Summary Report

Author: Elizabeth Dubois, Associate Professor & University Research Chair in Politics, Communication and Technology, University of Ottawa

Panel Theme: Disinformation, Digital Space and Democratic Processes

Key Issues:

This report focuses on the question: What approach should Canada take in confronting the challenge that mis-, dis- and mal- information (MDM) poses to our democratic institutions: targeting the substance of the information, those who produce it, the mechanisms by which it is disseminated?

In doing so other issues are considered, including whether and how the government publicly identifies MDM attributed to foreign actors, how MDM unevenly affects different communities, the role of building public resilience and educating citizens, and the responsibility of social media platforms in combating MDM.

Assessment:

To understand how to identify and deal with MDM, and other information campaigns created or promoted by foreign actors in elections, it is critical to call attention to how different elements of the information ecosystem relate to, and are dependent upon, one another. Responses to the challenges of MDM by foreign actors must not focus uniquely on particular tools, content, or actors, but rather relationships among them. Focusing on the network of actors, tools, content and their relationships underscores important characteristics of the information ecosystem and the flow of MDM within it.

A piece of MDM posted to a private Facebook page could be commented on in a large but private WhatsApp group, discussed face-to-face, and talked about by an influencer publicly on TikTok. By the time the idea reaches TikTok the form of the content has changed, the idea has likely evolved as people's own perspectives are added, and the idea has traversed a range of settings.

Indeed, in the current ecosystem, MDM does not stay in one place, be that on a particular platform, within a single organization, or between specific actors. MDM flows both online and offline, again and again, through day-to-day social interactions. MDM also flows through public, semi-private and completely private spaces, presenting unique challenges when trying to understand how information moves through the complex ecosystem. Finally, MDM is not confined to its original form; as the ideas in the content are reproduced, they can evolve, and leave lasting impressions on users, shaping their beliefs and interactions with others. This understanding of a networked flow of information is crucial when trying to track foreign interference and MDM.

Within this context of a networked information ecosystem, this assessment considers four key factors in the spread of MDM by foreign actors within Canada.

Foreign actors leverage systems that control the spread of information to insert and promote MDM

Social media platforms are points of entry through which foreign actors can insert MDM into the ecosystem. The reach of these platforms allows them to target communities that might otherwise be difficult or impossible to reach.[1] Once introduced, foreign actors count on MDM flowing across the ecosystem.[2] This makes it important to develop tools to trace the spread of MDM across multiple platforms and users. The challenge is that ideas are much harder to trace than specific pieces of content, and as MDM flows through the ecosystem the content form may change.

There is far more content available in the ecosystem than any person can consume.[3] Systems, such as the algorithms underpinning social media feeds, which curate and control the flow of information, dictate what a person is likely to see or what content is presented as most important. Foreign actors learn how to interact with these systems to ensure their messages are spread across a platform and beyond. To limit the spread of MDM, it is necessary to understand how these systems make decisions and what type of content they incentivize and disincentivize.

Further, when foreign actors insert MDM into the ecosystem, they understand that ideas will show up for a given person in multiple online spaces, and capitalize on the human tendency to believe things more when seen repeatedly.[4]

Information flow camouflages the activity of foreign actors

Foreign actors understand that MDM entering the ecosystem will spread beyond the initial platform, developing a flow that cannot be completely controlled.[5] They capitalize on the ecosystem's networked structure by strategically placing content in one part of the system, knowing it will be distributed more widely across different spaces: on- and offline, private and public, and back again. This multi-stepped information flow creates distance between the instigating foreign actors and MDM, and can make it appear as though foreign-funded content is domestic in origin. As MDM is consumed and shared, a piece of content initially created by a foreign actor is inserted and re-inserted into legitimate domestic conversations, further complicating attribution.

This makes it difficult to trace the flow of the content or ideas back to the instigator and undermines a "follow the money" approach for dealing with MDM and identifying foreign actors. While these actors may spend money on securing the initial placement of content, unknowing platform users may reproduce MDM within their own unique content. Consider the

---

[1] Ronan Ó Fathaigh, Tom Dobber, Frederik Zuiderveen Borgesius, et al., "Microtargeted propaganda by foreign actors: An interdisciplinary exploration," *Maastricht Journal of European and Comparative Law* 28, no. 6: 856-877, accessed October 30, 2024. https://journals.sagepub.com/doi/10.1177/1023263X211042471.

[2] *Ibid*.

[3] Paul Hemp, "Death by Information Overload," *Harvard Business Review*, September 2009, https://hbr.org/2009/09/death-by-information-overload.

[4] Raunak M Pillai and Lisa K Fazio, "The effects of repeating false and misleading information on belief," *Wiley Interdisciplinary Reviews: Cognitive Science* 12, no. 6:1-21, accessed October 30, 2024. https://pubmed.ncbi.nlm.nih.gov/34423562/.

[5] Dominique Cardon et al., "Fake News in the Digital Public Space," Sciences Po, April 23, 2020, https://www.sciencespo.fr/en/news/the-digital-public-space-and-the-problem-of-fake-news/.

example of Tenet Media, a Canadian-led right-wing media start-up alleged by the United States to have received illicit funding via Russian sources.[6] Six established social media influencers were hired to create online content, which was distributed not only through Tenet Media, but also across their various networks using strategies like collaborations, reaction videos, and building from their own follower base.[7]

Although MDM attribution is important for understanding and controlling its flow, the lifecycle, ideas represented, and various actors and platforms involved in sharing the content in its various forms must be considered to understand the actual impacts on elections and voters.

Assessing risk levels of MDM by foreign actors requires a long view

In 2019, during the 43rd General Election, the Critical Election Incident Public Protocol (CEIPP) was created to "establish a mechanism to communicate clearly, transparently and impartially with Canadians during an election in the event of an incident or a series of incidents that threatened the election's integrity."[8] There is currently a high threshold for alerting the public to foreign interference;[9] however, much online MDM by foreign actors never comes close to that threshold because the goal of foreign information campaigns is longer term. Within the context of an election, attention is called to only the highest-level threats (e.g., those things most likely to pose a risk to the integrity of that election).

Yet, lower threshold incidents can also threaten elections through repeated low-level MDM. This MDM can undermine trust in the wider information ecosystem,[10] which, when no longer trusted, can in turn undermine trust in wider electoral systems. The risk is, in an information ecosystem where no one knows what or whom to trust, people will become less engaged, and less trusting of all political systems including specific elections, whether their beliefs are founded or not.[11]

Notably, these lower-level threats often begin before a formal election period because foreign information campaigns, like most modern political campaigning, happens continually.[12] Consider social media influencer accounts where resources and energy are poured into building audiences for years. The real value of having content spread by that influencer is based on their audience and placement in the wider information ecosystem.

---

[6] Zachary Cohen, Donie O'Sullivan, Evan Perez, Sean Lyngaas, and Majlie de Puy Kamp, "DOJ alleges Russia funded US media company linked to right-wing social media stars," *CNN* online, last modified September 5, 2024, https://www.cnn.com/2024/09/04/politics/doj-alleges-russia-funded-company-linked-social-media-stars/index.html.

[7] Elizabeth Dubois, Michelle Hennessey, Michelle Bartleman, and Louise Stahl, "Incident Update 3 | Exploring Impacts of Using Influencers for Foreign Interference," Canadian Digital Media Research Network, October 10, 2024, https://www.cdmrn.ca/publications/russianfundingcanadianinfluencers/impact.

[8] "Critical Election Incident Public Protocol," Government of Canada, last modified July 11, 2024, https://www.canada.ca/en/democratic-institutions/news/2023/02/critical-election-incident-public-protocol.html.

[9] *Ibid*.

[10] Gabriel R Sanchez and Keesha Middlemass, "Misinformation is eroding the public's confidence in democracy," Brookings, July 26, 2022, https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/.

[11] *Ibid*.

[12] "Tackling Disinformation, Foreign Information Manipulation & Interference," European Union External Action, May 27, 2024, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

Diaspora and hyper-connected communities are at an increased risk

Foreign interference and MDM disproportionately target marginalized communities.[13] Diaspora communities have been identified as both potentially targets of, and more susceptible to, foreign interference. In online settings, this is partly because the close social relations among people within many diaspora communities allows MDM to travel quickly through their networks.[14] These close social ties can also be found within hyper-engaged online communities, such as intensely partisan groups and conspiracy theory groups, which also become targets.

Recommendations

A: Increase communication from government to the public

As described above, CEIPP/the Panel have a high threshold for when to share information about foreign interference in elections with the public. This approach should be modified in at least three ways:

1) Develop response options for low-level threats, which may in fact be higher level in their aggregate and over time. Various governmental actors beyond The Panel could be involved ahead of the election to help identify and address such lower-level threats and develop responses, which will require different strategies and approaches.

2) In decisions about the public communication of foreign interference in elections, the focus should not only be on identifying who has created or shared the MDM, but also on how the public perceives or will perceive their information environment. The risk of the public knowing about threats should be weighed against the risk of the public losing trust in the reporting system, as well as in their information environment. Clarity on this assessment criteria and process should also be made public to the extent that it does not compromise investigations.

3) Better reporting following elections is needed and should include information on the kinds of threats that were identified but not addressed in real time, as well as justification for those choices.

B: Build citizen resilience through media and digital literacy and political engagement

Prebunking and debunking are generally effective at reducing reliance on misinformation,[15] but are strategies best implemented within the context of comprehensive digital and media literacy campaigns, which should include education to help people understand how ideas flow through the information ecosystem. An electorate that feels capable of assessing and navigating their complex information ecosystem is essential. This is particularly important because there is a concern that as more evidence of foreign interference and disinformation comes to light, people

[13] Samuel Woolley, "In Many Democracies, Disinformation Targets the Most Vulnerable," Centre for International Governance Innovation, July 18, 2022, https://www.cigionline.org/articles/in-many-democracies-disinformation-targets-the-most-vulnerable/.

[14] Cailin O'Connor and James Owen Weatherall. "Why we trust lies," Scientific American, vol. 321, no. 3, 2019, pp. 54–61.

[15] Bruns, H., Dessart, F.J., Krawczyk, M. *et al.* Investigating the role of source and source trust in prebunks and debunks of misinformation in online experiments across four EU countries. *Sci Rep* **14**, 20723 (2024). https://doi.org/10.1038/s41598-024-71599-6

could disengage from their information and political systems, not knowing what to trust.[16] While understanding all the technical components is not feasible, increased understanding is possible. Supporting civil society groups, especially those who are trusted among people who are most often targets of MDM by foreign actors, and increasing education about the information environment, and media and political systems is needed.

C: Legislate transparency from platforms

Social media platforms have the power to change their technical structures so that their algorithms are less easily exploited by nefarious actors. They also have near exclusive access to data about how often MDM is being created and shared on their platforms, by whom, and across which user groups.

While platforms do need to take steps towards self-regulation, self-imposed regulations or safeguards are not enough. These can quickly be changed without notice, which is extremely problematic in the context of an election. Should a platform suddenly remove safeguards they had put in place, there would be limited options to deal with sudden influxes of MDM during an election.

[16] Lukito, Josephine. "Digital Disinformation, Electoral Interference, and Systemic Distrust." Routledge Handbook of Disinformation and National Security, 1st ed., Routledge, 2024, pp. 122–34, https://doi.org/10.4324/9781003190363-12.