Centre for International
Governance Innovation

This policy brief is part of CIGI's project on freedom of thought: Legitimate Influence or Unlawful Manipulation?

Find out more at: www.cigionline.org/fot

Policy Brief No. 3 — January 2024

Foreign Interference Online: Where Disinformation Infringes on Freedom of Thought

Wesley Wark

Key Points

- Online disinformation operations by foreign state actors continue to be a prominent tool of disruption.
- Disinformation operates in a permissive information environment. In a functioning democracy, although disinformation can make the maintenance of freedom of thought more difficult, its potential impacts on freedom of thought are limited.
- Disinformation needs a rigorous definition, distinguishing it from other forms of false narratives, including misinformation, so that it can be recognized and the appropriate tools adopted to counter it in a democracy.
- The best tools to use in countering disinformation campaigns involve educating the public about how to recognize disinformation and building resilience in targeted and vulnerable communities.

Introduction

Foreign interference allegations involving Chinese state actors have rocked Canadian politics since the fall of 2022. The allegations have been driven by leaks of classified intelligence to the media, and have been ridden hard by opposition political parties who decry what they see as a lack of decisive government action in response. Parliamentary committees have played an important role in trying to hold the government to account for what are seen as failures in the Canadian system to counter foreign interference.[1] The issue is now the subject of a judicial inquiry, which will hold public briefings and submit reports in 2024.[2]

Although the experience of foreign interference is not unique to Canada, some of the dynamics of its recent expressions are. Allegations centre on efforts by Chinese officials based in Canada to influence electoral outcomes through a variety of methods, including targeted support to preferred candidates, the spreading of disinformation on social media and intimidation tactics used against specific political actors. Mixed in with intelligence leaks about these alleged tactics are accusations of other efforts by foreign actors to use intermediaries, often political staffers, to engage in espionage. Controversy

[1] For coverage of the Canadian debate, see the columns in Wesley Wark's substack newsletter on national security and intelligence at wesleywark.substack.com.

[2] See https://foreigninterferencecommission.ca/about/the-commission.

About the Author

Wesley Wark is a senior fellow at CIGI and a fellow with the Balsillie School of International Affairs. He recently retired from the University of Toronto's Munk School of Global Affairs and Public Policy, where he had taught since 1988. He served two terms on the prime minister of Canada's Advisory Council on National Security (2005–2009) and on the Advisory Committee to the President of the Canada Border Services Agency from 2006 to 2010. More recently, he provided advice to the minister of public safety on national security legislation and policy. He has appeared on numerous occasions before parliamentary committees and comments regularly for the media on national security issues.

Wesley is the co-editor (with Christopher Andrew and Richard J. Aldrich) of *Secret Intelligence: A Reader*, second edition (Routledge, 2019) and series editor (with Aaron Shull, CIGI's managing director and general counsel) of the CIGI digital essay series Security, Intelligence and the Global Health Crisis. He is a former editor of the journal *Intelligence and National Security* and now serves on the journal's advisory board.

has focused on disinformation and its potential election impacts.[3] A watchdog mechanism, involving a task force drawn from the intelligence agencies to monitor signs of election interference and an independent panel of five senior officials empowered to issue public warnings about known, serious interference threats, has been in operation since 2019.[4] The good news is that independent reviews of the 2019 and 2021 federal elections in Canada have found that foreign interference did not affect the conduct or outcome of free and fair elections.[5]

However, the objectives of such foreign interference campaigns might be both direct and indirect, in equal measure. A non-democratic state's intention to try to mess with electoral processes could overlap with a broader objective to sow seeds of doubt about the legitimacy of such democratic processes, even if nothing concrete in terms of swaying the electorate is achieved. Undermining democracy and faith in governance would be a clear win. Canadians are discovering that some of the characteristics of the Chinese state interference plans are similar to those of the Russian influence campaign unearthed in 2017 in the United States.

A US intelligence report on the Russian disinformation campaign targeting the US 2016 presidential election drew conclusions about Russia's intention. The report from the Office of the Director of National Intelligence (ODNI) assessed not only that the campaign was intended to undermine trust in the US electoral process but also that Russia used multiple tools to achieve its objective. The ODNI found that "Moscow's use of disclosures during the US election was unprecedented, but its influence campaign otherwise followed a longstanding Russian messaging strategy that blends covert intelligence operations — such as cyber activity — with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls'" (ODNI 2017, 2).

[3] See the policy brief by Alexa Raad (forthcoming 2024), which extends the discussion of disinformation used for foreign interference (and other purposes) to the technological enablers for influence operations: how content is targeted and fed to users, why information that is false has greater potential than true information for engagement and viral spread, and how influence campaigns can be "stymied, throttled or mitigated."

[4] See www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html.

[5] For the reports on the 2019 and 2021 elections, see, respectively, Judd (2020) and Rosenberg (2023).

Public attention to the issue of foreign state interference, such as that recently experienced in Canada, is the first indicator that freedom of thought principles might be in play. At the core of a concept of freedom, and the associated democratic rights, as Susie Alegre demonstrates, is freedom of thought. Alegre (2022, xvi–xvii) defines three branches: an ability to keep thoughts private; freedom from manipulation of thoughts; and protection against being penalized for thoughts alone.

Where might disinformation perpetrated by a foreign state actor touch on freedom of thought?

Manipulative Threats to Freedom of Thought

The most likely impact of foreign influence operations would be interference with Alegre's second category: freedom from manipulation of thoughts. Foreign state actors are unlikely to be able to reach from afar into the other two branches, although they could, of course, deploy repressive techniques to achieve such ends against their own populations. It could be argued that in its broadest form espionage targets private thoughts and that intimidation campaigns are a form of penalizing thought. But these are very expansive projections of threats and will not be considered further here. It may be sufficient to argue that espionage targets secrets, not private thoughts, and that intimidation campaigns, while mounted against dissidents and critics, especially among diaspora communities, target actions, including expressive speech, not private thoughts alone.

An abundance of tools are available to foreign state actors who intend to intrude into other societies for the purposes of influence or disruption. Among these tools, online influence operations hold primacy of place.

These tools can be applied broadly to three streams of information operations: misinformation; disinformation; and malinformation. These streams are distinct but also overlapping, with blurred boundaries. Canadian and US security agencies share common definitions for these three streams. Here are those offered by the Canadian Centre for Cyber Security: "*Misinformation* refers to unintentionally false information that is not intended to cause harm. *Disinformation* refers to intentionally false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction. *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, 12).

Two key properties are at work in these definitions: one is truth; the other is harm.

Truth and harm both have clear implications for the manipulation of thought. Doing harm follows from the deliberately false properties of disinformation and malinformation, and these two streams will be the focus when it comes to this brief's discussion of foreign interference.

Waging Cognitive Warfare Online

Foreign interference targeting democratic societies works not by the classic Orwellian formula of ruthless powers limiting sources of information and knowledge — that is, not by creating "memory holes," as the novel *Nineteen Eighty-Four* would have it[6] — but by pursuing an opposite effect. The opposite effect is *multiplying* and *amplifying* chosen channels of information, and attempting to corrupt the availability of true information in favour of that which is both false and harmful. At its most intense, foreign state actor campaigns of disinformation and malinformation amount to cognitive warfare, a hostile attempt to alter thinking.

The dangers posed by disinformation and malinformation involve the competitive "advantages" they may present, advantages that render true freedom of thought fragile. Freedom of thought is not undermined by disinformation and malinformation per se. Rather, the complex web of personal thinking has a permeable membrane, which admits all manner of information. That information competes for attention and traction in our personal, private mental world.

[6] See Orwell (1949).

How do we understand the competitive advantages of disinformation and malinformation? There are two distinct questions here. One is about how well a foreign state actor can identify and latch on to these competitive advantages to conduct cognitive warfare. The other is about how disinformation and malinformation find competitive traction in the inner sanctum of our thinking.

The Information Environment

To take advantage of disinformation and malinformation opportunities, a foreign state actor has to have significant knowledge of a target country's "information environment." The main actors in any interference operation are likely to be members of a foreign adversary's intelligence system; diplomats (or officials using diplomatic cover) posted to a target country; and local collaborators (proxies), both the witting and unwitting. There is likely a hierarchy of local knowledge at play, with local collaborators at the higher end of the spectrum; diplomats posted to a host country in the middle realm; and intelligence officials, operating from afar for the most part, at the lower end. Local collaborators can include private firms engaged by foreign state actors to conduct information operations.

A foreign state-directed information operation will often require significant staff and budget, including spending on research and development, resources the University of Oxford's Computational Propaganda Research Project calls "high cyber troop capacity" (Bradshaw, Bailey and Howard 2021, 18).

A recent threat assessment from the Australian Security Intelligence Organisation (ASIO) called particular attention to the role that proxies can play. The assessment highlighted an operation involving what ASIO called an influential "lackey," who targeted a group of Australian journalists as part of an interference campaign. Mapping out and trying to build connections with selected journalistic influencers on behalf of a foreign state (unnamed in this case) is a good illustration of attention to local knowledge (ASIO 2023).

Avenues for disinformation and malinformation might be identifiable across a journalistic community, particularly for foreign-language media and specific websites and messaging platforms serving diaspora communities, such as the Chinese WeChat app. Yet in-depth knowledge of the information environment may be very partial and influenced by foreign regime perceptions. Those officials with responsibility for creating information operation campaigns, whether operating within intelligence agencies or in a diplomatic service, are unlikely to have the full picture, and may possibly lack even a realistic picture, of the informational environment in a target democracy. The seminal *Weapons of Mass Distraction* report noted inherent problems in Chinese-sponsored media campaigns, finding that clear bias and problematic actions undermined such campaigns, leading to a conclusion that "Chinese journalists' efforts are aimed more at impressing their superiors than truly swaying hearts and minds overseas" (Nemr and Gangware 2019, 22).

In recent leaks of intelligence reports concerning Chinese interference in Canada, evidence of at least one election-related disinformation campaign has surfaced. During the Canadian election campaign in 2021, Chinese diplomats and local "proxies" were instructed to emphasize that the Conservative Party of Canada was too critical of China and would institute harmful policies if elected. The information operation was designed to suggest that the Conservatives would take an approach similar to that of Donald Trump's administration and would ban Chinese students from certain Canadian universities or education programs. The message for Chinese-Canadian voters, aside from playing on any anti-Trump feelings, argued that by extension voters' children would be affected because the Conservative Party would limit their kids' educational opportunities (Fife and Chase 2023).

Such an information campaign, if conducted at the behest of Beijing, illustrates a classic problem in thinking about disinformation as an intrusion into freedom of thought.

Intentions that animate a disinformation or malinformation campaign may be divorced from actual capabilities for a variety of reasons. We do not know if the "instructions" were ever carried out, or how widely. We also have no way to measure their impact. Did such a campaign have a capacity to reach people, which would arguably depend on its understanding of the information environment? Did it have an ability to change people's thinking or merely reinforce pre-existing beliefs? Or was it simply background "noise"?

Even without a fully accurate picture of the information environment of a target state, and weighed down by political bias and institutionalized careerist thinking, an information operation will still find many and diverse channels for disinformation and misinformation in a social media–saturated world.

Distinguishing between Impact and Noise

The Russian influence campaign during the US presidential elections in 2016 demonstrates this problem in full. The delivery of real harms depends on the opportunities these campaigns have to succeed, and on their difficult-to-measure impacts. As *Weapons of Mass Distraction* relates, "Kremlin-generated impressions were a drop in the bucket compared to total user activity [on the Twitter and Facebook platforms], which calls into question their ability to have played a decisive role in swaying public opinion" (Nemr and Gangware 2019, 18).

When it comes to China, the sheer volume of pro-China content broadcast by state media organs creates an inevitable exposure for diaspora communities in foreign states (ibid., 23).

Iran's comparatively lower-volume efforts, whether made for geopolitical effect or to boost Iran's impact as a military power, likely suffer from problems in generating real impacts in target diaspora audiences (ibid., 24).

While the impacts of these operations may be impeded and are difficult to measure, the opportunities to make an impact must be understood. Opportunities for disinformation and malinformation campaigns to land are generated through a combination of technological means, including largely unregulated platforms governed by business models (as Raad discusses[7]) and through the identity characteristics of potentially receptive, or vulnerable, audiences.

What are these identity characteristics? The first thing we can point to is that disinformation and malinformation's ability to go "viral" depends on the inculcation of "fearful unknowing" — a combination of fear, anxiety and emotional response — in the audience. Viral potentiality also depends on a herd mentality[8] stoked by an impression of a post's mass readership (whether real or imagined on the basis of, say, bot amplification, the herd equating many readers with greater truth) and a reinforcing notion of a shared community of knowledge, which is sometimes reduced to an echo chamber (Dyer et al. 2008).

Steps to Counter Information Operations

The challenge of reducing a target audience's vulnerabilities to disinformation and malinformation is compounded because some of the suggested strategies to protect freedom of thought also involve sending messages into the information environment. Suggested strategies include deploying various counter-narratives. These counter-narratives can entail repeated injections of facts and evidence into the information environment; pre-emptive warnings about sources and narratives; the use of debunking narratives; and the encouraging of being open to differing viewpoints. But all of these strategies themselves have the potential to intrude on freedom of thought, and all are difficult undertakings with uncertain metrics for success (Nemr and Gangware 2019, 13).

Whether technological tools will, on balance, help reduce vulnerabilities to disinformation or malinformation, or instead deepen them through such things as the proliferation of deepfakes and synthetic imagery, is an open question.

In any consideration of societal vulnerabilities and freedom of thought, the ability of disinformation and malinformation campaigns to actually alter thinking must be a key concern. Campaigns with this ability are distinguishable from information operations that simply contribute to the

[7] See Raad (forthcoming 2024).

[8] See ScienceDaily (2008) and Dyer et al. (2008) regarding a "herd mentality" study conducted by the University of Leeds.

background noise in an information environment without noticeable impact, or which serve merely to reinforce existing views and outlooks.

A working hypothesis, perhaps provocative, might be that state-sponsored disinformation and malinformation campaigns are rarely able to actually change societal thinking, that is, to have real manipulative effect on freedom of thought. But they can pollute an information environment by adding "noise," making the exercise of freedom of thought more difficult. They can also reinforce existing mental maps, thereby further eroding any free ability to contest ideas, in the form of an internal mental debate.

Freedom of thought includes the freedom to hold beliefs, what may be called "lawful but awful" ideas. Disinformation and malinformation campaigns that purposefully strengthen lawful but awful concepts, in the interests of some foreign state actor's policy objectives — to steer an election, undermine faith in democracy, deepen polarization, fuel disruptive conspiracy theories, chill dissent — do not directly amount to the manipulation of freedom of thought. What they can accomplish is a mission to make freedom of thought more difficult.

Foreign state information operations can be countered in a variety of ways. The most promising involve:

→ public education about the nature of the threat, particularly through published threat assessments;

→ various forms of "threat reduction measures" to disrupt such operations, typically carried out by intelligence and law enforcement agencies;

→ special protections for electoral processes through intelligence-backed warnings, regulations and laws; and

→ close engagement with targeted communities in society to ensure they enjoy maximum protection of their freedoms.

The Canadian government is currently exploring the creation of a foreign influence transparency registry, to try to reduce the potential for foreign state actors to deceptively engage in influence campaigns through Canadian intermediaries. Under the proposed scheme, such Canadian intermediaries would be required to register activities they undertake that are directly sponsored by a "foreign principal" (a foreign state or state-connected entity).[9]

A recent report by the Canadian non-governmental organization Alliance Canada Hong Kong (ACHK), entitled *Murky Waters: Beijing's Influence in Canadian Democratic and Electoral Processes*, advances important recommendations around enhancing government outreach to targeted diaspora communities, stressing the need for "an overarching strategy for culturally and linguistically sensitive outreach, as well as community-specific action plans that align with their interests and cultural experiences" (ACHK 2023, 40). The ACHK report also advocates funding of independent channels of information, to make communities targeted by foreign interference "less susceptible to foreign influence and [to] promote independent community-based services" (ibid., 41).

Foreign interference seeks out individuals and societal groups vulnerable to online influence campaigns. Diaspora communities are inevitably in their sights. Countering foreign interference involves an especial effort to protect the freedom of thought of such vulnerable communities; it also requires a broader effort to protect society as a whole.

The counter-foreign interference tool box begins and ends with public education for all and measures to create greater resilience in targeted populations, especially by helping to ensure the maintenance of an information environment where disinformation is rightly seen as background noise, nothing more. Ensuring that disinformation remains noise and cannot escape its own limitations requires a genuine understanding of the technological enablers of false information flows.[10]

Recommendations

This discussion leads to three key recommendations aimed to protect freedom of thought in the context of countering foreign disinformation campaigns:

[9] See www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nfluence/index-en.aspx.

[10] That subject will be explored in Alexa Raad's policy brief in this series (forthcoming 2024).

- Government national security and intelligence systems must play a lead role in enhancing, on a systemic basis, public understanding of all national security threats, including threats posed by disinformation.

- Public understanding of how disinformation might infringe on freedom of thought through manipulation of thinking must be based on a balanced appreciation of, on the one hand, the inherent weaknesses of disinformation campaigns in a democratic system, and on the other hand, the strengths of the opportunities the system offers for this influence.

- The perils presented by disinformation efforts to manipulate freedom of thought most threaten targeted individuals and communities, in particular those of a diaspora. Vulnerable diaspora communities need support and understanding in maintaining their resilience. Key elements of that support are sensitive outreach and engagement by government, and opportunities for enhancing local resistance to disinformation through community funding initiatives.

Works Cited

ACHK. 2023. *Murky Waters: Beijing's Influence in Canadian Democratic and Electoral Processes.* Ottawa, ON: ACHK. https://alliancecanadahk.com/wp-content/uploads/2023/05/ACHK_Murky_Waters_Bejings_Influence_in_Canadian_Democratic_and.pdf.

Alegre, Susie. 2022. *Freedom to Think: Protecting a Fundamental Human Right in the Digital Age*. London, UK: Atlantic Books.

ASIO. 2023. "Annual Threat Assessment 2023 — Director-General of Security." February 21. YouTube video, 40:53. www.youtube.com/watch?v=4YqS_Av--58.

Bradshaw, Samantha, Hannah Bailey and Philip N. Howard. 2021. *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation.* Oxford, UK: Computational Propaganda Project. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf.

Canadian Centre for Cyber Security. 2022. "An Introduction to the Cyber Threat Environment." CAT D96-9/2022. Ottawa, ON: Communications Security Establishment. www.cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf.

Dyer, John R. G., Christos C. Ioannou, Lesley J. Morrell, Darren P. Croft, Iain D. Couzin, Dean A. Waters and Jens Krause. 2008. "Consensus decision making in human crowds." *Animal Behaviour 75* (2): 461–70. https://doi.org/10.1016/j.anbehav.2007.05.010.

Fife, Robert and Steven Chase. 2023. "CSIS documents reveal Chinese strategy to influence Canada's 2021 election." *The Globe and Mail*, February 17. www.theglobeandmail.com/politics/article-china-influence-2021-federal-election-csis-documents/.

Judd, James. 2020. *Report on the assessment of the Critical Election Incident Public Protocol.* Ottawa, ON: Government of Canada. www.canada.ca/content/dam/di-id/documents/rpt/CEIPP-rpt-eng.pdf.

Nemr, Christina and William Gangware. 2019. *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age.* Washington, DC: Park Advisors. www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

ODNI. 2017. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution." Washington, DC: ODNI. www.dni.gov/files/documents/ICA_2017_01.pdf.

Orwell, George. 1949. *Nineteen Eighty-Four.* 1st ed. London, UK: Secker and Warburg.

Raad, Alexa. Forthcoming 2024. *Protecting Freedom of Thought: Mitigating Technological Enablers of Disinformation.* Legitimate Influence or Unlawful Manipulation? Policy Brief No. 4. Waterloo, ON: CIGI.

Rosenberg, Morris. 2023. *Report on the Assessment of the 2021 Critical Election Incident Public Protocol.* Ottawa, ON: Privy Council Office. www.canada.ca/content/dam/di-id/documents/rpt/CEIPP-rpt-eng.pdf.

ScienceDaily. 2008. "Sheep In Human Clothing: Scientists Reveal Our Flock Mentality." Science News, February 16. www.sciencedaily.com/releases/2008/02/080214114517.htm.

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.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
CIGI Senior Fellow and Project Co-Leader Susie Alegre
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Lynn Schellenberg
Senior Publications Editor Jennifer Goyder
Graphic Designer Abhilasha Dewan

This policy brief was made possible thanks to the financial support of the Konrad-Adenauer-Stiftung (KAS) Canada.

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.

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