Building Democratic Resilience to Foreign Disinformation in Canada

Final Report | June 2024

Toronto Metropolitan University

the dais

DEMOCRACY XCHANGE

Acknowledgements

The Dais at Toronto Metropolitan University

The Dais is Canada's platform for bold policies and better leaders. We are a public policy and leadership think tank at Toronto Metropolitan University, connecting people to the ideas and power we need to build a more inclusive, innovative, prosperous Canada.

For more information, visit **dais.ca**
20 Dundas St. W, Suite 921, Toronto, ON M5G 2C2

@daisTMU
/daisTMU
The Dais at Toronto Metropolitan University

The Dais proudly engages a diverse group of funders to support and catalyze our work, consistent with our values, and subject to a thorough internal review. As a non-partisan, public-interest think tank, we only accept funds from organizations that support our mission and enable us to undertake work independently, with full editorial control. The names of all of our financial supporters are publicly and transparently displayed on all online and printed material for each project or initiative.

Design and Illustration: Zaynab Choudhry

Copy Editing: Suzanne Bowness

Contributors:
Tiffany Kwok, Policy Analyst, the Dais
André Côté, Director of Policy and Research, the Dais
Sam Andrey, Managing Director, the Dais
Nina Rafeek Dow, Communications and Marketing Lead, the Dais
Marium Hamid, Manager of Partnerships, the Dais
Angus Lockhart, Senior Policy Analyst, the Dais
Jake Hirsch-Allen, Senior Fellow, the Dais

DemocracyXChange

DemocracyXChange, this year in its fifth edition, is an annual summit to connect, celebrate and equip people who are taking action to strengthen democracy. Co-hosted by the Dais at TMU, OCAD University and the Open Democracy Project, DemocracyXChange aims to strengthen the community of practice that already exists across Canada and provide new opportunities to build democratic resilience over the course of three days of live talks, hands-on workshops and networking opportunities.

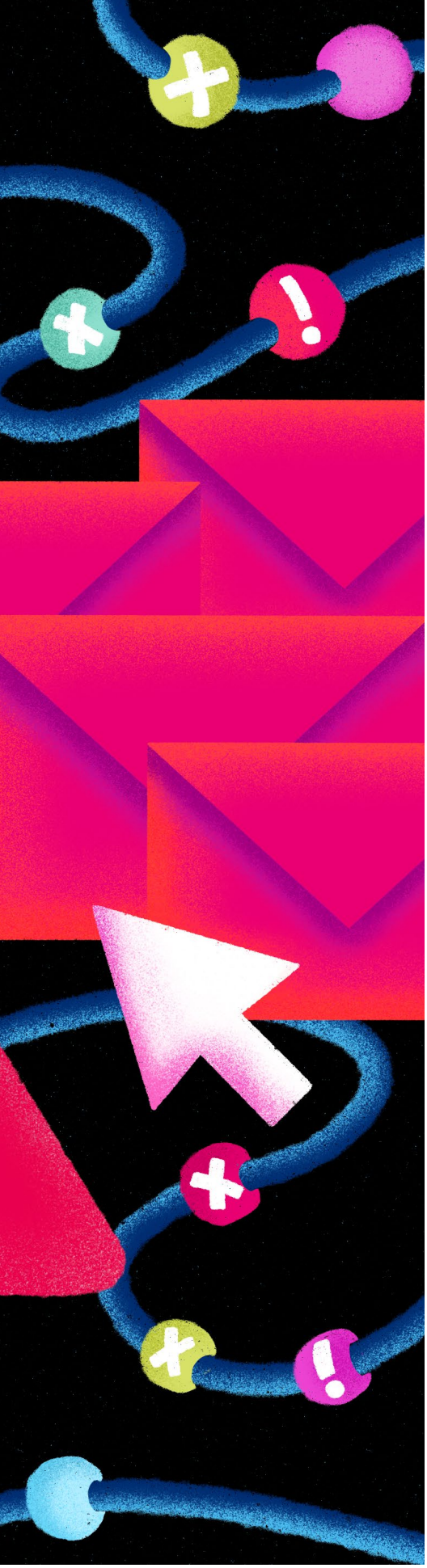
Funded by the Government of Canada | Canada

This work is supported in part by:
Government of Canada through the Privy Council Office's Democratic Institutions Secretariat

The opinions and interpretations in this report are those of the authors and do not necessarily reflect those of the Government of Canada.

How to Cite this Report

The Dais. *Building Democratic Resilience to Foreign Disinformation in Canada: Final Report*. Toronto Metropolitan University, 2024.
https://dais.ca



Workshop participants who consented to having their names included:

This report was greatly informed by the varied perspectives of our workshop participants. That said, the statements and recommendations in this report are solely the responsibility of its authors.

Aaron Shull, Centre for International Governance Innovation
Akaash Maharaj, Global Organization of Parliamentarians Against Corruption
Andrea Cecchetto, Markham Public Library
Anthony Seaboyer, Royal Military College of Canada
Bessma Momani, University of Waterloo
Chris Russill, Carleton University
Chris Tenove, University of British Columbia
Christina de Castell, Vancouver Public Library
Colette Brin, Université Laval
David Morin, Université de Sherbrooke
Diana Fu, University of Toronto
Dianna English, Centre for International Governance Innovation
Elizabeth Dubois, University of Ottawa
Emile Dirks, Citizen Lab
Emily Laidlaw, University of Calgary
Erin Taylor, Meta
Ghayda Hassan, UQÀM
Helen A. Hayes, McGill University
Isabelle Corriveau, McGill University
Jean-Christophe Boucher, University of Calgary
Jennie Phillips, McGill University
Kathryn Ann Hill, MediaSmarts
Laurie Mulvey, Penn State University, World in Conversation Center for Public Diplomacy
Lee Slinger, Munk School of Global Affairs & Public Policy
Marla Boltman, Friends of Canadian Media
Mohammed Hashim, Canadian Race Relations Foundation
Nicole Jackson, Simon Fraser University
Renee Black, GoodBot
Sabiha Tursun, McGill University, Uyghur Rights Advocacy Project
Samantha Reusch, Apathy is Boring
Sam Richards, Penn State University
Samantha Meyer, University of Waterloo
Seher Shafiq, Mozilla
Shelly Ghai Bajaj, University of Waterloo
Shlomit Broder, Digital Public Square
Steven Hassan, Freedom of Mind Resource Center
Viola Tian, Canadian Race Relations Foundation
Wendy Chun, Simon Fraser University
Wesley Wark, Centre for International Governance Innovation

Executive Summary

In March and April 2024, the Dais organized a two-part workshop with over 40 participants from academia, civil society, government, and industry. These workshops aimed to bring experts together to discuss the threat from foreign disinformation today. The workshop also considered opportunities to advance evidence-informed solutions for building democratic resilience in Canada.

From the beginning of the workshop, participants debated the ability to define and identify "foreign disinformation," emphasizing the need to differentiate between a spectrum of activities, tactics and threat actors. They also acknowledged the complex web of online interactions, often blurring the origins of false content. These challenges set the scene for the remainder of the discussions, where participants deliberated the issues and associated opportunities at each level.

The workshop discussions were organized into three sections: the first to address Canadians' experiences with foreign disinformation at the citizen level; the second to examine the ways in which civil society and businesses are involved in combatting foreign disinformation; and the third to discuss the decisions that governments and institutions must make when combatting foreign interference, along with opportunities they may have to enhance information-sharing and build public trust.

Participants collectively expressed the need for coordinated, multi-level approaches at the citizen, civil society and business, and government and institution level.

At the **citizen** level, opportunities identified included:

- Collecting more individual- and community-level data, to better understand experiences of foreign disinformation through online and offline media, including nuances in susceptibility to disinformation, and to take a closer look at all targeted vulnerable groups beyond just diaspora communities.
- Pre-bunking (building preemptive resilience), cultivating "good and accurate" information, and expanding evidence-based civic education initiatives as avenues to empower and build the digital literacy capacity of communities.
- Collaborating with trusted actors like doctors, scientists, and online influencers, in addition to framing digital-literacy education programming as opportunities to build on other skills to make citizen-level initiatives more approachable and well-received.

At the **civil society and business** level, opportunities identified included:

- Bolstering protection for academics, journalists, and civil society in the form of legal support and related costs, a support or ombudsperson function to support victims of harassment, and a renewed approach for law enforcement to take online threats more seriously.
- Learning lessons from civil-society efforts in jurisdictions further ahead in their development of resilience to foreign interference than Canada. These include efforts developed in countries such as Estonia, Finland, and Taiwan.
- Requiring additional transparency from online platforms to assess effectiveness of measures for platform governance that would address disinformation, such as fact-checking and labelling initiatives, or restrictions on automated content and paid advertising.

At the **government and institution** level, opportunities identified included:

- Reviewing the threshold for governments to share information with the public or affected communities regarding information attacks, in order to encourage more open sharing where possible.
- Introducing an annual threat assessment of foreign disinformation, to pre-bunk emerging issues, and keep governments and institutions informed of threats facing the country.
- Reviewing vulnerabilities that have been exploited by foreign disinformation campaigns abroad, in order to apply lessons in Canada.

Introduction

Project overview

Amidst the ongoing public inquiry into foreign interference with a targeted focus on the 2019 and 2021 federal elections, and ongoing disinformation in Canada's information ecosystem, we saw an opportunity to engage experts and stakeholders in a broad discussion about the nature of the threat from foreign disinformation today and opportunities to advance evidence-informed solutions for building democratic resilience in Canada.

In March and April 2024, a cross-section of government, industry, academic and civil-society experts and practitioners working at the intersection of disinformation and democracy were convened to participate in a two-part workshop:

- A 90-minute virtual pre-workshop on March 26, 2024 to offer initial issue presentations and discussion, and to introduce the key themes and approach for the in-person workshop to follow.
- A full-day in-person workshop on April 12, 2024 at the DemocracyXChange summit that engaged participants in an intensive, facilitated session that sought input on approaches to addressing foreign disinformation in Canada at the citizen, civil society, and government/institutional level.

Following the workshops, a summary of key themes, findings, and proposals from the discussions have been incorporated into this final report. The report explores opportunities to combat and address foreign disinformation at the citizen, civil society and business, and government and institution level.

Background: Foreign disinformation in Canada

Disinformation has long plagued the information ecosystem. In the rapidly evolving digital information ecosystem, its changing forms and increasingly elusive dissemination methods have amplified the difficulties of addressing or mitigating disinformation.[1] This challenge becomes more difficult with the geopolitical complexities from foreign disinformation campaigns, the aim of which is to erode public trust, and threaten the integrity of democratic institutions.

Foreign disinformation has only recently surfaced as a major issue in the public discourse about national security and democratic integrity. This is spurred by its prominent role in major global events like Russia's invasion of Crimea in 2014. In Canada, the 2019 federal election marked more public instances of Canada attempting to intervene and address foreign interference, including disinformation. Tools and teams, like the federal Security and Intelligence Threats to Elections (SITE) Task Force and the G7 Rapid Response Mechanism (RRM), were established, and the 2018 Elections Modernization Act included measures to guard against disinformation. These tools included digital ad transparency, as well as foreign influence through donations during an election period.[2] Civic education and media literacy efforts were also bolstered through programs like the Digital Citizen Initiative and community organization programs.[3] More recently, proposed amendments to the Canada Elections Act include expanding the ban on foreign influence during the election period to vote or refrain from voting for a particular candidate or party, to also include potential candidates and parties, and to apply at all

times beyond the election period. Prohibitions on impersonation and false statements to affect election processes or results were also clarified to include content created by artificial intelligence (AI).[4]

Canada's National Cyber Threat Assessment describes online foreign influence activities as a "new normal," with the deployment of disinformation as a growing and complex threat to Canada.[5] In some instances, malicious foreign actors seek to shift narratives or spur divides about global issues within democratic nations. Recent examples include disinformation campaigns concerning the COVID-19 pandemic and the 2022 Russian invasion of Ukraine.[6] Other efforts have sought to directly influence elections and democratic processes, such as recent revelations about the targeting of Canadian Members of Parliament (MPs) and prospective political nominees. Concerns have also grown around the targeting of diaspora communities, particularly through media avenues like native language programming and social platforms such as VKontakte (VK), Telegram, and WeChat.[7]

Given the framing and scope of this report on foreign disinformation, workshop participants stressed the challenge of defining what "foreign" constitutes, particularly in the context of disinformation narratives that flow from the United States to Canada. They also discussed how to differentiate between diplomatic engagement and foreign interference, in order to properly understand and define "foreign interference". The nature of "foreign disinformation" was also contested, recognizing the interconnected nature of the online information ecosystem, blurring the lines between foreign and domestic information. Discussions also focused on the differences in influence campaigns by different foreign-state actors, as some spread specific disinformation both broadly but also by targeting diaspora communities, while others operate by aiming to spread chaos through large scattershot operations or by amplifying existing polarization.

International landscape

From engaging with citizens to coordinating actions at the state level, other jurisdictions have taken various approaches to addressing foreign disinformation. Until recently, the United States (US) took a comprehensive approach by engaging directly with and informing social media platforms, and countering disinformation through a variety of agencies, including the Global Engagement Center, the Federal Bureau of Investigation, and the Cybersecurity and Infrastructure Security Agency.[8] Amid recent legal challenges to this approach, social media platform briefings are currently on pause.[9] A new US-led Framework to Counter Foreign State Information Manipulation was also jointly endorsed by the United Kingdom (UK) and Canada in February 2024, which focuses in part on going beyond "monitor-and-report" approaches to ones that include strategies to counter threats.[10]

The European Union (EU) has also taken a mixed approach by creating a framework to counter foreign information manipulation and interference (FIMI), establishing a Code of Practice on Disinformation, and deploying a Rapid Alert System (RAS) to share analyses, best practices, and communication materials with EU institutions, member states, and international partners.[11] The EUvsDisinfo website engages visitors at the citizen level by debunking disinformation cases, while EU member states have also taken their own approaches to combatting disinformation.[12] France, for example, passed a law in 2018 aiming to empower judges to remove "fake news" during election campaigns.[13] The UK's approach includes its Online Media Literacy Strategy that seeks to raise media-literacy rates among teachers, carers, librarians, and youth workers,[14] and its National Security Online Information Team (NSOIT) targets foreign disinformation.

KEY THEME 1

Citizen level

This section focuses on Canadians' experiences with foreign disinformation, and offers potential opportunities to combat and build resilience against disinformation at the level of the citizen.

THE ISSUE:

Canadians are being targeted by foreign disinformation campaigns.

SUMMARY OF POTENTIAL OPPORTUNITIES:

- **Collect more data to better understand the experiences of foreign interference within vulnerable communities, such as diaspora communities.**
- **Better understand outcomes of community organizations combatting disinformation, with the goal to improve future program iterations, including in translation to languages beyond English and French.**
- **Educate Canadians of all ages about foreign disinformation to equip individuals with the tools and ability to think critically and identify disinformation, including through culturally-relevant public education and digital-literacy programs and initiatives.**

Diaspora communities in Canada have long been the targets of foreign interference campaigns by nation-state actors. Disinformation, the popularized use of online platforms, and historical distrust of authorities have become avenues for interference by foreign actors to create campaigns targeting specific vulnerable communities. The heavy reliance and higher levels of trust that some diaspora communities have on content circulating within private communication channels, like WeChat and WhatsApp, pose particular challenges to identifying and combatting such disinformation.[15]

The development of culturally-relevant measures to reach targeted communities requires a deeper understanding of different communities' experiences with foreign interference. Efforts to address disinformation must take into account the needs and experiences of these communities or they may face potentially negative consequences.

As in the cases of disinformation and information manipulation campaigns targeting MP Michael Chong and former MP Kenny Chiu, malicious foreign actors seek to discourage targeted MPs from political participation, to pollute public discourse, and to ultimately undermine democratic participation.[16] Without culturally- and linguistically-relevant information sources, diaspora community members risk difficulties in forming accurate and authentic political opinions. This risks that they will accept false information as truth, deterring citizens from participating in elections and other democratic processes.

Foreign disinformation efforts have also sought to influence democratic discourse and public opinion in Canada amongst the broad citizenry. One example of these efforts relates to Russia's lengthy disinformation campaign, from influencing discourse around vaccine hesitancy and anti-lockdown narratives during the COVID-19 pandemic, to disinformation around Russia's invasion of Ukraine.[17]

Three potential opportunities to address the threat of foreign disinformation at the citizen level are identified.

Collect more data to understand communities' experiences with foreign interference.

First, conduct research and seek out local engagement to better understand communities that experience foreign interference, plus explore the underlying factors that contribute to the spread of false and misleading information. While existing research highlights increased potential susceptibility due to factors like historical and contemporary traumas, as well as identity-based appeals, more data needs to be collected to understand the nuances in this susceptibility, and to inform any future approaches to combat disinformation.

Beyond diaspora communities, workshop participants raised the need to explore other targeted vulnerable groups — namely those who may have traditionally lower trust in institutions. Participants brought up the Freedom Convoy and COVID-19 conspiracy communities in Canada as examples of such groups. Participants also pointed to the importance of developing a better understanding the role of content creators and social media influencers in spreading mis- and disinformation. Research shows that influence and engagement is unequal, with the top 10 percent of social media accounts generating approximately 93 percent of engagement on major platforms.[18] Results also reveal that doctors and scientists are the most trusted information providers, warranting greater investigation into how to leverage these trustworthy figures.

Participants also discussed the relative availability of aggregate data, as opposed to individual-level data, highlighting the need to better understand individuals' interactions with social media and disinformation. While aggregate data may be able to provide broad, high-level insights into different community groups' experiences on social media, individual-level data can highlight linguistic, cultural, and habitual nuances within communities that may not otherwise be captured in group-level data. Collecting and using both individual and aggregate data would provide the insights to create multi-levelled solutions to combatting disinformation. Participants also discussed how Canada's proposed Online Harms Act creates new regulatory obligations for online platforms to provide transparent information and access to data for research, but that the scope is limited to the narrow categories of illegal content, rather than disinformation.

Participants also suggested looking at local news sources that connect diaspora communities to their countries of origin as a way to gain a better understanding of international discourse on issues, although some voiced the need to distinguish between malicious interference and simple social engagement between people. Participants also recommended looking beyond traditionally researched social media platforms, to online tools such as private messaging platforms, gaming platforms, and podcasts.

Track and analyze outcomes of community organizations' work to combat disinformation.

Second, seek to better understand the outcomes of community organizations' work to combat disinformation. This can be done through program and/or community evaluations of those who receive funding through the Digital Citizen Contribution Program, or the Digital Literacy Exchange Program. As part of these funding opportunities, organizations have developed a variety of learning materials, public awareness programs and tools, and civic literacy campaigns. Assessing users of these products for their improved understanding and digital know-how can be one way to identify whether these programs and tools have been effective, and to identify remaining gaps.

One workshop participant shared the need to collect success stories coming from existing programs to understand why they worked, in order to implement these elements into future initiatives. Others noted the challenge of building long-term impact-tracking into what are often one-year grants. Others expressed the need to protect community members' privacy as an utmost priority when analyzing all tracking and outcomes. This was mentioned

specifically with respect to organizations working in communities that held lower levels of trust in governments, as they may feel uncomfortable with sharing their insights and data, even if the results aid improvements in programming.

Efforts can also be made to identify cultural community organizations that may not have received funding, but who are doing work to combat disinformation in their communities. Collecting outcomes-based data can also contribute to improving future iterations of disinformation interventions and digital-literacy programming to targeted populations. While research has shown that improving digital literacy can support users' discernment of accurate information from false, it remains unclear how long this impact lasts, and whether it prevents users from sharing false information online.[19] As a result, greater attention should also be paid to users' abilities and their online interactions over time.

Educate and equip Canadians with the tools and abilities to think critically and identify disinformation.

Third, applying the insights from the efforts above, expand communications with Canadians of all ages on the topic of foreign disinformation, equipping individuals with the tools and education to think critically and identify disinformation. Culturally-relevant and relatable public education, plus digital literacy in languages beyond English and French may be particularly important to reaching vulnerable communities. Supporting grassroots initiatives like community websites Factchequeado and Auntie Betty, as well as local organizations, will expand the reach of digital-literacy education to people outside of the formal education system.[20] Any initiatives and materials should be co-created with diaspora community members to achieve full impact and to build trust in democratic institutions. Participants also suggested the need to market digital-literacy programming initiatives to citizens as opportunities to build on other skills, to avoid scams, and to engage trusted actors like influencers and celebrities to build citizen resilience at a larger scale.

Workshop participants emphasized the need to empower and build capacity within communities rather than purely relying on regulation, offering the option to pre-bunk and inoculate against mis- and disinformation to build up digitally-literate citizens. Discussions also mentioned the ultimate need for expanded civic education, and a greater focus in cultivating "good and accurate" information, rather than just combatting false information, to rebuild trust in institutions.

In contrast, some participants voiced their skepticism around the effectiveness of education and expanded communications as a sole approach, pointing to the tactics of cognitive overload that are foreign-state actors use on social media. Participants explained that the crowding out of the information space leads to information apathy and paralysis, and alluded the ways in which "dark" and catchy news and content can overpower educational efforts. Others pointed to the roots of cognitive overload through the concepts of fourth- and fifth-generation psychological warfare, aiming to create distrust in experts, scientists, and institutions.

KEY THEME 2

Civil society and business level

This section examines the ways in which civil society and businesses—including social media platforms—are involved in combatting disinformation, and offers potential opportunities to bolster and coordinate the civil society and industry-led efforts.

THE ISSUE:

Various efforts across organizations and platforms, such as media, libraries, schools, newcomer settlement agencies, cultural community groups and online platforms, are struggling to keep ahead of threats to individuals and communities exposed to disinformation.

SUMMARY OF POTENTIAL OPPORTUNITIES:

- **Increase protections for journalists, civil society members, and researchers from harassment and threats related to their work combatting disinformation.**
- **Enhance tools for community leaders and organizations to increase resilience and debunk foreign disinformation within their communities.**
- **Combat the spread of foreign disinformation on online platforms through fact-checking initiatives, restrictions on tools such as bots, coordinated inauthentic behaviour and AI-generated content, and enforcing policies against disinformation through paid advertisements.**

From journalists and librarians to teachers to researchers, members of civil society are increasingly engaged with and affected by foreign disinformation. Yet, due to the fast-changing nature of disinformation, and the evolving use of AI to generate and spread that disinformation, coordinated attempts to stifle its spread and protect the information ecosystem have often fallen short. While preventing the creation of false information and pre-emptively stopping its spread have proven to be challenging, there are measures that can be continually taken to protect and equip civil-society members and businesses with the tools and abilities to stay ahead of threats to individuals and communities that are exposed to disinformation.

The ability to find truth in a polluted information ecosystem, to report on recent events with accuracy, and to maintain high cognizance with framing in news reports has become increasingly challenging for journalists. Journalists, researchers, and civil society members involved in topics like disinformation and social cleavages have also become personal targets of harassment and online intimidation in Canada and abroad.[21]

Online platforms have also, to a varying degree, deployed measures to address disinformation. For example, many platforms have policies and measures to mitigate "coordinated inauthentic behaviour" that is often deployed by foreign disinformation campaigns to artificially amplify false narratives, with mixed measures of success.[22] Some platforms have also partnered with governments, agencies, and fact-checking efforts to address the accuracy of information disseminated online, in the case of elections, or public-health emergencies.

We identify three opportunities to bolster the work of civil-society organizations and businesses.

Increase protections and resources for journalists, members of civil society, and researchers from harassment and threats related to their work combatting disinformation.

First, increase protections from online harassment, threats, and hacks against individuals like journalists, researchers, and members of civil society. Canada's proposed Online Harms Act may provide clearer pathways to report cases and receive support in cases of targeted hate, incitement of violence, and intimate image abuse, as well as assign new responsibilities on platforms to minimize the risks of exposure to this content.[23] Canada has also made recent investments in enhancing the cybersecurity of research institutions to mitigate the risk of foreign threats.[24] Workshop participants pointed to the role of politicians in their spread of disinformation, noting a need for greater protection for civil society to call leaders out. Participants referenced British Columbia's Election Amendment Act and its laws against disinformation about the electoral process, expressing curiosity as to how the law's enforcement by the election administrator will play out.

Participants made a number of suggestions to better protect academics, journalists and civil society engaging in disinformation research, including offering support with legal defenses and related costs, creating a support person or ombudsperson function to support victims, and for law enforcement to take online threats more seriously.

Workshop discussions also raised the need for more funding for non-profit and academic efforts aimed at bolstering citizens' digital resilience against disinformation. Participants noted, however, that if funds come only from government for digital-literacy initiatives, the perception risk of bias may be increased for some communities. Participants expressed the need to diversify the philanthropic, academic, and other funding sources for this work as well.

Enhance tools for community leaders and organizations to increase resilience and debunk foreign disinformation within their communities.

Second, participants advocated the need to introduce new tools, co-developed based on the needs of community leaders and organizations to increase community resilience and debunk foreign information manipulation and interference. These tools should take into account the role of AI in creating and spreading disinformation, teaching digital literacy that includes skills to distinguish AI-generated content (e.g., deepfakes). Existing tools like curriculum and critical-thinking toolkits should also be updated to meet citizens' changing needs as a result of evolving technology. Tools created to target vulnerable communities, such as diaspora communities, should ideally be co-designed, and incorporate any cultural and linguistic needs. Xīn Shēng Project (formerly the WeChat Project)'s podcasts on misinformation in both English and Simplified Chinese are an example of a resource created with cultural and linguistic needs in mind.[25] The Council of Agencies Serving South Asians (CASSA)'s toolkit to combat online hate is another example of a resource built with and for racialized communities and involved agencies combatting online hate.[26] Collaborating with individuals already working to fight foreign interference in vulnerable communities and learning from their best practices can also serve as a foundation to future resource development.

Workshop participants also pointed to Taiwan, Finland, and Estonia as examples of countries that had seen success in deploying citizen awareness activities through civil society, across various age groups. Regarding Taiwan, participants noted the country's approach to cultivating healthy information spaces via civil-society organizations, while keeping governments at an arm's length to build public trust. Finland was noted to have implemented critical-thinking training beginning in kindergarten, as well as running a prime-time show to pre-bunk public knowledge, and nation-wide courses on AI and digital literacy. Estonia has a similar model of teaching media literacy to students by integrating content into other existing subjects.

Participants also mentioned the need to leverage issues and concerns that the broader citizen population cares about, in the design and promotion of any programs and initiatives. They noted the benefit to recognizing the role of close family, friends, employers, and businesses in holding individuals accountable with information dissemination, and providing training and awareness.

Examples of tools that could be brought to the Canadian context included dashboards and websites that track disinformation in real time, similar to the EUvsDisinformation website, and others that track the official news narrative for a certain issue or event, similar to the Hamilton 2.0 Dashboard website in the US. These tools were proposed as potentially helpful information references for civil-society members and journalists.

Participants also raised the need to go beyond building resilience in online spaces, but also looking at "offline" spaces by examining how people are engaging in physical, social spaces. They also discussed the role of mental health, as well as the void that online communities fill in the absence of offline options. The role of libraries and possible interventions they could organize were also raised as a vital element in a civil-society response. Examples include libraries' offerings of tools such as digital-proficiency courses, subscriptions to platforms with online learning tools like LinkedIn Learning, and strategic leveraging of the public's interest in navigating frauds and scams to digitally empower and equip users.

Combat the spread of foreign disinformation on online platforms through a combination of approaches.

Third, encourage online platforms to expand their efforts to protect users and reduce the spread of foreign disinformation. Some social media platforms have introduced proactive measures such as restrictions on bots and coordinated inauthentic behaviour (CIB), policies against disinformation through paid advertisements, and active deployment of fact checkers and nudges to verify information. However, some platforms are more active in their crackdown on disinformation than others. For example, while Meta has been relatively diligent in identifying and taking down coordinated inauthentic accounts, these same accounts still exist on X.[27] Meta also recently announced its plan to label AI-generated content, putting both visible markers and invisible watermarks to identify select content.[28] However, there are limitations to these efforts, as content will only be labelled if it has pre-existing watermarks and metadata identifying its AI-generated origins.[29] Online advertising is another area that online platforms can take greater control of, recognizing that 92 percent of Canadian internet advertising is attributed to foreign internet sites and platforms.[30]

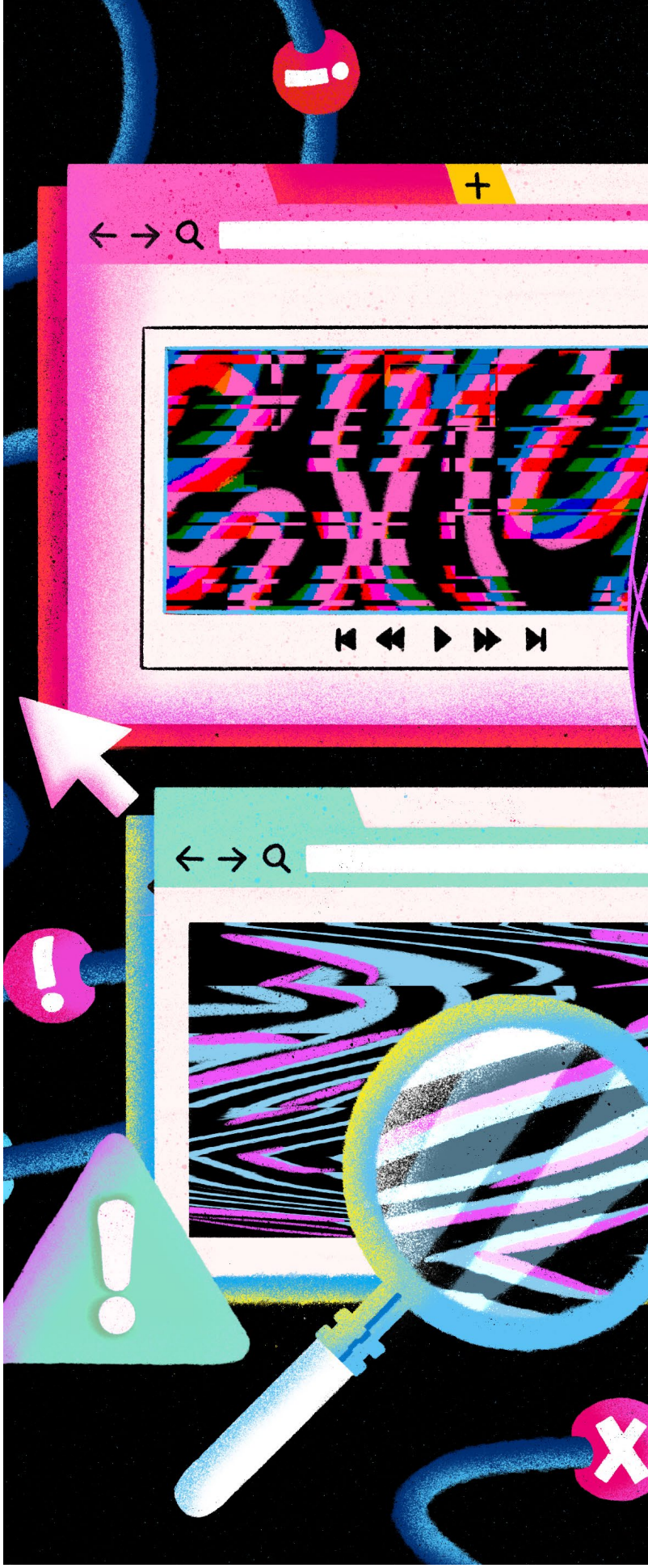
Similar to the EU's AI Act,[31] proposed amendments to Canada's Artificial Intelligence and Data Act in Bill C-27 include requirements for generative AI platforms to enable detection of AI-generated audio-visual content.[32] Experts expect that platforms will need to update their policies around synthetic media leading up to the next election period.[33]

Although workshop participants agreed on the need for platform governance, they recognized the nuances in citizen perceptions, depending on who is identifying the mis- and disinformation (whether community-driven, platform, or state actor). Participants pointed to Wikipedia and X's Community Notes as good examples of crowdsourcing verified information. Participants also noted Mozilla's platform accountability campaign at the beginning of April 2024 as an example of an effort to pressure platforms like WhatsApp into more responsible

action without regulation. Through Mozilla's letter to WhatsApp, calling on the platform to add friction to forwarding messages, disinformation warning labels to viral content, and reduce the platform's broadcast capabilities during the global election period in 2024, the public is able to participate in the campaign by signing on.[34]

Participants raised the need for additional transparency from platforms with respect to information integrity, and the need for access to data on what past platform-governance measures have been effective, to inform future measures. Discussions also mentioned the proposed Online Harms Act and the role of the ombudsman albeit narrowly covering selective harms, and suggested introducing minimum requirements for platforms' resourcing of their "trust and safety" teams and activities, whether that be for content moderation or frequent review of the platform's policies.

Discussions touched on limitations of platform-governance measures, citing the absence of such measures on private messaging platforms like WeChat. Participants also brought up the need to seek international cooperation on platform governance, noting the multinational nature of their operations and governance. Participants also raised skepticism with platforms to have any incentives to enforce harsher governance measures unless penalties compel them.



KEY THEME 3

Government and institution level

This section discusses the decisions that governments must make when combatting foreign interference, along with opportunities to enhance information-sharing and build public trust.

THE ISSUE:

Government balancing the disclosure of foreign interference threats with the need to respect citizens' right to privacy and maintain classified intelligence sources, which can impede efforts to counter threats.

SUMMARY OF POTENTIAL OPPORTUNITIES:

- **Review the threshold for governments to share information with the public or impacted communities regarding information attacks to encourage more open sharing where possible.**
- **Forecast for and create action plans to proactively respond to potential negative side-effects associated with disclosures of foreign interference.**
- **Review vulnerabilities that have been exploited by foreign disinformation campaigns abroad to apply lessons in Canada.**

Democratic institutions grapple with the challenges of maintaining transparency with citizens by disclosing known foreign interference threats, while still protecting the public from risks of privacy infringement, for example, by focusing analysis only on open-source materials, and maintaining classified intelligence sources gathering threats from abroad. This is done with acknowledgment of the difficulties around drawing clear lines between foreign and domestic disinformation, given the nature of the information ecosystem. The reach of foreign information influence also extends beyond verifiable disinformation through, for example, information pollution and amplification of subjective disagreements that have far-reaching impacts on individual perceptions and trust of the information environment. The Government of Canada has made recent moves to increase transparency, including consultations on a Foreign Influence Transparency Registry, as well as amendments to the Canadian Security Intelligence Service Act to enable greater disclosure of information to those outside the Government of Canada.[35]

Canada's Rapid Response Mechanism (RRM) has shared cases of detected information operations including the probable "spamouflage" campaign in 2023, in which bot networks targeted MPs across Canada on Facebook and X.[36] Scholars have looked at Russia's role in the Freedom Convoy, while other scholars have shared their own experiences of foreign disinformation while attempting to conduct a political campaign.[37] Regardless of the forum in which intelligence and reports of disinformation have been shared, information-sharing remains an important act of transparency to enable counter-measures such as inoculation warnings and to build public trust between the government and Canadians.

We identify three key opportunities for democratic institutions to respond to the threats of foreign disinformation.

Review the threshold for governments to share information with the public or impacted communities regarding information attacks, to the extent possible.

Governments can review the threshold to share information with the public regarding information attacks, to encourage more open sharing to the extent possible, particularly when filling information vacuums. Workshop participants noted the need for more context to be provided when intelligence is shared, in efforts to better inform citizens who would likely be unfamiliar with an issue's global or historical context. The importance of the format in which intelligence is communicated was also raised in discussions, due to the need to both build and leverage citizen trust in reliable sources. VIGINUM, a government agency dedicated to publishing official content with the aim of detecting and characterizing foreign digital interference in France, was raised as a relevant example.[38] However, some participants contested whether governments would even want to be more transparent and noted there would be difficulty in setting these thresholds in a non-partisan manner, particularly with respect to disinformation on sensitive political topics.

Through RRM reports, the Critical Election Incident Public Protocol, and other intelligence on foreign mis- and disinformation, governments should continually revisit their methodologies and thresholds both for ethical monitoring and reporting. Acknowledging both the benefits and consequences of encrypted messaging, workshop participants stated the need to maintain strong encryption and to seek alternate means to collect intelligence, such as metadata, open-source information, transparency reports from private platforms, and direct engagement and surveying.

Forecast for and create action plans to proactively respond to potential negative side-effects associated with disclosures of foreign interference.

Beyond monitoring and reporting, governments can also forecast for and create proactive action plans in the case of potential negative side-effects associated with disclosures of foreign disinformation. Participants raised the need for government interventions to be mindful, ensuring that any interventions do not become an act of interference for democratic processes like elections. This was mentioned particularly in relation to the challenges that security and intelligence agencies can encounter through the ways in which intelligence is collected, to ensure these methods do not directly or indirectly impact election outcomes.

Workshop participants also suggested that both an annual threat assessment of foreign disinformation and regular information ecosystem updates be introduced, similar to or as part of the National Cyber Threat Assessment. This would be a proactive effort on the government's part to pre-bunk emerging issues, reduce chances of issues being sensationalized, and keep governments and institutions at all levels informed of threats facing the country in greater detail than is currently available.

Review vulnerabilities that have been exploited by foreign disinformation campaigns abroad to apply lessons in Canada.

Foreign disinformation campaigns also exploit increased polarization and deepening of existing social cleavages to target and exploit divisions in Canada. Governments and public institutions should also take the opportunity to review existing vulnerabilities, rather than only focus on known threats. Similar to the examination of the Freedom Movement by the Public Order Emergency Commission, other social cleavages can be likewise analyzed to inform future preparatory measures.[39] An extended, cross-departmental review of the possible threats from violent extremism driven by politics, religion and ideology noted in the Security and

Intelligence Threats to Elections (SITE) Task Force's June 2023 report may be a good starting point.[40]

International examples of exploited divisions include Russian campaigns to sow discord among racial and religious groups, leveraging the Black Lives Matter movement, and religious tensions following former US President Trump's inflammatory statements.[41] Participants also mentioned the MAGA movement in the United States, pointing out its organic nature in organizing, not driven solely by disinformation campaigns. Other participants noted Chinese campaigns targeting Hong Kong democracy protestors, and Indian campaigns targeting farmer protests, in efforts to discredit individuals and their movements.[42]

One participant was able to reflect upon their personal experience interacting with protestors at the Freedom Convoy, in hopes of understanding their perspectives and engaging in conversation. Other participants pointed to engaging with newcomers as soon as they arrive in Canada, equipping individuals to think critically, provide accurate information about Canadian institutions and media, and to address any potential distrust of the Canadian government.

By proactively analyzing tensions both online and offline, transparently working with and genuinely dialoguing with community groups, and resourcing and responding to community needs, institutions have the chance to build public trust and increase resilience to future threats.

References

[1] Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2023-2024," https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024; Canada's National Cyber Threat Assessment 2023-2024 uses the term MDM - misinformation, disinformation, and malinformation. Misinformation is false information not intended to cause harm; disinformation is false information intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction; malinformation is information that is exaggerated in a way that misleads and causes potential harm.

[2] Government of Canada, "Security and Intelligence Threats to Elections Task Force," June 2023, https://www.canada.ca/en/democratic-institutions/services/reports/security-intelligence-threats-elections-task-force-threats-canadian-federal-by-elections-june-2023.html; Global Affairs Canada, "Rapid Response Mechanism Canada: Global Affairs Canada," https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng; Elections Modernization Act, Statutes of Canada 2018, c.31. https://laws-lois.justice.gc.ca/eng/annualstatutes/2018_31/page-1.html.

[3] Government of Canada. "Digital Citizen Initiative - Online disinformation and other online harms and threats," https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html.

[4] Government of Canada: Democratic Institutions, "Proposed amendments to the Canada Elections Act." https://www.canada.ca/en/democratic-institutions/news/2024/03/proposed-amendments-to-the-canada-elections-act.html.

[5] Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2023-2024," https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.

[6] Yasmin Dawood, "Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats," Election Law Journal: Rules, Politics, and Policy 20 , no. 1 (March 17, 2021): 10-31. http://doi.org/10.1089/elj.2020.0652; Media Ecosystem Observatory, "Mis- and Disinformation During the 2021 Canadian Federal Election," March 2022, https://www.mcgill.ca/maxbellschool/files/maxbellschool/meo_election_2021_report.pdf; 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," Conflict Report Series, Centre for Artificial Intelligence, Data, and Conflict, March 2023, https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf?index=true.

[7] Dave McMahon, "Maligned Influence and Interference in Canada," Canadian Global Affairs Institute, July 2023, https://www.cgai.ca/maligned_influence_and_interference_in_canada/.

[8] Cybersecurity & Infrastructure Security Agency, "Foreign Influence Operations and Disinformation," https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation.

[9] Naomi Nix and Cat Zakrzewski, "U.S. Stops Helping Big Tech Spot Foreign Meddling Amid GOP Legal Threats," The Washington Post, November 30, 2023, https://www.washingtonpost.com/technology/2023/11/30/biden-foreign-disinformation-social-media-election-interference/.

[10] US Department of State, "The Framework to Counter Foreign State Information Manipulation" (Fact Sheet), January 18, 2024, https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/; Government of Canada, "Joint Statement by Canada, United States and United Kingdom on Foreign Information Manipulation," February 16, 2024, https://www.canada.ca/en/global-affairs/news/2024/02/joint-statement-by-canada-united-states-and-united-kingdom-on-foreign-information-manipulation.html.

[11] European Union External Action, "Tackling Disinformation, Foreign Information Manipulation & Interference," October 27, 2021, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en; European Commission, "The 2022 Code of Practice on Disinformation," July 4, 2022, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[12] EuvsDisinfo, https://euvsdisinfo.eu/, accessed May 27, 2024.

[13] République Française, "LOI no. 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (1)," https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/.

[14] Department for Digital, Culture, Media & Sport, and Caroline Dinenage MP, "Minister Launches New Strategy to Fight Online Disinformation," GOV.UK, July 14, 2021, https://www.gov.uk/government/news/minister-launches-new-strategy-to-fight-online-disinformation.

[15] Wesley Wark, "Foreign Interference Online: Where Disinformation Infringes on Freedom of Thought," Policy Brief No. 3, Centre for International Governance Innovation, January 22, 2024, https://www.cigionline.org/publications/foreign-interference-online-where-disinformation-infringes-on-freedom-of-thought/; Inga Trauthig, "Diaspora Communities and Computational Propaganda on Messaging Apps," Policy Brief No. 183, Centre for International Governance Innovation, January 2024, https://www.cigionline.org/static/documents/PB_no.183.pdf.

[16] Parliament of Canada, "Foreign Interference and the Threats to Integrity of Democratic Institutions, Intellectual Property and the Canadian State: Report of the Standing Committee on Access to Information, Privacy and Ethics," October 2023, https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-10.; Government of Canada, "WeChat Account Activity Targeting Canadian Parliamentarian Suggests Likely Foreign State Involvement," https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/wechat.aspx?lang=eng.

[17] Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2023-2024," https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024; 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," Conflict Report Series, Centre for Artificial Intelligence, Data, and Conflict, March 2023, https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf?index=true.

[18] Aengus Bridgman, Alexei Abrahams, Thomas Bergeron, Thomas Galipeau, Blake Lee-Whiting, Haaya Naushan, Jennie Phillips, Zeynep Pehlivan, Saewon Park, Sara Parker, Benjamin Steel, Peter Loewen and Taylor Owen, "The Canadian Information Ecosystem," Media Ecosystem Observatory (Canadian Digital Media Research Network), 2023, https://osf.io/b29q8/download/?format=pdf.

[19] Nathaniel Sirlin, Ziv Epstein, Antonio A. Arechar, and David G. Rand. "Digital Literacy is Associated with More Discerning Accuracy Judgments but not Sharing Intentions," Harvard Kennedy School (HKS) Misinformation Review, December 2021, https://misinforeview.hks.harvard.edu/article/digital-literacy-is-associated-with-more-discerning-accuracy-judgments-but-not-sharing-intentions/.

[20] Factchequeado. https://factchequeado.com/english/.; Auntie Betty. https://auntiebetty.ca/.

[21] Brodie Fenlon, "Our Journalists are Facing More Harassment, Threats for Doing Their Jobs," CBC News, February 8, 2022, https://www.cbc.ca/news/editorsblog/editor-note-pandemic-protests-media-experience-1.6343672; Cristina Caicedo Smit, "Data on Online Hate Directed at BBC Journalists Mirrors Global Trend," VOA News, August 10, 2023, https://www.voanews.com/a/data-on-online-hate-directed-at-bbc-journalists-mirrors-global-trend/7220041.html.

[22] Monica Murero, "Coordinated Inauthentic Behavior: An Innovative Manipulation Tactic to Amplify COVID-19 Anti-vaccine Communication Outreach *via* Social Media," *Frontiers in Sociology* 8 (March 16, 2023), doi:10.3389/fsoc.2023.1141416; Kasey Stricklin, "Social Media Bots: Laws, Regulations, and Platform Policies," Center for Naval Analyses, September 2020, https://apps.dtic.mil/sti/trecms/pdf/AD1112566.pdf.

[23] Parliament of Canada. "Bill C-63". https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading.

[24] Government of Canada, "New Investment Seeks to Build Canada's Research Security Capacity," (Press release), November 14, 2022, https://www.rsf-fsr.gc.ca/news_room-salle_de_presse/latest_news-nouvelles_recentes/2022/new_investment_research_security_capacity-nouvel_investissement_securite_recherche_canada-eng.aspx.

[25] Xīn Shēng Project. "Podcast." https://www.xinshengproject.org/archive.

[26] Council of Agencies Serving South Asians (CASSA), "#EradicateHate: A Collaborative to Combat Online Hate," https://www.cassa.ca/eradicatehate/.

[27] Joseph Menn, Aaron Schaffer, Naomi Nix, and Clara Ence Morse, "Chinese Propaganda Accounts Found By Meta Still Flourish on X," The Washington Post, February 16, 2024, https://www.washingtonpost.com/technology/2024/02/16/x-meta-china-disinformation/; Nicolas Hénin and Maria Giovanna Sessa, "Disinformation on X: Research and Content Moderation Policies," EU DisinfoLab, January 2024, https://www.disinfo.eu/wp-content/uploads/2024/01/20240116_Twitter-X_factsheet.pdf.

[28] Nick Clegg, "Labeling AI-Generated Images on Facebook, Instagram and Threads," Meta, February 6, 2024, https://about.fb.com/news/2024/02/labeling-ai-generated-images-on-facebook-instagram-and-threads/.

[29] Kate Irwin, "Meta will Label AI-Generated Content, But There's a Catch," PC Mag, February 6, 2024, https://www.pcmag.com/news/meta-will-label-ai-generated-content-but-theres-a-catch.

[30] Peter Miller and David Keeble, "Close the Loophole! The Deductibility of Foreign Internet Advertising," Friends of Canadian Media, March 6, 2024, https://friends.ca/wp-content/uploads/2024/03/Close-the-Loophole-2024-update-March-6-FINAL-1.pdf.

[31] European Commission, "AI Act," (last updated May 6, 2024), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=The%20AI%20Act%20is%20the,play%20a%20leading%20role%20globally.&text=The%20AI%20Act%20aims%20to,regarding%20specific%20uses%20of%20AI.

[32] Innovation, Science and Economic Development Canada, "Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems," September 2023, https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems; Parliament of Canada, Bill C-27, https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

[33] Michelle Bartleman and Elizabeth Dubois, "The Political Uses of AI in Canada," Pol Comm Tech Lab, University of Ottawa, 2024, https://www.polcommtech.com/_files/ugd/eeebb0_6d49ce7a5cbe4f249bf5ee051ffce03d.pdf.

[34] Mozilla, "WhatsApp: Reform Features *Now* to Protect Election Integrity," Mozilla, April 2, 2024, https://foundation.mozilla.org/en/blog/whatsapp-reform-features-now-to-protect-election-integrity/.

[35] Canadian Security Intelligence Service, "Government of Canada's Launch of a Public Consultation on Legislative Amendments to Counter Foreign Interference," November 24, 2023, https://www.canada.ca/en/security-intelligence-service/corporate/government-of-canadas-launch-of-a-public-consultation-on-legislative-amendments-to-counter-foreign-interference.html; Public Safety Canada, "What We Heard Report: Consulting Canadians on the Merits of a Foreign Influence Transparency Registry," November 2023, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nflnc-wwh/index-en.aspx.

[36] Government of Canada, "Probable PRC 'Spamouflage' Campaign Targets Dozens of Canadian Members of Parliament in Disinformation Campaign," October 23, 2023, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2023-spamouflage.aspx?lang=eng.

[37] Caroline Orr Bueno, "Russia's Role in the Far-Right Truck Convoy: An Analysis of Russian State Media Activity Related to the 2022 Freedom Convoy," The Journal of Intelligence, Conflict, and Warfare 5, No. 3 (January 31, 2023), https://journals.lib.sfu.ca/index.php/jicw/article/view/5101; Kaveh Shahrooz, [@kshahrooz], "In light of insufficient time to conduct a campaign and due to unprecedented foreign interference which regrettably went unaddressed, I am hereby withdrawing from the Conservative Party of Canada nomination election in the riding of Richmond Hill. My full statement," X, February 22, 2024, https://twitter.com/kshahrooz/status/1760621192182923506?s=46&t=izoswVl4edVit4U2W3N56Q.

[38] Secrétariat général de la défense et de la sécurité nationale, "Service de vigilance et protection contre les ingérences numériques étrangères," November 17, 2022, https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques.

[39] Frank Graves, "Commissioned Paper: Social Cleavages Series Understanding the Freedom Movement: Causes, Consequences, and Potential Responses," Public Order Emergency Commission, https://publicorderemergencycommission.ca/files/documents/Policy-Papers/Social-Cleavages-Understanding-the-Freedom-Movement-Graves.pdf.

[40] Jim Bronskill, "Anti-authority Narratives Could Tear 'fabric of society,' Intelligence Report Warns," CTV News, March 24, 2024, https://www.ctvnews.ca/politics/anti-authority-narratives-could-tear-fabric-of-society-intelligence-report-warns-1.6820025.

[41] Adam Entous, Craig Timberg, and Elizabeth Dwoskin, "Russian Operatives Used Facebook Ads to Exploit America's Racial and Religious Divisions," The Washington Post, September 25, 2017, https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html.

[42] Tessa Wong, "Technology has Become the Double-edged Sword of Asia's Protests," BBC, March 25, 2023, https://www.bbc.com/news/world-asia-64300442.