Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

Deterrence by Denial: Protecting Chinese Diasporas and Canadian Federal Elections from Chinese Interference

Ivan Nuñez Gamez

Winter 2024 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Key Points

- Canada's Chinese diaspora communities have been targeted increasingly by mis-, dis- and malinformation (MDMI) through Chinese-owned and Chinese-language platforms. Of particular notoriety is WeChat, which is regulated by Chinese surveillance and data collection laws regardless of the geographic location of users.
- Canada's counter-interference strategy is not cognizant of digital means of interference; hence, it is technically and influentially incapable of deterring or reducing the impact of these operations.
- Australia, which possesses similar diaspora demographics as Canada, has successfully employed a deterrence-by-denial strategy to counter Chinese cyber-foreign interference, effectively developing digital infrastructure, organization and policy.
- With the help of community liaisons, the Australian Government has identified digital risks present in Chinese-owned platforms and engaged with at-risk sectors to raise awareness of such risks.
- Drawing inspiration from allies such as Australia, the Government of Canada should seek to adapt current mechanisms that counter foreign interference to acknowledge the impact of cybersecurity breaches, build long-term digital resilience among the citizenry and establish minimum transparency reporting requirements for Canadian foreign-owned platforms operating within Canada.

Introduction

Foreign interference is multifaceted and not exclusive to a single actor, with its use to alter the outcome of elections in democratic states significantly increasing in the past few years (Schmitt 2021). Recently uncovered political covert action operations in Canada have placed a certain illiberal state — China — in the spotlight. Of particular concern is the extent to which the Chinese government takes advantage of the local Chinese diaspora in Canada to overtly and covertly influence federal elections via WeChat and TikTok. These two very popular platforms are owned by Chinese tech companies and are the preferred avenues through which to conduct foreign influence operations. Chinese-owned telecommunication companies serve as proxies for the Chinese government to conduct espionage and intelligence collection regardless of where the platforms are located or operate (Committee on Homeland Security and Governmental Affairs 2020).

Canada's *First Report* on foreign interference, drafted by the former independent special rapporteur on foreign interference David Johnston (2023), revealed that effective misinformation tactics were used primarily on the Beijing-based social media platform WeChat. MDMI[1] campaigns sought to sway public support away from Canadian

1 MDMI consists of different forms of false and misleading "information." *Misinformation* refers to false information that is not intended to cause harm; *disinformation* refers to false information that is intended to manipulate, cause damage or guide people, organizations and countries in the wrong direction; and *malinformation* refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm (Canadian Centre for Cyber Security 2022).

candidates whose political and policy positions did not favour the Chinese Communist Party. The success of Chinese MDMI can be explained through its consistent use of anti-Western messaging presented through all state-owned and Chinese-language platforms, not unlike psychological warfare tactics employed in times of conflict (Fung 2024). Considering the extraction, storage and exploitation of individual and collective data provided by diaspora communities who use these platforms, China can perfect manipulative policy narratives designed to worsen social tensions between the diaspora and other Canadians who do not access these platforms in both the short and the long term (Office of the Director of National Intelligence 2020; Le Grip 2023). To date, Western states, such as Canada, tend to counter such activity by villainizing the Chinese government while being insensitive to sociocultural differences between diaspora members and other Canadians, causing the former to feel caught in the middle between their Chinese cultural roots and/or birthplace and their new Canadian home. This working paper will evaluate Canada's current strategy to counter Chinese interference among Chinese diaspora communities based on the Chinese government's capabilities outlined in Johnston's *First Report*. Based on the strategic weaknesses identified, the paper will offer solutions borrowed from deterrence-by-denial theory — an approach that has proven effective in Australia, which has similar diaspora demographics to Canada.

Background

MDMI campaigns are used by liberal and illiberal regimes to sway election results in Western states. These campaigns — using social media platforms, which have become vital — create an opportunity for foreign actors to advance their narratives and national interests. The duopoly of ownership of mainstream social media platforms, which are concentrated in China and the United States (Le Grip 2023), means Canadians are exposed to both. Chinese speakers will use Chinese platforms whereas non-Chinese speakers will use US-based platforms, mostly in English. Whereas access to and information posted on Chinese platforms is tightly controlled by the Chinese government, US-based platforms are privately owned, and US regulations apply a relatively light touch to managing access and content. While Bill C-18[2] (an act regarding online communications platforms that make news content available to people in Canada) received royal assent in June 2023, it does not address MDMI campaigns on Chinese platforms.

Canada is a multicultural state that is home to countless diaspora groups such as the Chinese-Canadian community, which comprises 4.7 percent of the population (Statistics Canada 2023). Seventy-one percent of Chinese-Canadians identify as "first-generation," meaning they were born outside of Canada and may have ties to mainland China, especially via extended family members (ibid.). Their primary means of communication with relatives on the mainland is WeChat, an all-in-one application with features that range from direct messaging to paying bills (Mozur 2020). As increased censorship in China has essentially prevented almost all use of Western applications before or since 2010, WeChat has become an indispensable part

2 *Online News Act*, SC 2023, c 23, online: *Justice Laws Website* <https://laws-lois.justice.gc.ca/eng/acts/O-9.3/page-1.html>.

of life among Chinese people, considering its overarching capabilities (ibid.). Unlike other Beijing-owned platforms, such as TikTok, WeChat has a unified network of users in and outside China, which is exposed to continuous surveillance, censorship and propaganda by Chinese government agents, making it a powerful tool of social control (ibid.). Users of Chinese platforms located outside China are not protected by China's data collection policy, meaning WeChat can be obliged to share user information with the Chinese government (ibid.). Hence, these users can be and, in many instances, have been victims of targeted propaganda that advances China's interests. For instance, Kenny Chiu (former Conservative member of Parliament [MP] of Hong Kong descent and candidate for the Steveston-Richmond East riding in the 2019 federal election) was targeted by a WeChat-based misinformation campaign in which he was labelled a "racist" for his foreign interference registry bill that was described as "put[ting] Chinese Canadians in danger" — something he claims is untrue (CBC News 2023; Johnston 2023). As this riding represents the largest Chinese-Canadian population in Canada,[3] this incident is particularly significant, given the number of Canadians who were potentially reached by the disinformation. While the most straightforward response to this ongoing surveillance and voter manipulation efforts would be a nationwide ban on WeChat, that would result in countless Chinese Canadians losing their main means of communication with their relatives in mainland China, not to mention an infringement on Canada's rules concerning free speech.

However, the Canadian government's lack of meaningful outreach in Mandarin to outline Canadian national interests and alternative narratives about the West on platforms used by the Chinese diaspora begs the question: How secure is Canada against Chinese interference?

What Is Canada's Current Cybersecurity Strategy, and Why Is It Ineffective?

As of 2023, Canada's cybersecurity strategy focuses on four pillars — transparency, accountability, protection and prevention (Government of Canada 2023). Of particular importance are the preventive measures to address cyber-foreign interference, as once the interference has occurred, it is much more difficult to address. According to the Government of Canada (ibid.), it has engaged with at-risk stakeholders and focused on enhancing citizen resilience against disinformation campaigns. Notwithstanding these efforts, the results are disappointing. For instance, between 2019 and 2020, the Department of Canadian Heritage launched the Digital Citizen Initiative (DCI), a federal strategy designed to protect Canadian democracy that aims to battle "online disinformation and [build] partnerships to support a healthy information ecosystem."[4] Despite the release of the DCI,

3 See www12.statcan.gc.ca/census-recensement/2016/dp-pd/prof/details/page.cfm?Lang=E&Geo1=FED&Code1=59031&Geo2=PR&Code2=59&SearchText=Steveston--Richmond%20East&SearchType=Begins&SearchPR=01&B1=All&GeoLevel=PR&GeoCode=59031&TABID=1&type=0.

4 See www.canada.ca/en/canadian-heritage/services/online-disinformation.html.

the 2021 federal election is now being investigated for numerous allegations of Chinese interference. So where did Canada's cybersecurity strategy fall short?

Canada's cybersecurity approach is inherently reactive rather than proactive and fails to build digital resilience largely because it is restricted to English and French languages. This suggests cybersecurity programs will fail to reach diasporas whose preferred languages, and consequently media platforms, are other than Western and in Canada's official languages. This also suggests that Canadian messages are likely not tweaked to reflect cultural differences such as humour, expressions and other culturally specific particularities and, consequently, are incapable of understanding the impact these may have on the citizenry. An example of this ineffective messaging is Canada's Critical Election Incident Public Protocol (CEIPP), which is a mechanism introduced in 2019 that enables high-ranking public servants, through thresholds, to determine how "meaningful" foreign interference is and if it prevents Canadians from having a "free and fair election."[5] The fault of this process not only lies in the subjectivity inherent to certain terms such as "meaningful," but also in its minimization of the impact of influential means of interference. One could argue the lasting psychological effects on the Chinese diaspora of the propaganda that slandered MP candidate Chiu prevented a "free and fair election," but this will not register with the CEIPP, which focuses on technical interference, not subtle messaging. Canada is forgetting the importance of deterrence by denial — which requires knowing and understanding the group or targets under threat long before any activity occurs.

Deterrence discourages or restrains an actor from taking unwanted actions because the potential adversary knows they are "seen," and that there will be detrimental consequences for any nefarious actions they take (Mazarr 2018). While it is usually framed as a tool to prevent armed attacks, the concept of deterrence has applications for foreign interference as well. Denying an adversary the ability to interfere can occur through two means: by technical means, which suggests enhancing counter-interference technology and capabilities of Canadian agencies, and by building citizen resilience against the psychological forms of adversaries' propaganda. Deterrence by denial presupposes the Canadian government has the equivalent of an "operating picture" of who in Canada is at risk of manipulation; understands and monitors the technical and influential means China uses; and ensures that supports offered by the Canadian government to the Chinese diaspora are made on an ongoing and culturally appropriate basis rather than only before and after a federal election.

While the Government of Canada has now identified the risk posed by the Chinese government to Chinese diaspora communities through social media platforms owned by Beijing tech companies such as WeChat, it falls short of using said intelligence information to bridge the communication and support gap to Chinese diaspora communities. Current strategies such as the DCI are not only reactive to interference but also solely focusing on providing resources to the broader Canadian electorate rather than to those more at risk of foreign interference, such as diaspora communities. In fact, out of the more than 20 projects launched to "strengthen citizens' critical thinking about disinformation," only one catered to new Canadian citizens.[6] Furthermore, despite

5 See www.canada.ca/en/democratic-institutions/news/2023/02/critical-election-incident-public-protocol.html.

6 See www.canada.ca/en/canadian-heritage/news/2019/07/backgrounder--helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html.

the heightened attention to foreign interference allegations in recent years, Canada's National Cyber Security Strategy has not been updated to include the particular issue of election tampering (Gold, Parsons and Poetranto 2020). Considering the multifaceted nature of Chinese cyber-foreign interference, Canada needs a cohesive cybersecurity policy that is not time specific and that integrates all of the cybersecurity efforts of the federal government so that Canada can deny successful attempts at interference. Legislatively similar allies such as Australia have developed effective cybersecurity strategies that consider both technical and sociocultural means to protect their diaspora against foreign interference by using a deterrence-by-denial approach.

Learning from Allies

In 2018, Australia's Department of Home Affairs created a national counter foreign interference coordinator[7] and a dedicated centre to support the coordinator, who oversees intergovernmental collaboration and provides advice on the implementation of the Counter Foreign Interference (CFI) Strategy, last updated in 2023. Three pillars of Australia's strategy that would be of particular use to Canada are to "engage at-risk sectors to raise awareness and develop mitigation strategies, deter perpetrators by building resilience in Australian society…[and] enforce our CFI laws by investigating and prosecuting breaches."[8] These efforts were a response to the growing disinformation and coercive behaviour aimed at Australian-Chinese communities on China's social media platforms such as WeChat and TikTok, identified by Mandarin-speaking community liaisons who monitored activity on the platforms (Senate Select Committee on Foreign Interference through Social Media 2023).

The Australian strategy is multifaceted and engages multiple government sectors for an effective whole-of-government approach. Noteworthy is the adaptation of existing government agencies to actively counter cyber-foreign interference on a day-to-day basis. For instance, Australia's Electoral Integrity Assurance Taskforce not only broadened its definition of "electoral integrity" to include recognition of threats coming from "cyber…security incidents" and "misinformation or disinformation campaigns," but also enabled a widely accessible disinformation register that fact-checks disinformation during election cycles while maintaining impartiality.[9] Furthermore, in 2018, the Australian Parliament passed the Foreign Influence Transparency Scheme Act 2018[10] into law, which requires anyone who undertakes any activity on behalf of a foreign actor to register in the scheme. Under the act, registrants have the responsibility to disclose all of their activities — including those pertaining to social media communications — to the attorney-general, who maintains a widely accessible list for the citizenry, and, if there is any sort of undisclosed activity or breach, criminal charges may follow.[11] This counter-interference framework has been

7 See www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-coordinator.

8 See www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-strategy.

9 See www.aec.gov.au/media/disinformation-register.htm; www.aec.gov.au/about_aec/electoral-integrity.htm.

10 *Foreign Influence Transparency Scheme Act 2018* (No 63) (Cth), 2018, online: *Federal Register of Legislation* <www.legislation.gov.au/C2018A00063/latest/text>.

11 See www.ag.gov.au/integrity/foreign-influence-transparency-scheme.

proven effective by the Australian Security Intelligence Organisation (ASIO),[12] whose most recent annual report revealed that 95 percent of stakeholders have a medium or higher satisfaction with the agency's interference identification and policy recommendations (ASIO 2023, 32). Furthermore, Australia's framework is one of a kind: MIT Technology Review Insights (2022) determined that it ranked first among the world's top 20 economies in terms of critical infrastructure, organizational capacity and policy commitment to countering cyber-foreign interference.

Recommendations

The Government of Canada should aim to implement four key policies to effectively acknowledge and counter foreign interference through deterrence by denial:

- Adapt current mechanisms that counter foreign interference, specifically the CEIPP, to acknowledge the impact that cybersecurity breaches, particularly disinformation campaigns, may have on the citizenry .
- Build long-term digital resilience among diaspora communities through culturally sensitive and multilingual civic literacy campaigns led by community organizations and transparency portals.
- Increase collaboration between Elections Canada,[13] the Canadian Security Intelligence Service[14] and Communications Security Establishment Canada (CSE),[15] with the potential goal of establishing an interagency electoral integrity commission dedicated to social media surveillance and citizenry awareness.
- Establish minimum transparency requirements (Solomun, Polataiko and Hayes 2021) and enhance existing privacy-preserving practices for all social media, including Chinese-owned social media applications operating in Canada, so that excessive disinformation can be tamed without limiting contact among members of diaspora communities with relatives on the mainland. Canada may find it advantageous to include allies in this third initiative.

12 ASIO is Australia's national security agency, which is tasked with, among other duties, identifying, investigating and providing policy recommendations to counter foreign espionage and interference while upholding national interests.

13 Elections Canada is a non-partisan, independent agency whose mandate most notably includes conducting legislation-compliant federal elections and education programs about electoral processes; see www.elections.ca/content.aspx?section=abo&dir=mis&document=index&lang=e.

14 The Canadian Security Intelligence Service investigates actual or perceived threats to Canada's national security and conducts threat-reduction measures; see www.canada.ca/en/security-intelligence-service/corporate/mandate.html.

15 CSE is the technical authority for cybersecurity, maintaining active cyber operations and obtaining foreign intelligence either covertly or otherwise; see www.cse-cst.gc.ca/en/corporate-information/mandate.

Conclusion

Canada's system of governance is a desired alternative to more authoritarian regimes such as China, and that is worth sharing and celebrating with the diaspora. Notwithstanding, the rate at which the Chinese-Canadian diaspora has become a target for sophisticated propaganda campaigns is alarming and gives the Chinese government or other malicious actors the opportunity to target other diaspora communities that are systemically neglected. As it stands, Canada's counter-interference strategy is short-sighted and fails to dismantle China's disinformation machine by not taking advantage of the theories of deterrence. As the number of WeChat users increases year after year, Canada must take swift action to prevent larger impacts to its electoral integrity. The answer does not inherently lie with only technical means, especially not with banning foreign platforms. Rather, the Government of Canada should ensure there is enough awareness among its citizens, and also within the government, about MDMI efforts taking place and the impacts these may have on diaspora communities. For counter-interference efforts to be sustainable, civic literacy initiatives need to be not only put permanently in place but also culturally sensitive and linguistically accessible to avoid alienation or misrepresentation of identities. Canada should avoid divisive narratives; instead, it should consider Australia's lead and establish an electoral transparency portal that debunks mainstream disinformation in one click. Countering foreign interference is a continuous effort that requires a dedicated long-term approach that builds resilience among at-risk groups, by effectively embracing deterrence by denial.

Acknowledgements

I am grateful to the Centre for International Governance Innovation (CIGI) for the opportunity to be an undergraduate fellow of the Digital Policy Hub and to my peer reviewers (Christelle Tessono and Tyler Stevenson) and CIGI Senior Fellow Alex He, for their excellent advice. I would also like to extend a huge thank you to my research supervisor Andrea Charron (Centre for Defence and Security Studies, University of Manitoba) for her support, mentorship and guidance. Lastly, my utmost gratitude goes to my parents, whose sacrifice and resilience have allowed me to pursue opportunities like this one.

About the Author

Ivan Nuñez Gamez is a first-generation Latino-Caribbean immigrant pursuing a political studies (honours) and economics degree at the University of Manitoba. Throughout his undergraduate studies, he has remained dedicated to serving his peers through student-led advocacy and policy making, serving as the University of Manitoba Students' Union governance chair, a role in which he effectively ensured equitable representation for marginalized students in governing bodies and reformed electoral proceedings to increase engagement. He is an undergraduate fellow at the Digital Policy Hub, where his research will examine current strategies enacted by the federal government to counter technical foreign interference.

Works Cited

ASIO. 2023. *Annual Report 2022–23*. Canberra, Australia: ASIO. www.transparency.gov.au/publications/home-affairs/australian-security-intelligence-organisation/asio-annual-report-2022-23.

Canadian Centre for Cyber Security. 2022. "How to identify misinformation, disinformation, and malinformation." CSE. February. www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.

CBC News. 2023. "Former B.C. MP says he lost his seat due to China allegedly meddling in Canadian election." CBC News, March 3. www.cbc.ca/news/canada/british-columbia/former-bc-mp-says-he-lost-his-seat-china-alleged-elections-interference-1.6766168.

Committee on Homeland Security and Governmental Affairs. 2020. *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*. Staff Report. Permanent Subcommittee on Investigations, United States Senate. www.govinfo.gov/content/pkg/GOVPUB-Y4_G74_9-PURL-gpo142492/pdf/GOVPUB-Y4_G74_9-PURL-gpo142492.pdf.

Fung, Benjamin. 2024. "Foreign Interference in Canada's Academia, Democracy, and Diasporas." Research presented at the University of Manitoba, February 27.

Gold, Josh, Christopher Parsons and Irene Poetranto. 2020. "Canada's Scattered and Uncoordinated Cyber Foreign Policy: A Call for Clarity." Just Security, August 4. www.justsecurity.org/71817/canadas-scattered-and-uncoordinated-cyber-foreign-policy-a-call-for-clarity/.

Government of Canada. 2023. "Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions." April 6. www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Countering-an-Evolving-Threat.pdf.

Johnston, David. 2023. *First Report*. May 23. Ottawa, ON: Government of Canada. www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Independent-Special-Rapporteur%20-Report-eng.pdf.

Le Grip, Constance. 2023. *Report on behalf of the Commission of Inquiry relating to political, economic and financial interference by foreign powers – States, organizations, companies, interest groups, private individuals – aimed at influencing or corrupting opinion relays, leaders or French political parties*. June 1. Paris, France: French National Assembly. www.assemblee-nationale.fr/dyn/16/rapports/ceingeren/l16b1311-t1_rapport-enquete.

Mazarr, Michael J. 2018. "Understanding Deterrence." RAND Corporation, April 18. https://doi.org/10.7249/PE295.

MIT Technology Review Insights. 2022. *The Cyber Defense Index 2022/23*. Cambridge, MA: MIT. www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/.

Mozur, Paul. 2020. "Forget TikTok. China's Powerhouse App Is WeChat, and Its Power Is Sweeping." *The New York Times*, September 4. www.nytimes.com/2020/09/04/technology/wechat-china-united-states.html.

Office of the Director of National Intelligence. 2020. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public." Press release, August 7. www.dni.gov/index.php/newsroom/press-releases/press-releases-2020/3473-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

Schmitt, Michael N. 2021. "Foreign Cyber Interference in Elections." *International Law Studies* 97 (1): 739–64. https://digital-commons.usnwc.edu/ils/vol97/iss1/32/.

Senate Select Committee on Foreign Interference through Social Media. 2023. *Select Committee on Foreign Interference through Social Media*. August. Canberra, Australia: Senate Printing Unit. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000062/toc_pdf/SenateSelectCommitteeonForeignInterferencethroughSocialMedia.pdf.

Solomun, Sonja, Maryna Polataiko and Helen A. Hayes. 2021. "Platform Responsibility and Regulation in Canada: Considerations on Transparency, Legislative Clarity, and Design." *Harvard Journal of Law & Technology* 34: 1–18. www.mediatechdemocracy.com/all-work/platform-responsibility-and-regulation-in-canada-considerations-on-transparency-legislative-clarity-and-design.

Statistics Canada. 2023. "Chinese New Year and quality of life among Chinese in Canada." January 24. www.statcan.gc.ca/o1/en/plus/2816-chinese-new-year-and-quality-life-among-chinese-canada.