

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Maligned Influence and Interference in Canada

by Dave McMahon

July 2023

POLICY PERSPECTIVE

MALIGNED INFLUENCE AND INTERFERENCE IN CANADA

by Dave McMahon

July 2023



CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

©2023 Canadian Global Affairs Institute
ISBN: 978-1-77397-274-9

Foreign influence, interference, disinformation, deception and disruption are entwined tools of modern statecraft – referred to collectively as cognitive warfare. While Canada likes to keep cognitive and cyber-operations in clean doctrinal boxes, these days disinformation is accelerated, amplified and propagated by the internet. Similarly, most cyber-attacks are facilitated through social engineering, phishing and other means of hacking the wetware of the user's brain. Cyber- and cognitive warfare domains are both converged and fluid.

The scope of potential foreign interference activities can be broad, encompassing a range of techniques familiar to intelligence agencies. These include human intelligence operations, the use of state-sponsored or foreign-influenced media and the use of sophisticated cyber-tools.[1]

The framework in which Canada defines, understands and operates across the information domain is mismatched with our competition. This paper will examine how our adversaries perceive and weaponize the information domain in ways that may differ from our own and each other. We are playing this game with different rules and objectives.

First, some definitions. Disinformation is misinformation deliberately spread to deceive people. Malinformation is information that is true, often private or confidential, that is intentionally leaked to inflict actual harm.

Cognitive warfare can be functionally defined as "the weaponization of public opinion, by an external entity, for the purpose of influencing public and governmental policy and destabilizing public institutions".[2] Cognitive warfare activities are conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting or disrupting individual and group cognitions to gain an advantage. These activities vary greatly and may encompass supporting or conflicting cultural or personalized components – social psychology, game theory and ethics are all contributing factors. Our adversaries conduct cognitive warfare throughout the continuum of conflict and aim to stay in the grey zone below the threshold of armed conflict.[3] Canadian doctrine, policy and mandates don't appreciate shades of grey.

Pacing Threats

A 2019 report written by Clairvoyance Cyber Corp. for Public Safety Canada prophetically stated that "hostile intelligence services and militaries will continue to exploit, interfere with and influence Canadian interests domestically and abroad, using cyber as part of a broader hybrid warfare campaign. And China's strategy particularly, which includes activities by Chinese tech

[1] Public Safety Canada, "Foreign Interference – China's Use of the United Front Work Department," June 9, 2020, https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20200930/015/index-en.aspx.
[2] A. Bernal et al., "Cognitive Warfare: An Attack on Truth and Thought," NATO, 2020, https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20Warfare.pdf
[3] Ibid., "Cognitive Warfare: Strengthening and Defending the Mind," April 5, 2023, https://www.act.nato.int/articles/cognitive-warfare-strengthening-and-defending-mind.

companies, will attempt to control Canadians through disinformation, interference, media manipulation, psychological warfare and legal warfare."[4]

China and Russia maintain vast disinformation ecosystems and run sophisticated operations-at-scale against domestic and global target audiences. The open nature of liberal society and democratic institutions makes it difficult to effectively counter grey-zone operations.[5] Robert Joyce of the U.S. National Security Agency said, "I kind of look at Russia as the hurricane. It comes in fast and hard. China, on the other hand, is climate change: long, slow, pervasive."[6]

The National Security and Intelligence Committee of Parliamentarians (NSICOP) released a Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack. In the report, NSICOP and CSE quote industry sources who recognize that Russia engages in malicious cyber-threat activity, including cyber-espionage and foreign interference, to support a wide range of strategic intelligence priorities. These include the identification of divisive events and trends in rival states to conduct influence campaigns and undermine liberal democratic norms and values.[7] Foreign states veer from diplomacy into foreign interference when their influence activities are covert, deceptive or threatening. But there is also a considerable grey zone in which activities might appear largely benign.[8] Again, more grey.

The Russian and Chinese states exercise control over domestic media, which targets foreign diasporas through native language programming and platforms such as VKontakte (VK), Telegram and WeChat. The targeting of English-speaking native communities in Canada by adversaries is a bit more nuanced. Here, foreign influence is often directed at fringe groups. Russia targets left- and right-wing groups in Canada and those who are prone to believing in conspiracies.[9] China tries to prevent public inquiry into its influence campaigns, as the *National Post* commented: "Dismissing worries over election interference as 'racism' is part of a well-known China propaganda tactic."[10] The spectre of foreign interference with democratic

[4] Sam Cooper, "China, Russia, Exploiting High-Tech in 'Hybrid Warfare' Costs Up to $100B in Canada: Report," Global News, June 24, 2021, https://globalnews.ca/news/7975330/china-russia-exploiting-high-tech-hybrid-warfare-cost-billions-canada/.
[5] Sze-Fung Lee, "How Beijing's Disinformation Campaign Threatens International Security in the Post-Truth Era," Modern Diplomacy, 2021, https://moderndiplomacy-eu.cdn.ampproject.org/c/s/moderndiplomacy.eu/2021/11/25/how-beijings-disinformation-campaign-threatens-international-security-in-the-post-truth-era/amp/.
[6] Andy Langenkamp, "From Russian Rain to Chinese Storm," The Hill, May 8, 2022, https://thehill.com/opinion/national-security/3479964-from-russian-rain-to-chinese-storm/.
[7] National Security and Intelligence Committee of Parliamentarians (NSICOP), "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," February 14, 2022, https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-en.html.
[8] Government of Canada, "First Report: The Right Honourable David Johnston, Independent Special Rapporteur on Foreign Interference," n.d., https://www.canada.ca/en/democratic-institutions/services/reports/first-report-david-johnston-independent-special-rapporteur-foreign-interference.html.
[9] Brian McQuinn, Marcus Kolga, Cody Buntain and Laura Courchesne, "Enemy of My Enemy: Russian Weaponization of Canada's Far Right and Far Left to Undermine Support to Ukraine," Centre for Artificial Intelligence, Data, and Conflict (CAIDAC), University of Maryland College of Information Studies and Digital Public Square, March 2023, https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf.
[10] Terry Glavin, "Beijing Apologists Have Conjured a Racist Bogeyman. It's Total Nonsense," *National Post*, March 31, 2023, https://nationalpost.com/opinion/beijing-apologists-have-conjured-a-racist-bogeyman-its-total-nonsense.

institutions is particularly corrosive because it can damage the public's trust in the electoral process, which is essential to a functioning democracy.[11]

Both Russia and China use disinformation as a weapon to disrupt and harm the Canadian economy and the democratic socio-political framework. Their strategy is to empower organic disinformation nodes and fuel opposition within Canada. Meanwhile, both powers employ traditional agents of espionage, influence and interference.

Russia

Kremlin military and intelligence thinkers talk about information not in the familiar terms of persuasion, public diplomacy or even propaganda, but in weaponized terms, as a tool to confuse, blackmail, demoralize, subvert and paralyze.[12]

The U.S. Department of State Global Engagement Centre explains that Russia's disinformation and propaganda ecosystem is the collection of official, proxy and unattributed communication channels and platforms that Russia uses to create and amplify false narratives.[13] There is no single media platform for propaganda and disinformation. Nor is there uniformity of messages among different sources. Individual messages within the system may appear contradictory. The ecosystem approach is fitting for this dynamic because it does not require harmonization among the different pillars.[14] This provides strategic ambiguity in the information ecosystem.

In the weeks and months leading up to Russia invading Ukraine on February 24, 2022, the Kremlin and pro-Kremlin media employed false and misleading narratives to justify military action against Ukraine, mask the Kremlin's operational planning and deny any responsibility for the coming war. Collectively, these narratives served as President Vladimir Putin's casus belli to engage in a war of aggression against Ukraine.[15]

Since the invasion, competition in the information space has intensified. Despite pervasive efforts to spread maligned narratives about Ukraine, it appears that Ukraine and its allies are, in key respects, winning the war[16] in the information space across most of the transatlantic community. The report, *Shielding Democracy: Civil Society Adaptations to Kremlin Disinformation about Ukraine*, identified three allied advantages: deep preparation, open networks of co-operation and

[11] Jean-Nicolas Bordelau, "Securing Elections: A Comparative Assessment of Canada's Response to Foreign Interference," Centre for International and Defence Policy 7:3, July 2021; Pippa Norris, *Why Electoral Integrity Matters* (Cambridge: Cambridge University Press, 2014).
[12] Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," The Interpreter, The Institute of Modern Russia, n.d., https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.
[13] U.S. Department of State Global Engagement Centre, "GEC Special Report: Pillars of Russian Disinformation and Propaganda Ecosystem," n.d. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.
[14] Ibid.
[15] Atlantic Council, "Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression Against Ukraine," n.d., https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/.
[16] The efficacy of influence campaigns is constantly being measured through surveys, target audience analysis and social media analytics in much the same way as a commercial marketing campaign is measured. This is a mature science.

active use of new technology. All of these have allowed civil-society organizations and governments in Ukraine and Central and Eastern Europe to build trust.[17]

Sometimes, anti-West propaganda or disinformation is used to support Russian foreign policy objectives, such as promoting pro-Russian sentiment and advancing Russia's geopolitical interests,[18] while destabilizing rival governments in fragile states such as those in Africa.[19] Russia seeks to create opportunities through chaos and is opportunistic in spinning up disinformation campaigns such as with the pandemic or for an election. Some examples of Russian disinformation campaigns include promoting bizarre conspiracy theories and spraying a "fire hose of falsehoods."[20] These campaigns often involve the use of bots, trolls and other automated systems to amplify their message in mainstream channels and home-grown conspiracy movements like QAnon to make it appear more credible.[21]

China has been trying to promote the adoption of Chinese 5G technology under the Belt and Road Initiative, whereas Russia is trying to literally burn it all down because its own fifth-generation initiatives have stalled owing to a lagging information communications technology supply chain.[22] Some Canadian followers who believed Russian disinformation about 5G have torched cell towers in Canadian cities.[23] Online disinformation also ironically hampers China's grand initiatives for data supremacy and artificial intelligence, which relies on the veracity of big data.

China

The Chinese government fuses a whole-of-society approach for collecting intelligence and propagating disinformation. This sets it apart from anything undertaken by Western governments.[24] Attempts at foreign interference are ubiquitous, especially from the PRC.[25]

A report on China's propaganda and disinformation landscape concludes that "the Chinese Communist Party (CCP) is not copying Russia's playbook when it comes to propaganda and disinformation—they're authoring their own" with the benefit of advanced technology and human

[17] Adam Fivenson, Galyna Petrenko, Veronika Víchová and Andrej Poleščuk, "Shielding Democracy: Civil Society Adaptations to Kremlin Disinformation about Ukraine," NED Forum, February 2023, https://www.ned.org/wp-content/uploads/2023/02/NED_FORUM-Shielding-Democracy.pdf.
[18] Pomerantsev and Weiss.
[19] David Ehl, "Russia's Wagner Group in Africa: More Than Mercenaries," *Deutsche Welle*, June 24, 2023, https://www.dw.com/en/more-than-mercenaries-russias-wagner-group-in-africa/a-64822234.
[20] Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," Rand Corporation, 2016, https://www.rand.org/pubs/perspectives/PE198.html.
[21] Dave McMahon, "Cognitive War and Information Peacekeeping," Sapper Labs Group, December 20, 2021, https://www.sapperlabs.com/post/cognitive-war-and-information-peacekeeping.
[22] Adam Satariano and Davey Alba, "Burning Cell Towers Out of Baseless Fear They Spread the Virus," *New York Times*, April 10, 2020, https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html.
[23] Kelvin Chan, Beatrice Dupuy and Arijeta Lajka, "Conspiracy Theorists Burn 5G Towers Claiming Link to Virus," CTV News, April 21, 2020, https://www.ctvnews.ca/health/coronavirus/conspiracy-theorists-burn-5g-towers-claiming-link-to-virus-1.4905039.
[24] Calder Walton, "China Has Been Waging a Decades-long All-out Spy War," *Foreign Policy*, March 28, 2023, https://foreignpolicy.com/2023/03/28/china-has-been-waging-a-decades-long-all-out-spy-war/.
[25] Government of Canada, "First Report … David Johnston."

resources.[26] The Chinese government continues to conduct global, covert, cyber-enabled influence operations. Those operations are now more frequent, increasingly sophisticated and increasingly effective.[27]

There are plenty of credible reports[28] of illegal activities overseen by Chinese diplomats in Canada, involving election interference,[29] Chinese "police stations",[30] military researchers entering our country on falsified visa applications on a mission to obtain sensitive Canadian technologies or harassing Canadians, including those of Uyghur and Tibetan origin[31] who speak their minds about China's human rights violations. In assembling its sphere of influencers, Beijing targets occupations that retired politicians and senior civil servants tend to move to, after careers spent serving the public trust.[32] Illegal police stations are just the tip of the iceberg.[33]

China recruits millions of its citizens as keyboard warriors to influence public opinion online and manipulate the truth on a massive scale similar to the troll farms in Russia or traditional mass line signals intelligence collection. These recruits are known as the "50 cent army" because they are paid 0.5 yuan per post.

Recently, Beijing has shifted towards covert, maligned Russian-style tactics, aggressive "wolf warrior"[34] online diplomacy and attacking Western media directly. For example, the Chinese state media shifted blame away from the origins of COVID by spreading the rumour that the virus was an American bioweapon.[35] Chinese Twiplomacy[36] has varied wildly in content and form engagement, suggesting the lack of a co-ordinated approach by the Chinese diplomatic corp.

---

[26] Clint Watts, "China's Propaganda and Disinformation Landscape: 2021 Snapshot," Substack, November 19, 2021, https://clintwatts.substack.com/p/chinas-propaganda-and-disinformation.
[27] Albert Jang, Tilla Hoja and Jasmine Latimore, "Gaming Public Opinion: The CCP's Increasingly Sophisticated Cyber-enabled Influence Operations," Australian Strategic Policy Institute, April 26, 2023, https://www.aspi.org.au/report/gaming-public-opinion.
[28] Dylan Robertson, "'Persona Non Grata': Canada Expelling Chinese Diplomat After Threats to Conservative MP," CTV News, May 8, 2023, https://www.ctvnews.ca/politics/persona-non-grata-canada-expelling-chinese-diplomat-after-threats-to-conservative-mp-1.6389430.
[29] Crispin Thorold, "Canada Claims China Interfered in its Elections," NPR, March 19, 2023, https://www.npr.org/2023/03/19/1164585528/canada-claims-china-interfered-in-its-elections.
[30] Leyland Cecco, "Canada Issues 'Cease and Desist' Warning to China Over 'Police Stations' in Ottawa," *The Guardian*, December 1, 2022, https://www.theguardian.com/world/2022/dec/01/canada-china-police-stations-cease-and-desist-warning.
[31] Raphael Tsvakko Garcia, "China's Harassment of Minority Groups Spills Out Beyond its Borders," Open Canada, July 19, 2019, https://opencanada.org/chinas-harassment-of-minority-groups-spills-out-beyond-its-borders/.
[32] Charles Burton, "To Protect Canadian Sovereignty, We Need Transparency about Foreign Influence: Charles Burton in the *Ottawa Citizen*," Macdonald Laurier Institute, April 27, 2023, https://macdonaldlaurier.ca/to-protect-canadian-sovereignty-we-need-transparency-about-foreign-influence-charles-burton-in-the-ottawa-citizen/.
[33] Danielle Pletka, "The Long Arm of China's Overseas Influence Operations," *Foreign Policy*, April 27, 2023, https://foreignpolicy.com/2023/04/27/china-ccp-spying-us-police-stations-influence-operations/.
[34] Wolf warrior diplomacy is a style of coercive diplomacy adopted by Chinese diplomats in Xi Jinping's administration; it is noted for being confrontational and combative. The term was coined from the Chinese action film *Wolf Warrior 2*.
[35] Steven Lee Myers, "China Spins Tale That the U.S. Army Started the Coronavirus Epidemic," *New York Times*, March 13, 2020, https://www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html.
[36] Michele Kelemen, "Twitter Diplomacy: State Department 2.0", *NPR*, February 21, 2012, https://www.npr.org/sections/alltechconsidered/2012/02/21/147207004/twitter-diplomacy-state-department-2-0

The Canadian Battleground

A 2021 Global News report[37] claimed that a network of websites linked to Russia had been spreading false and misleading information about COVID-19 in Canada. The report alleged that the websites were spreading conspiracy theories and misinformation about the origins and spread of the virus, as well as promoting unproven treatments and remedies. A report by the Council of Canadian Academies claimed that COVID-19 misinformation contributed to more than 2,800 Canadian deaths and cost $300 million.[38] That is four times the number of Canadian soldiers who have died in conflicts since the Second World War.

The Conversation[39] reported that "Canadians are being exposed to pro-Kremlin propaganda. Slightly over half of Canadians (51 per cent) reported encountering at least one persistent, false claim about the Russia-Ukraine war on social media pushed by the Kremlin and pro-Kremlin accounts. The most prevalent claim, encountered by 35 per cent of Canadians, was Ukrainian nationalism is a neo-Nazi movement."

The Report of the Public Inquiry into the 2022 Public Order Emergency discussed social media, social movements and the problems of mis- and disinformation. It is clear from the evidence the inquiry heard that social media played a critical role in shaping the Freedom Convoy. Social media platforms were the tools by which organizers met, co-ordinated and connected with participants. But these platforms do not only permit social movements to organize at a previously unachievable rate and scale. Social media also allows hate speech, propaganda, conspiracy theories and lies to spread farther, faster and cheaper than ever before. This too was an important dynamic both before and during the Freedom Convoy protests. False beliefs that COVID-19 vaccines manipulate DNA, social media feeds rife with homophobic or racist content and inaccurate reporting of important events all featured in the evidence.[40]

According to the National Observer,[41] home-grown protesters who participated in Canada's Freedom Convoy last year were aided by the Russian state-funded propaganda outlets to exploit their grievances, amplify social divisions and delegitimize the Trudeau government. Ironically, the Chinese government had allegedly[42] been trying get the Liberals re-elected at the same time.

The independent special rapporteur on foreign interference[43] concluded "there is no doubt that foreign governments are attempting to influence candidates and voters – a fact successive federal

[37] Ashleigh Stewart, "The Great COVID-19 Infodemic: How Disinformation Networks Are Radicalizing Canadians," Global News, December 18, 2021, https://globalnews.ca/news/8450263/infodemic-covid-19-disinformation-canada-pandemic/.
[38] Darren Major, "COVID-19 Misinformation Cost at Least 2,800 Lives and $300M, New Report Says," CBC, January 26, 2023, https://www.cbc.ca/news/politics/cost-of-covid-19-misinformation-study-1.6726356.
[39] The Conversation, "Russian Propaganda is Making Inroads with Right-wing Canadians," July 17, 2022, https://theconversation.com/russian-propaganda-is-making-inroads-with-right-wing-canadians-186952.
[40] Public Order Emergency Commission, "Final Report," n.d., https://publicorderemergencycommission.ca/final-report/.
[41] Caroline Orr, "Russia Used State-funded Propaganda Outlet to Whip Up Support for the 'Freedom Convoy' and Undermine the Trudeau Government," National Observer, February 10, 2023, https://www.nationalobserver.com/2023/02/10/analysis/russian-propaganda-freedom-convoy-disinformation.
[42] Robert Fife and Steven Chase, "China Views Canada as a 'High Priority' for Interference: CSIS Report," *Globe and Mail*, May 1, 2023, https://www.theglobeandmail.com/politics/article-china-targets-mps-csis/.
[43] Government of Canada, "First Report … David Johnston."

governments have known about for many years." A rudimentary Google search will turn up media reporting dating back decades.

Project Sidewinder is a 1997 declassified study[44] investigating Chinese intelligence services and Triads Financial Links in Canada.[45] The study's key allegation was that "a number of Canadian politicians are under the influence of Chinese intelligence." The investigation was conducted by a Canadian Security Intelligence Service (CSIS) and Royal Canadian Mounted Police (RCMP) joint task force and reported to political leadership – 26 years ago. It controversially argued that Chinese intelligence and Triads have been working together on intelligence operations in Canada. Independent researchers cite the report as part of a long line of evidence showing the influence operations of the United Front in Canada.[46] Today, we know much of this to be true and an integral part of China's Unified Front Strategy. On June 9, 2020, the Australian Strategic Policy Institute (ASPI) published an analysis of the CCP's use of the United Front Work Department (UFWD) as a primary foreign interference tool.

The CSIS public report, released on May 20, 2020, stated that espionage and foreign-influenced activities are almost always conducted to further the interests of a foreign state. NSICOP's 2020 annual report outlined foreign interference activities, including the targeting of Canadian institutions by threat actors, and pointed to China and Russia as being particularly active. In 2020, Public Safety Canada posted that CSIS has longstanding investigations into foreign interference threat activities targeting democratic processes and institutions across Canada.[47] National security advisor Jody Thomas testified to a Commons committee on March 1, 2023 that the prime minister had been briefed regularly about foreign interference in Canadian elections, which has been a persistent and growing threat coming largely from China.[48]

State-sponsored disinformation, maligned influence and foreign interference often operate in the shadows and through intermediaries, cutouts, front companies' agents of influence and proxies. These proxy sites play an important role for Russian disinformation. The Internet Research Agency (IRA) linked to Russian oligarch Yevgeny Prigozhin, based in St. Petersburg, Russia, are engaged in online propaganda and influence operations on the Kremlin's behalf. The IRA was indicted[49] in 2018 for illegal interference in the 2016 presidential elections and actively operates against Canada as well. Prigozhin also owns the Wagner Group, a private paramilitary army of Russian President Vladimir Putin, and a sanctioned transnational criminal organization and terrorist group. A special report on Russian mercenaries, privateers and proxies says "the Wagner Group is one of the most serious threats to peace in Europe and Africa. They are engaged in

[44] Granite Adams Unger, "Red Scare Three: Now with Chinese Characteristics," The Journal of Intelligence, Conflict, and Warfare, 4 (1): 21–39: May 31, 2021, doi:10.21810/jicw.v4i1.2748. ISSN 2561-8229. S2CID 236416375.
[45] Government of Canada Publications, n.d., https://publications.gc.ca/collections/Collection/JS71-1-2000E-2.pdf.
[46] Andrew Mitrovica and Jeff Sallot, "China Set Up Crime Web in Canada, Report Says," *Globe and Mail*, April 29, 2000, https://www.theglobeandmail.com/news/national/china-set-up-crime-web-in-canada-report-says/article4163320/.
[47] Public Safety Canada, "Foreign Interference: China's Use of the United Front Work Department," June 9, 2020, https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20200930/015/index-en.aspx.
[48] Ryan Tumilty, "Trudeau Was Regularly Briefed on Foreign Interference in Elections, National Security Adviser Says," *National Post*, March 1, 2023, https://nationalpost.com/news/politics/canada-elections-foreign-interference-committee.
[49] U.S. Department of Justice, "United States of America v. Internet Research Agency," Case 1:18-cr-00032-DLF, https://www.justice.gov/file/1035477/download.

violence, war crimes, propaganda, influence, interference, and dis-information operations on a large scale."[50]

Closer to home, the U.S. State Department[51] identified the Montreal-based Global Research platform as a major Kremlin-aligned proxy amplifying Russian propaganda and disinformation.

CSIS[52] and the Communications Security Establishment[53] have both published concerns that Russian state-sponsored disinformation campaigns are distorting Canada's effort to help Ukraine defend itself. Russian disinformation is considered a serious threat to democratic societies, as it can undermine public trust in institutions and create division among citizens.

The recent joint report by the Centre for Artificial Intelligence, Data, and Conflict (CAIDAC) investigated Russian weaponization of Canada's far right and far left.[54] The research found that the far-right and far-left communities in Canada are increasingly polarized and their rhetoric has been shifted from differences over policy to framing opponents as enemies who pose an existential threat to Canada. The far-right and far-left networks in Canada are among the most active online political communities. Russian-aligned networks produced 27 times more content and three times as much engagement with Canadian members of Parliament than did legitimate Canadians.[55]

Researcher Marcus Kolga, founder of Disinfowatch, writes that the Russian government continually monitors Western societies for divisive issues to exploit. Once such issues are identified, Russian mouthpieces and proxies inject and amplify these narratives in our information environment to intensify political divisions.[56]

Analysis found that Russian influence operations integrated sophisticated narratives with incendiary images and videos tailored to Canadian audiences, and average Canadians unwittingly amplify Russian influence operations. The campaign's responsive nature to trending issues and the breadth and volume of the narratives produced suggest a well-funded effort by the Russian government and its proxies. Pro-Russian accounts ramped up influence operations in Canada three months before the invasion and built a supportive ecosystem.[57]

The recent Chinese disinformation campaigns have focused on the treatment of Canadian citizens of Chinese origin, allegations of systemic racism against Canada and tarnishing Canada's reputation in international trade. China continues to threaten the Canadian agriculture sector and food safety, by spread disinformation that its inspectors had found pests in samples of Canadian

[50] Sapper Labs Group, "The Spectre of Violence: Maligned Influence and Interference," February 6, 2023, https://www.sapperlabs.com/post/the-spectre-of-violence-maligned-influence-and-interference.
[51] U.S. Department of State GEC, "Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem"
[52] CSIS, "Who Said What? The Security Challenges of Modern Disinformation," February 2018, https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_eng.pdf.
[53] Government of Canada, "How to Identify Misinformation, Disinformation, and Malinformation," Canadian Centre for Cyber Security, February 2022, https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.
[54] McQuinn, Kolga, Buntain and Courchesne.
[55] Ibid.
[56] Marcus Kolga, "Confusion, Destabilization and Chaos: Russia's Hybrid Warfare Against Canada and Its Allies," Canadian Global Affairs Institute, October 2021, https://www.cgai.ca/confusion_destabilization_and_chaos_russias_hybrid_warfare_against_canada_and_its_allies.
[57] McQuinn, Kolga, Buntain and Courchesne.

canola. Canola is the number one cash crop for many farmers across the Prairies. China imports $2.8 billion worth of Canadian canola annually, amounting to about 40 per cent of Canada's exports of the crop. Disinformation can do profound financial damage.[58]

Reaction

The Canadian government has taken steps to address concerns about foreign interference, including the creation of a dedicated co-ordination office and the passing of legislation[59] to strengthen election security and foreign interference prevention. However, it is doubtful whether covert Russian and Chinese operatives will be signing on to Canada's foreign influence transparency registry[60] any time soon.

In March 2023, the Prime Minister's Office announced the following measures:

- Launching public consultations relating to the creation of a foreign influence transparency registry;
- A review by NSICOP of the state of foreign interference in federal electoral processes;
- A review by NSIRA of how Canada's national security agencies handled foreign interference during the 43rd (2019) and 44th (2021) federal general elections;
- Establishing a national counter-foreign interference co-ordinator in Public Safety Canada;
- Issuing a Ministerial Directive requiring CSIS to "seek, wherever possible within the law and while protecting the security and integrity of national security and intelligence operations and investigations, to ensure that parliamentarians are informed of threats to the security of Canada directed at them.";
- Developing a plan to address outstanding recommendations from NSICOP, the Rosenberg Report and other reviews on foreign interference (outlined in an April 6, 2023 report by Dominic LeBlanc, Minister of Intergovernmental Affairs, Infrastructure and Communities, and Janice Charette, Clerk of the Privy Council and Secretary to the Cabinet, entitled *Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions*; and
- Investing $5.5 million in the Canadian Digital Media Research Network.

[58] Community Safety Knowledge Alliance, "Cyber Barn Raising," November 2022, https://cskacanada.ca/wp-content/uploads/2023/03/CSKA-CyberBarnRaising-FIN-digital.pdf.
[59] Public Safety Canada, "Enhancing Foreign Influence Transparency: Exploring Measures to Strengthen Canada's Approach," March 10, 2023, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nfluence/index-en.aspx.
[60] Ibid., "Consultation on a Foreign Influence Transparency Registry," n.d., https://www.canada.ca/en/services/defence/nationalsecurity/consultation-foreign-influence-transparency.html.

Effective Countermeasures

The public process should focus on strengthening Canada's capacity to detect, deter and counter foreign interference[61] and influence, dis-information and information warfare.

Effective countermeasures will require co-ordinated action between public and private sectors along a number of strategic trajectories: audience resiliency, message cleaning, programming, infrastructure mitigation and threat reduction measures, likely through persistent engagement.

We will need to build resiliency in vulnerable targeted audiences in their ability to recognize dis-, mis- and malinformation. This starts with security awareness education, critical thinking and promoting access to authoritative sources of information. Funding fact-checking, media literacy programs and increased transparency in social media advertising can help audiences make informed decisions. This initiative is similar to cyber-security, counter-radicalization and violent extremism programs led by the private sector.

Maligned messaging can be countered with content-based filters and suspending the accounts of maligned influencers on social media platforms. Programming would support global delivery of fact-based counter-narratives and involve pre-bunking and debunking toxic messaging online and in broader mediums. Counter-narratives are highly effective but should always be fact-based as part of an information peacekeeping strategy,[62] rapid response mechanism[63] or global peace and stabilization operations.

Disinformation campaigns rely on cyber-space to propagate and amplify their message. Cyber-space also offers an effective means to hide through obfuscation and non-attribution networks. Enumerating foreign global disinformation infrastructures requires effective open-source intelligence and targeting resources. The objective will be co-ordinated takedowns of malevolent infrastructures by government and industry. This has proved to be a far more effective strategy[64] than chasing billions of toxic messages consumed by a target audience or compromised machines. Industry has a wealth of experience and horsepower in established upstream cyber-security and intelligence programs that can be mobilized.

Threat-reduction measures require strong attribution that is substantiated with sophisticated intelligence. Effects can include sanctioning illicit companies and individuals, freezing assets, dismantling financial networks, disrupting the adversary's command and control, maintaining persistent engagement or following through with indictment and prosecution. Any countermeasure requires intelligence and strategic listening to assess the degrees of impact or threat-reduction measure, through to the detection and the resonance in the target audience and

[61] Government of Canada, "First Report … David Johnston."
[62] Robert Garigue, "Information Warfare: Developing a Conceptual Framework," Internet Archive, 1995, https://archive.org/details/INFORMATIONWARFAREByRobertGarigue1995.
[63] Global Affairs Canada, "Rapid Response Mechanism Canada," n.d., https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide.
[64] Government of Canada Publications, https://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf.

the overall efficacy of campaigns. This activity can provide necessary feedback to shape, steer and tune counter-disinformation campaigns.

It is important to recognize that, to protect Canadians, we must be prepared to defend forward and engage abroad. Global Affairs Canada, the Canadian Armed Forces, the Communications Security Establishment, CSIS, non-government organizations, civil society, industry and allied intelligence services all have roles to play.

Conclusion

Canada requires a sophisticated and objective approach to national security. Foreign interference can undermine the foundations of our democracy, not just particular political parties. Ideally, this issue should transcend partisanship and unite all political actors in a common cause to defend our democracy and the integrity of our elections.[65] Interference is not limited to politics. Deliberate interference in critical infrastructure is arguably even more dangerous.

Although foreign influence, disinformation, interference and cyber-attacks have received boosted air time in the past year, Canada still considers them to be separate issues and uniquely a public sector problem. David Johnston's independent special report on foreign interference relied solely on internal government testimony and documents for a subject where expertise, initiatives and intelligence principally exist in the private sector and open-information commons.

The private sector, including industry, security researchers, academics, investigative journalists and civil society, are leading some of the most evolved initiatives to counter foreign disinformation, influence and interference. For example, Google is expanding its misinformation pre-bunking efforts[66] and Microsoft is launching a coalition to combat media disinformation.[67]

Consider that disinformation is uniquely discovered through open-source intelligence and countered with open effects. Consequently, one can envision that the private sector will continue to play a central role with government in countering foreign disinformation, influence and interference.

[65] Government of Canada, "First Report … David Johnston."
[66] David Klepper, "Google to Expand Misinformation 'Pre-bunking'Initiative in Europe," Associated Press, February 13, 2023, https://www.pbs.org/newshour/politics/google-to-expand-misinformation-prebunking-initiative-in-europe.
[67] Gavin Phillips, "Microsoft Launches Coalition to Combat Media Disinformation," Make Use Of, February 23, 2021, https://www.makeuseof.com/microsoft-launches-coalition-to-combat-media-disinformation/.

About the Author

Dave McMahon is the chief intelligence officer of Sapper Labs Group, and former co-chair, interdepartmental committee on information warfare.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.