Public Inquiry Into Foreign Interference
in Federal Electoral Processes and
Democratic Institutions

Enquête publique sur l'ingérence étrangère
dans les processus électoraux et les
institutions démocratiques fédéraux

Summary Report

Author: Professor Heidi Tworek, Canada Research Chair and Director, Centre for the Study of Democratic Institutions (CSDI), University of British Columbia, Vancouver

Panel Theme: Disinformation, Digital Space, and Democratic Processes

Key Issues:

Many of the key issues around the role of foreign interference in information environments also pertain to regulating social media more broadly. But particularly germane for my report to this inquiry are the following:

How does MDM affect democratic institutions? Should Canada address and identify the actors, behaviour, content, or other aspects of MDM? What is the role of government versus social media platforms versus civil society?

Given that MDM is a long-standing tool for many states, what can Canada learn from other jurisdictions affected by this problem?

Finally, what do we know about the effects of MDM and tools to counter it?

Assessment:

Foreign interference in elections is as old as elections themselves. Russia interfered in the democratic election of a king in Poland-Lithuania back in 1697. The phenomenon was common during the Cold War: from 1946 to 2000, the United States and Soviet Union intervened in around 11 percent of all national executive elections around the world.[1]

The specific role of information, however, has changed quite dramatically over time. The past offers no simple solutions. But it helps to parse out what is unprecedented and requires new policies.

I see at least five major new developments with the emergence of digital media:

First, there is a considerably lower barrier to entry to use and abuse platforms and messaging.

Second, there are substantially greater financial incentives to produce information, whether through ads, selling products, or other forms of online influencing.

Third, more individualized targeting can occur due to far more granular data.

[1] https://global.oup.com/academic/product/meddling-in-the-ballot-box-9780197519882

Fourth, there is a proliferation of private spaces, e.g. messaging apps, that enable communication amongst groups such as diaspora communities.

Finally, there is the rapid disappearance of material. There is link rot; there is the disappearance of websites; and there is the inaccessibility to platforms. This can make it hard to understand what happened last week, let alone last decade. Findings of the historical sort I outlined become nearly impossible in an environment controlled mostly by private companies who have little incentive to store data for the long-term or to make it accessible to researchers.[2]

Despite these changes, many underlying dynamics are similar to the past. My own historical research on how new communications technologies affect democracy has shown that informational interference is an international relations problem.[3] States often turn to information as a cheap form of interference. As the cost continues to drop, the incentives to invest in information grow. At the same time, information exchanges across borders are a legitimate and important part of human life. And some measures to prevent misuse of information can ironically enable problematic censorship and control of content by less democratic governments in the future or by autocrats abroad.[4]

All this suggests that while content obviously matters, there are other ways to address networks of foreign interference. The specific harms may stem less from the information itself than the manipulation of the information environment. Camille Francois, for example, suggested the ABC framework: actors, behaviour, content.[5] Actors and behaviour can be problematic, even if the content is not.

History suggests at least two other factors: the first is communications infrastructure, though this lies less within the Commissioner's mandate.[6] The second factor is finance. Financial interference can take multiple modes. To name two examples: paying to promote posts on platforms or paying domestic actors off-platform to spread information online. New communications technologies often offer new ways to finance information operations. But the methods of tracking financial flows generally already exist. I and others have long warned about the importance of this aspect of the online ecosystem.[7]

It is also critical to remember that some foreign actors may be driven solely or primarily by profit. The now infamous Macedonian town of Veles produced many hoax stories during the 2016 election; ethnographic work has shown that "the driving force behind the Veles fake news business is economics rather than politics."[8]

[2] https://www.cigionline.org/articles/open-access-to-data-is-critical-in-a-democracy/ On link rot, see https://www.theatlantic.com/technology/archive/2021/06/the-internet-is-a-collective-hallucination/619320/

[3] https://www.hup.harvard.edu/books/9780674988408 and https://www.cambridge.org/core/books/disinformation-age/policy-lessons-from-five-historical-patterns-in-information-manipulation/143E9A2A61FEBEA66E012966C90B5ECF

[4] https://www.theatlantic.com/international/archive/2019/05/germany-war-radio-social-media/590149/

[5] https://www.ivir.nl/publicaties/download/ABC_Framework_2019_Sept_2019.pdf

[6] https://www.cigionline.org/articles/internet-governance-cant-be-divorced-infrastructure-governance/

[7] https://www.cigionline.org/articles/authorities-were-warned-about-extremist-fundraising-online-but-did-not-seem-to-hear/

[8] https://www.cambridge.org/core/journals/ps-political-science-and-politics/article/macedonian-fake-news-industry-and-the-2016-us-election/79F67A4F23148D230F120A3BD7E3384F

Another important aspect of MDM is online abuse and harassment, which may overlap with information operations. Online harassment can affect politicians and political candidates psychologically; it can rob them and their teams of time to campaign and govern, because they are busy dealing with threats; it can undermine their feelings of and actual physical safety. It can deter potential office-seekers. Such online abuse may particularly dissuade women, racialized, and other candidates from equity-deserving groups.[9] Online abuse of civil servants or others such as public health officials can similarly reduce people's willingness to serve in these important posts.

One final important point: it remains difficult to measure the exact effects of particular pieces of information on individuals and, arguably, this may not even the right question as it is too narrowly focused on a single moment or single platform and does not view people as embedded within communities and online-offline relationships.[10] Scholars also continue to investigate the broader question of the causal relationship between accurate information and attitudes, for example about immigration.[11] We also know that these issues existed long before the rise of social media.

For the purposes of this Inquiry, what sometimes matters more than how information may affect voters is how politicians *think* it affects voters and thus the measures that they might enact. Any measures need to be considered in the long-term, with the understanding that there are still many open questions in the research on effects, and in light of how to preserve broader democratic values like freedom of expression.

Any policy approaches thus need to consider three questions: first, what are pre-existing problems for which we already have policies in place? Second, how do we enforce existing policies more stringently? Third, for new issues, what new policies are necessary?

Recommendations:

First and broadest: Informational interference cannot be addressed through information alone. On the supply side, much information interference arises from issues within diplomacy. What is needed is better analysis and understanding of when states turn to informational interference and why. That means creating concrete links between, for example, the Rapid Response Mechanism and foreign policy analysts. Another complementary approach would be to create an expert council of scholars and civil society organizations to advise about potential sources and dynamics of MDM. This could be similar to the National Expert Committee on Countering Radicalization to Violence at the Public Safety Ministry (on which I currently am serving a two-year term).[12]

Second, financial flows require more attention, whether through FINTRAC or the Financial Action Task Force. More enforcement of existing rules and greater international coordination could go a long way.

Third, developing and enforcing transparency rules for platforms will help researchers to identify and understand more about the prevalence and effects of information operations.[13] Bill C-63 goes

[9] https://democracy2017.sites.olt.ubc.ca/files/2020/10/Trolled_Oct-28.pdf

[10] https://euvsdisinfo.eu/disinformation-is-one-problem-among-many-in-the-information-environment-interview-with-alicia-wanless/

[11] https://www.journals.uchicago.edu/doi/abs/10.1086/699914

[12] https://www.publicsafety.gc.ca/cnt/bt/cc/ntnl-xprt-cmmtt-en.aspx

[13] https://www.cigionline.org/articles/how-transparency-reporting-could-incentivize-irresponsible-content-moderation/

some way towards this. Such transparency will enable more Canada-specific research on susceptibility to foreign interference and effects, including a more differentiated look at a wide range of communities. We should also consider as much transparency as feasible from the government's side. Such transparency has increased trust in Taiwan, for example, though we should not see transparency as a simple panacea.[14]

Fourth, it is crucial to develop more robust, whole-of-society policies to address online abuse. These include: supporting civil society efforts at counterspeech or proactive protections; requiring more rapid response from social media platforms around online threats to public figures; building insititutional policies and capacity to support civil servants and elected officials when they are faced with online abuse.[15]

Finally, I recommend applying a two-part test to any new policies. First, consider how an authoritarian regime might copy and misuse a policy. This can ensure that measures preserve broader democratic values like freedom of expression. Second, think through how non-cooperative platforms might react. Tech companies might call this red-teaming, or thinking through the worst-case scenario uses of a policy in Canada in the future or abroad.

Additional Remarks: I assessed the US government's attempt to create a Disinformation Governance Board in 2022 and suggested reasons for its failure in the article linked in this footnote.[16]

[14] On Taiwan, https://www.theguardian.com/commentisfree/article/2024/jul/22/taiwan-bucked-global-trend-trust-politics-hired-protesters On the limits of transparency for increasing trust, see https://www.researchgate.net/profile/Stephan-Grimmelikhuijsen-2/publication/254886772_Linking_Transparency_Knowledge_and_Citizen_Trust_in_Government_An_Experiment/links/5a1843d7a6fdcc50ade7daa2/Linking-Transparency-Knowledge-and-Citizen-Trust-in-Government-An-Experiment.pdf

[15] For more suggestions, see https://democracy2017.sites.olt.ubc.ca/files/2020/10/Trolled_Oct-28.pdf

[16] https://www.cigionline.org/articles/can-we-move-beyond-disinformation-studies/