Summary Report

Author: Chris Tenove, Research Associate (School of Public Policy and Global Affairs), and Assistant Director (Centre for the Study of Democratic Institutions), University of British Columbia

Panel Theme: Disinformation, Digital Space, and Democratic Processes

Key Issues:

My contribution focuses on four issues:

- The nature of threats that foreign information operations pose to democratic processes and institutions.
- Characteristics of information operations that make them potentially harmful to Canadian democracy.
- Roles that government, industry and civil society actors can play in identifying and countering malign information operations.
- Policies by and for social media platforms that can help reduce threats posed by malign information operations.

Assessment:

While there is a long history of foreign information operations targeting democratic countries, the last decade has seen major developments in the forms they take and measures needed to address them. Of particular concern are information operations that may harm these core democratic goods:

- The free, full and informed participation of citizens, such as by deceptive messages about when and how to vote, or by using illegitimate methods to amplify some voices and marginalize others in online spaces.
- The fair competition among contestants for elected office, including efforts to intimidate or disparage candidates.
- The functional capacity of democratic institutions, such as by promoting false claims or violence in response to election outcomes.

Information operations can cause near-term harms to these democratic goods. In aggregate, they can contribute to long-term changes in our information systems and societies that put these goods at risk.

When seeking to identify and address foreign interference via communication, the terms "misinformation," "disinformation" and "malinformation" (MDM) have significant limitations. These terms focus on the content (truth or falsehood) and intent of messages. However, as the EU DisinfoLab and others note, "malicious actors have long understood that the best influence operations are not simply limited to false information."[1] Furthermore, it is often unhelpful to assess message intent because contemporary information operations are typified by *participatory propaganda.*[2] Propagandists rely on other individuals or organizations to (often unwittingly) spread their messages, or they amplify authentic content that aligns with the propagandists' goals.

Rather than MDM, this report focuses on "malign information operations." Information operations involve coordinated or complementary actions, including but not necessarily limited to acts of communication (for example by spreading material acquired through a cybersecurity breach). They are "malign" when they involve elements of coercion, financial interference, or deception. If a foreign actor contributes to a malign information operation, we can consider this to be foreign *interference* rather than legitimate *influence*.

Coercion is the use of violence, threats, or psychological abuse to manipulate behavior, including to undermine people's ability to participate in politics, compete for office, or enact their role in a democratic institution.

Canadian politicians, as we and other researchers have found, face increasing online and offline abuse. Both the intensity and volume of online abuse can reduce its targets' physical security or sense of security, harm their mental health, and shift their attention and resources away from campaigning or governing roles. [3] Online abuse tends to more negatively impact members of under-represented groups, including women and racialized individuals. Relatedly, information operations by Russia and other countries often seek to promote hostility and division on issues of gender, race, and immigration.[4]

The full extent of coercive communication targeting Canadian politicians and officials remains unclear. For comparison, a survey of state legislators in the United States found that 43% had faced a violent threat during their term in office and the preceding campaign, [5] often via social

[1] EU DisinfoLab. 2023. "FIMI: towards a European redefinition of foreign interference," p. 4. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf

[2] Wanless and Berk. 2022. "Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications." https://doi.org/10.2478/9788366675612-009

[3] Tenove and Tworek. 2020. Trolled on the Campaign Trail: Online Incivility and Abuse in Canadian Politics. https://democracy.ubc.ca/platforms/online-incivility-in-politics-in-canada/trolled-on-the-campaign-trail-online-incivility-and-abuse-in-canadian-politics/

[4] Al-Rawi and Rahman. 2020. "Manufacturing Rage: The Russian Internet Research Agency's Political Astroturfing on Social Media." https://doi.org/10.5210/fm.v25i9.10801; Bradshaw and Henle. 2021. "The Gender Dimensions of Foreign Influence Operations." https://ijoc.org/index.php/ijoc/article/view/16332.

[5] Brennan Center for Justice. 2024. Intimidation of State and Local Officeholders, p. 6. https://www.brennancenter.org/our-work/research-reports/intimidation-state-and-local-officeholders.

media. The full extent of *foreign* involvement in online abuse of Canadian politicians and office holders is also unknown.

A second element is financial interference, as discussed by Professor Heidi Tworek in her submission. This includes the illegal or illegitimate use of funds to amplify voices or narratives. For instance, the U.S. Department of Justice indicted two Russian nationals, accused of covertly directing funds that were ultimately funnelled to influencers based in the U.S. and Canada.[6]

Social media platforms have allowed foreign political advertising that contravenes campaign finance regulations.[7] Actors can amplify content using networks of fake accounts, achieving the goals of advertising without money transfers.

The third element is deception, which involves a misrepresentation of *who is communicating* or how *communication is occurring*, possibly in addition to misleading or abusive *content*. Meta's policy on "coordinated inauthentic behavior" (CIB) captures some of these factors, including the use of fake accounts or other deceptive techniques to promote content or evade platforms' terms of service.[8] Meta has publicized and acted on many cases of CIB employed by state-aligned actors against democratic countries.

AI technologies reduce the costs of producing and spreading deceptive content.[9] This includes the creation of deepfakes of individuals, such as the voice-cloning in the 2023 Slovakia election that has been attributed to Russia-aligned actors,[10] or the non-consensual intimate images that are frequently used to undermine women in politics. Generative AI can also be used to produce fake websites that appear to belong to legitimate news organizations or government departments.[11]

Some forms of coercion, financial interference or deception in communication may be illegal in Canada. However, foreign actors frequently skirt the edges of legality, such as by promoting hostility toward politicians rather than making direct violent threats. The European External Action Service notes that foreign information operations are "mostly non-illegal," which complicates legal responses.[12] Nevertheless, government responses are better directed at malign

---

[6] U.S. Attorney's Office. 2024. "Two RT Employees Indicted for Covertly Funding and Directing U.S. Company That Published Thousands of Videos In Furtherance of Russian Interests." https://www.justice.gov/usao-sdny/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published

[7] AI Forensics. 2024. No Embargo in Sight: Meta Lets Pro-Russia Propaganda Ads Flood the EU. https://aiforensics.org/work/meta-political-ads.

[8] Meta. 2024. https://transparency.meta.com/en-gb/policies/community-standards/inauthentic-behavior/

[9] McKay et al. 2024. Harmful Hallucinations: Generative AI and Elections. https://doi.library.ubc.ca/10.14288/1.0445035.

[10] Zmušková, B. 2023. "More Details about Russian Interference in Slovakia's Election Emerge." https://www.euractiv.com/section/politics/news/more-details-about-russian-interference-in-slovakias-election-emerge/.

[11] EU DisinfoLab. 2024. "What Is the Doppelganger Operation? List of Resources." https://www.disinfo.eu/doppelganger-operation/.

[12] EU DisinfoLab, *supra* note 1, p. 5.

information operations, which may or may not violate Canadian laws, rather than trying to evaluate the accuracy and intent of large volumes of content.

Recommendations:

A whole-of-society approach is needed to address foreign information operations. Different sectors have different capabilities and limitations to identify and mitigating them. Here I focus on three sectors: government, journalists and independent researchers, and social media platforms.

When it comes to identifying malign information operations, journalists and independent researchers can bring probable cases to light. However, they may struggle to identify surreptitious funding, deceptive foreign involvement, or coordination of online and offline activities. For these details, journalists and independent researchers frequently rely on information from social media companies or government.[13]

Social media platforms can identify coordinated online activities, patterns in violations of their own terms of service, and other elements of malign information operations. They can publicize these findings in transparency reports. Platforms can also provide data to external researchers and journalists to conduct investigations. Some of the most incisive research on foreign information operations draws on dataset of inauthentic Russian and Iranian accounts that Twitter published.[14]

Government actors, particularly those engaged in human and signal intelligence, may have critical insights for government and civil society actors regarding a nexus with malign offline activities or threat actors. This has been an important role of the G7 Rapid Response Mechanism.

Information sharing between government and social media platforms is necessary but fraught, and has been the focus of litigation and politicization in the U.S. To avoid risks to freedom of expression due to undue government pressure, government actors and social media platforms need clear guidelines and processes for information sharing.[15] This includes guidelines for information sharing between CSIS and platforms, made possible by Bill C70.

Mitigation of malign information operations can sometimes be achieved by exposing them and disseminating corrective information. This process, when driven by journalists and other private actors without government intercession, was referred to as "self-cleansing" of the media

[13] Tenove and MacLellan. 2022. "Confronting Disinformation: Journalists and the Conflict over Truth in #Elxn43." https://osf.io/p3r8q/download.

[14] Twitter. 2018. "Enabling Further Research of Information Operations on Twitter." https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter

[15] Perault. 2023. "Trust the Process." http://knightcolumbia.org/blog/trust-the-process-could-jawboning-process-solve-jawboning-problems.

ecosystem in the Inquiry's Initial Report. The Commissioner expressed some concern about this idea.[16]

More apt than "self-cleansing" are the terms "error detection" and "public correction." These are hallmarks of well-functioning democratic media systems, including in response to foreign propaganda and malign conspiracy theories.[17] However, there are factors that limit adequate public correction by private actors:

- Some individuals are unlikely to encounter corrective information in their information sub-systems. This can occur when people cannot access relevant and high-quality information in their spoken languages, or when they primarily inhabit dysfunctional sub-systems like the U.S. far right-wing media sphere.[18]
- Private actors may lack *capacity* to detect coordinated activity or a nexus with offline activities. For instance, journalists with exceptional skillsets played a pivotal role exposing the Buffalo Chronicle campaign in Canada's 2019 federal election,[19] but their news organization (*Buzzfeed News*) no longer exists.
- Private actors may lack *time* for effective error detection and public correction, particularly if malign information operations target moments like the eve of an election to push content.
- Public correction does not address direct harms from coercion and financial interference. In fact, publicizing these activities can sometimes exacerbate harms by further spreading abusive or illegitimately amplified content.

If these or other factors pertain, government actors – including the Panel of 5 – may need to publicly identify information operations or provide relevant information to private actors (e.g. journalists and social media platforms).

Social media platform policies are also key to mitigation. Most platforms have policies on harassment, illegitimate political advertising, misleading AI-generated content, and other forms of communication that relate to coercion, financial interference or deception. Government should therefore encourage social media platforms to pursue the ongoing improvement and fair enforcement of their policies.

The proposed Online Harms Act, currently before Parliament, does not specifically address foreign interference or disinformation. It may, however, enhance resilience to them. For instance, this legislation would require platforms to develop processes to address incitement of violence, intimate content shared without consent (including those that are AI-generated), and other forms of coercive communication. It would also improve platform transparency. Clear, enforceable

---

[16] Hogue. 2024. Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions: Initial Report, p. 26.

[17] Benkler et al. 2018. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. https://academic.oup.com/book/26406

[18] Ibid.

[19] Hogue, *supra* note 16, pp. 121-2.

regulations for social media are increasingly necessary, given the declining willingness or ability of some platforms to take good-faith efforts to protect democratic processes.[20]

Finally, mitigation of information operations is not limited to informational responses. Also important are mechanisms to support targets of coercion (including security and psychological support), to freeze funds used for financial interference, and to hold to account foreign and domestic actors that participate in illegal activities.

[20] Free Press. 2023. Big Tech Backslide: How Social-Media Rollbacks Endanger Democracy Ahead of the 2024 Elections. https://www.freepress.net/big-tech-backslide-report; Jackson and Hendrix. 2024. "Musk, X, and Trump 2024: Where Are the Legal and Ethical Boundaries?" https://www.justsecurity.org/100265/musk-trump-legal-boundaries/.