the offence is committed outside of Canada, it is deemed to have been committed in Canada. If none of those criteria are met, but a perpetrator, after the time that the offence is alleged to have been committed outside of Canada, is present in Canada, the offence may likely be prosecuted under section 20.1(1) if the additional criteria contained in that section are met.

Revisions to the Canada Evidence Act

Part 3 of Bill C-70 includes amendments to the Canada Evidence Act, creating a structured approach to handling sensitive information related to international relations, national defence, or national security. These revisions are intended to streamline legal procedures involving such information, bolstering the government's ability to protect Canada's interests.

Foreign Influence Transparency and Accountability Act (FITAA)

One of the most critical components of Bill C-70 is the enactment of the Foreign Influence Transparency and Accountability Act (FITAA). This act requires individuals or entities entering into arrangements with foreign principals to register these arrangements within 14 days. Although FITAA aims to increase transparency around foreign influence, its scope is limited to political or governmental processes, such as legislative actions, policy developments, and elections. This limitation means that foreign influence activities unrelated to these processes, including TNR targeting vulnerable communities, may escape scrutiny.

FITAA includes exemptions for foreign nationals with diplomatic credentials and employees of foreign principals acting in an official capacity. It also grants a new Foreign Influence Transparency Commissioner the power to conduct investigations, impose penalties, and take enforcement actions. However, the covert nature of foreign influence operations, often involving proxies and indirect channels, may pose significant challenges to effective enforcement.

Recommendations

Below are a set of recommendations for the Canadian government to protect Canadians and vulnerable communities, as well as to prevent, disrupt, and deter PRC information and influence operations and TNR.

1. Strengthen Government Frameworks and Coordination

Adopt a universal framework and disruption strategy amongst like-minded democracies
Develop a clear and unified definition of foreign interference and TNR. This framework should set a common threshold for action, including a structured kill chain approach to identify, disrupt, and ultimately stop these activities—as proposed at the end of this report.

Strengthen coordination and information sharing
Improve collaboration within the security and intelligence community and relevant government units and civil society organizations (CSOs) by fostering regular information sharing, real-time threat assessments (when possible), and a unified understanding of foreign interference activities. This will bridge intelligence-to-evidence gaps and support more strategic decision-making.

Improve communication and transparency
Strengthen and integrate strategic communication efforts by educating media, elected officials, and the public on foreign information operations, their objectives, and tactics. Increase transparency through regular release of unclassified reports on influence operations. Robust mechanisms should also be established for reporting and disrupting ongoing operations.

Regulate social media
Encourage social media platforms to remove or label state-affiliated entities to identify them and moderate their platforms to remove inauthentic behavior. Legislation modelled after Europe's Digital Services Act[38] may be required to force reluctant platforms to comply.

Ensure platforms provide researchers access to data to analyze influence tactics. Where necessary, introduce legislation or regulations to prevent foreign authoritarian regimes, such as the PRC, from accessing, manipulating, and weaponizing Canadian information spaces through

[38] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

regime-controlled platforms like WeChat.

The Canadian government could consider how to mitigate the risk of threats occurring on foreign authoritarian state-controlled platforms. This may include compelling such platforms to divest from foreign adversaries or imposing full or partial bans. Other long-term solutions such as banning cross-border data transfer to foreign adversaries, and scrutinizing laws and regulations for data brokers should also be considered.

2. Address Gaps in Support for Victims of TNR

Improve law enforcement engagement and response
Canadian law enforcement units are under-resourced and under-prepared to address the persistent and growing threat of TNR. Improving threat awareness at all levels of law enforcement and enhancing communication between them and vulnerable communities will help respond to future cases. Providing greater resources to strengthen the responsiveness of Canadian law enforcement to cases of TNR will ensure that threats, harassment, and digital attacks targeting activists and vulnerable communities are properly investigated and prosecuted. These improvements in intervention and disruption of TNR operations will lead to greater long-term deterrence and prevention.

Provide support for vulnerable communities and rehabilitation for victims of TNR
Victims of TNR often suffer from psychological trauma, damage to their reputations, and ongoing legal challenges. They may also suffer physical and financial damages. Providing comprehensive support is essential, including access to specialized mental health services and peer support networks, which foster resilience and solidarity among those affected. Rehabilitation of reputations should involve partnerships with media and civil society to counter disinformation and restore victims' personal and professional standing. Additionally, encouraging pro-bono legal assistance will help address legal challenges and support victims in re-establishing their careers. A specialized fund for victims of TNR should be considered.

3. Empower Civil Society and Community Engagement

Promote grassroots and knowledge-sharing initiatives
Support organizations that promote awareness of foreign information operations and those that foster democratic resilience within vulnerable

communities. Encourage the development of community networks and regular communications between them and government, media, and other CSO organizations.

Support and cultivate capacity for detection, disruption, prevention
Support specialized think tanks and organizations dedicated to analyzing influence operations and organizations that produce regular reports that analyze and explain the objectives, tactics, and narratives deployed by foreign authoritarian governments in order to inoculate Canadians against them. This includes activists, CSOs, and journalists who expose such operations and contribute to their disruption and the prevention of them through deterrence.

4. Enhance Legislative and Policy Tools

Institutionalize foreign interference coordination
Create a dedicated unit that integrates all aspects of cybersecurity, intelligence analysis, and political and diplomatic responses to foreign interference, focused on countering PRC and all other foreign authoritarian influence and information operations—such as the Swedish Psychological Defence Agency.[39] The Global Affairs Canada Rapid Response Mechanism could serve as a foundation for this effort. This Canadian unit should be independent from the government to avoid any partisan manipulation.

All-party parliamentary FIMI & TNR committee
A committee made up of representatives from all major political parties and Canada's intelligence community should meet monthly to brief elected officials on emerging and ongoing information and influence operations. This committee would keep party leaders and their caucuses informed about these threats, enhancing their awareness, critical thinking, and resilience against foreign narratives that aim to undermine Canadian democracy.

Global coordination and leadership
As a leading member of the Media Freedom Coalition and the G7 on foreign information operations, Canada could take the lead in establishing a Global Alliance Against Transnational Repression (GAATR). This initiative would enhance knowledge sharing and raise awareness among allies about authoritarian activities, facilitate the exchange of best practices to strengthen social and democratic resilience, and build a unified coalition dedicated to protecting the citizens of allied nations from foreign interference.

[39] https://mpf.se/psychological-defence-agency/about-us/our-mission

PRC Transnational Repression Framework and Kill Chain*

*A "kill chain" is a systematic process that outlines the steps required to identify, target, disrupt, and neutralize an adversary

Operation Kill Chain & Tactics, Techniques, and Procedures (TTPs)

Proposed Countermeasures

Prevention, Mitigation, & Disruption

SEVERITY INCREASES

PLAN

Plan Strategies & Objectives

- Define the desired political outcomes
- Develop strategies and policy initiatives

Identification

- Surveillance and intelligence gathering via online and offline means
- Identify targets susceptible to influence and repression
- Identify potential assets for intelligence gathering, coercion, and other operations

Digital Surveillance

- Monitor social media profiles and online communications
- Infiltrate and monitor social network groups
- Hack personal devices and accounts to collect personal data, passwords, or compromising information

Physical Surveillance

- Stalk and tail individuals
- Use diplomatic channels and diaspora networks to identify targets

Planning Disruption Inoculation (Deterrence by Denial)

- Increase awareness and digital security training for vulnerable commmunities
- Develop tools for communities to report suspicious activities and potential targeting
- Establish a universal framework for collective response
- Create a Global Alliance Against Transnational Repression (GAATR)

PREPARE

Select and Prioritize Assets & Targets

- Assess priorities using data collected through covert and overt means
- Identify and cultivate networks of influence: potential enablers, influencers, and assets (e.g. regime-aligned activists, journalists, former officials, academics)
- Develop and strengthen connections with diaspora groups, laying the groundwork to leverage them against specific targets
- Assign resources to high-priority targets
- Coordinate with existing domestic and foreign assets

Microtargeting

- Gather intelligence on the target(s)
- Identify vulnerabilites and tailor tactics, techniques, and procedures (TTPs) to execute operations

Establish Legitimacy

- Prepare for legal warfare (lawfare) in a later phase
- Develop content and narratives against targets, including legal framework and disinformation materials
- Incorporate grey zone activities and influence operations to further legitimize its assertiveness

Mobilize Resources for Operations

- Mobilize resources and coordinate different entities, including state actors, diplomatic staff, state media and domestic media, influencers and groups, to execute its influence operations and transnational repression campaigns

Preperation Disruption

- Engage law enforcement, intelligence communities, and CSOs to assess and identify vulnerabilities and threats
- Enhance communication and intelligence-sharing inside government with CSOs and allied nations
- Identify groups and individuals known to collaborate with the regime, and conduct regular monitoring and analysis

Deterrence by Denial

- Better strategic communication to inform the public about tactics, techniques, and procedures
- Foster and promote awareness and defence mechanisms within vulnerable communities
- Strengthen cooperation and communications between vulnerable communities and law enforcement

EXECUTE

Cyber Attacks and Information Operations

- Exploit digital vulnerabilities and leverage assets captured in planning and preparatory stages
- Conduct influence operations to manipulate the information environment and steer public opinion in its favored direction

Information Operations

- Propaganda campaigns and false media publications
- Leverage state media, gray media, and other social media assets such as influencers to apply pressure on the targets

Hacking and Cyber Attacks

- Hacking and data breaches
- Distributed denial of service (DDoS)
- Malware and phishing

Harassment and Intimidation

- Targeted defamation campaigns
- Pro-regime protests/events disruption
- Community intimidation and online harrasment
- Social and economic isolation
- Diplomatic pressure to ostracize targets
- Incitement of anger and hate towards target community

Threats & Intimidation

- Threatening communications (phone calls, mail, emails, etc.)
- Blackmail
- Harassment and threats against family members both domestically and abroad

Legal and Judicial Harassment (Lawfare)

- Travel bans and sanctions
- Visa coercion
- Passport and documentation manipulation

Extraterritorial Legal Harassment

- Criminalize individuals and issue bounties
- Misuse/abuse of interpol notices

Lawfare

- Threat and application of frivolous lawsuits

Physical Attacks, Assassinations, Kidnapping, and Vandalism

- Utilize intelligence agencies, fronts, proxies, and local criminal organizations to instigate or incite violence against the targets (individuals or communities) as a means to deter, coerce, and retaliate
- Vandalism
- Kidnapping and unlawful detention
- Physical assaults
- Assassinations and poisoning

Execution Disruption

- Establish a robust mechanism with social media platforms for reporting and disrupting ongoing operations
- Community-based interventions
- Coordinated law enforcement action

Deterrence by Punishment

- Targeted sanctions and diplomatic actions
- Public accountability, attribution, and exposure

Rehabilitation

- Offer physcological, legal, and social reintegration support
- Rehabilitate reputations
- Develop support networks

SEVERITY INCREASES >>>>

Note: Severity increases from top to bottom of each category. For the severity scale: Severity increases (1) from top to bottom of each category, and (2) from left to right (cyber attacks and information operations being the mildest and physical attacks being the most severe)

Digital Public Square is a Toronto-based not-for-profit whose objective is to rethink and redesign the way technology is used to support communities worldwide. We find ways for communities to engage in healthy debate, share knowledge, and co-create solutions to their most pressing challenges.

digitalpublicsquare.org

hello@digitalpublicsquare.org

DIGITAL
PUBLIC
SQUARE