International Journal

Policy Brief

Countering foreign disinformation: Building a resilient Canadian democracy through stronger education and regulation

International Journal
2025, Vol. 80(3) 513–523

DOI: 10.1177/00207020251372185
journals.sagepub.com/home/ijx

Simon Hogue
Université du Québec à Montréal, Montréal, Québec, Canada

Magalie Lavallée
Université du Québec à Montréal, Montréal, Québec, Canada

Benjamin C.M. Fung
McGill University, Montréal, Canada

Abstract

Canada's Foreign Interference Commission released its initial report in May 2024, expressing concerns about meddling by foreign actors in Canadian elections and threats to public confidence in Canada's democratic institutions. Just three days later, the Canadian government tabled its response in the form of Bill C-70, the Countering Foreign Interference Act. Both constitute considerable progress and demonstrate Ottawa's willingness to act against the growing threat. However, both are limited—the report focusing on internal institutional dynamics, and Bill C-70 remaining mostly silent on one of the most important tactics of interfering countries: disinformation. Does Canada have the tools to respond to this threat effectively? In examining the Commission's reports, Bill C-70, and current Canadian practices, we argue that while Ottawa already deploys tactics to counter disinformation, it could do more by implementing two tested strategies: working with provincial, territorial and Indigenous governments to integrate media literacy within education curriculums,

Corresponding author:
Simon Hogue, Department of Political Science, Université du Québec à Montréal, Pavillon des Sciences de la gestion, 315 Rue Sainte-Catherine Est, Montreal, Quebec, H3C 3P8, Canada.
Email: hogue.simon@uqam.ca

and implementing stronger regulation of social media platforms responsible for circulating disinformation.

Keywords
foreign interference, disinformation, Canada, democracy, media regulation, resilience

After months of public and partisan pressure on the Canadian government—including the premature resignation of Prime Minister Trudeau's appointed special rapporteur to examine foreign interference, warnings by national security advisors, and the expulsion of a Chinese diplomat accused of foreign interference—Canada launched a public inquiry into foreign interference in September 2023. The Foreign Interference Commission released its initial report in May 2024, expressing concerns about meddling by foreign actors in Canadian elections and threats to public confidence in Canada's democratic institutions. Only three days later, the Canadian government tabled its response in the form of Bill C-70, the Countering Foreign Interference Act. Both constitute considerable progress and demonstrate Ottawa's willingness to act against the growing threat. However, both are limited in their own respects—the report focusing on internal institutional dynamics, and Bill C-70 remaining mostly silent on one of the most important tactics of interfering countries: disinformation.

Disinformation is arguably one of the most damaging threats to Western societies, including Canadian society, and, by extension, to democracy.[1] Interference practices to influence the vote, such as busing students to vote in party-level elections, certainly deserve scrutiny, but disinformation polarizes, targeting the social cohesion and trust that make public debates and democracy possible. In the public inquiry's final report in 2025, Commissioner Marie-Josée Hogue[2] remarks that "information manipulation (whether foreign or not) poses the single biggest risk to our democracy" and remains an "existential threat" invite further exploration.[3] Building on the Commissioner's observations, we ask: does Canada have "the tools to effectively respond" to this threat?[4]

We begin by examining the Commission's work and Bill C-70 to understand the place of foreign disinformation in these recent efforts, before turning to Canada's response to the threat. We argue that while Ottawa is deploying tactics to counter disinformation, Canada should implement two tested strategies to help protect its citizens from disinformation: working with provincial, territorial, and Indigenous governments to integrate media literacy into education curriculums, and more strongly regulating social media platforms responsible for circulating disinformation.

Disinformation: An existential threat to tackle urgently

The Commission's initial and final reports are unequivocal about the risks of foreign interference: it is not only a real threat to Canadian democracy and national security,

but an "incredibly sophisticated" one.[5] Although the Commission acknowledges that malevolent foreign actors targeted the 2019 and 2021 general elections, particularly by interfering at the riding level and in candidate nominations, the Commission affirms that overall election results were not affected by these efforts.[6] At the same time, the Commission notes, "While allegations of interference involving elected officials have dominated public and media discourse, the reality is that misinformation and disinformation pose an even greater threat to democracy."[7] In response to this serious threat, the Commission's final recommendations focus—as the Johnston Report's did previously[8]—on the machinery of federal institutions, treating the roles of the media, social media platforms, and civil society as secondary. Over 80 percent of the recommendations focus on national security institutions (such as intelligence, police, and relevant departments); coordination between institutions; parliament and political parties; and Canada's independent electoral agency, Elections Canada.[9] While these mechanisms certainly play a central role in monitoring and countering foreign disinformation, the longer-term value of what the Commission categorizes as "civic resilience" must not be underestimated, as it targets two key actors in the disinformation ecosystem: citizen-consumers and social media platforms.[10]

Despite the urgent need to tackle disinformation, Bill C-70, the Countering Foreign Interference Act—introduced at the same time as the Commission's initial report—provides little support on this matter.[11] It aims to strengthen the courts' capacity to act against foreign interference, but it was not intended—and, thus, is not designed—to tackle the issue of disinformation. Instead, it creates new legal instruments and strengthens existing sanctions while creating new ones to enable the courts to punish a wider range of fraudulent or clandestine activities committed in Canada by individuals or organizations harming Canada's interests on behalf of foreign states, such as undermining the integrity of its electoral mechanisms. It introduces new offences to punish the deliberate sabotage of Canada's critical infrastructure as well as activities of interference—such as intimidation, threats, or acts of violence—to protect the population, particularly members of diasporas at risk of exposure to coercive influence.[12] It also updates the Canadian Security Intelligence Service Act, which has undergone no significant modifications since its creation during the Cold War, to reflect the realities of the digital era, and establishes a foreign agents registry. From all of this, however, disinformation remains largely absent.

In sum, the two most recent federal initiatives propose, at best, partial solutions to the problem of foreign disinformation. Pursuing the Commission's objective to equip Canada with effective tools, we now examine what Canada is doing, and offer policy recommendations.

The multifaceted Canadian approach to disinformation: Acting with caution

Ottawa has taken a broad approach to fighting a problem shaped by two related issues: foreign interference and disinformation. In this sense, we could conclude that Canada's

approach to foreign disinformation is in the image of its disinformation strategy: multifaceted, "first, because it employs a suite of tactics; and second, because it involves a mix of regulatory approaches."[13] The Canadian approach also includes various governmental and private—corporate and civilian—actors. Yet, as the Commission observes, foreign disinformation remains a threat despite these measures.

Under the Government of Canada's "Plan to Protect Democracy," the government commits to four "pillars of action": enhancing citizen preparedness, improving organizational readiness, combatting foreign interference, and building a healthy information ecosystem.[14] Among these, some initiatives stand out as key to fighting foreign interference.[15] The Critical Election Incident Public Protocol (CEIPP) and the Security and Intelligence Threats to Elections Task Force (SITE TF), both composed of top-level civil servants of relevant ministries and security agencies, monitor elections for foreign threats and inform the public of any events that could jeopardize electoral integrity. More broadly, they encourage communication between the many institutions of the federal government. In addition, two coordination structures, the Protecting Democracy Unit, established in 2022 within the Privy Council Office, and the National Counter Foreign Interference Coordinator, established in 2023 within the department of Public Safety Canada, exist to, respectively, "coordinate, develop, and implement government-wide measures" and facilitate the circulation of intelligence and provide advice on responses to threat.[16]

Alongside these, Canada initiated the Rapid Response Mechanism (RRM) at the 2018 G7 Summit to deliver a coordinated response to foreign disinformation. Situated within Global Affairs, the RRM brings together G7 countries, the European Union (EU), participating observer states—including Australia, New Zealand, the Netherlands, and Sweden—and NATO. It functions as a mechanism for monitoring incidents, anticipating future risks, and facilitating the exchange of best practices.

Finally, the Digital Citizen Initiative (DCI), established by the department of Canadian Heritage in 2019, provides recurring rounds of funding to support research and civilian activities to enhance democratic resilience. Most notably, it finances the Canadian Digital Media Research Network, administered by the Media Ecosystem Observatory, a joint initiative of McGill University and the University of Toronto. The research and activities within the DCI cover a broad range of topics, with previous special financing for fighting disinformation during the pandemic and the war in Ukraine, and more recent calls to develop "tools to support digital media and civic literacy skills," to "prevent and address online violence against women, girls and 2SLGBTQI + communities," and to promote "resilience to mis-/disinformation stemming from foreign governments."[17] In that sense, the DCI lies at the intersection of foreign and homemade disinformation.

More general measures initiated to combat disinformation—including non-state-sponsored disinformation—can also contribute to countering foreign interference.[18] Among these, the 2018 Elections Modernization Act creates the obligation for social media platforms to hold a registry of political advertising. It also prohibits the publication of content with the "intent of misleading the public into believing that it was … authorized"

by Elections Canada or a political party or candidate, and the publication of false statements on parties or candidates, narrowed to specific types of content to preserve freedom of expression.[19] In addition, Ottawa has proposed two norm-based initiatives, the Declaration on Electoral Integrity Online and the Digital Charter. [20] The two initiatives set norms of conduct for platforms as well as principles to guide future actions regarding disinformation. The latter, however—proposed as the Digital Charter Implementation Act in 2022—has since stalled in parliament. Canada thus encourages platforms to take responsibility for moderating their content, but as Dawood observes, "The main drawback to a norms-based approach … is that it relies on large social media platforms to do the right thing rather than requiring them to do so."[21]

In 2024, the government presented the Online Harms Act (Bill C-63) to Parliament. Intended to create a "safer online space," the bill seeks to increase the obligation of platforms to address harmful content such as nonconsensual intimate content, the bullying of children, child pornography, or content fomenting hatred and inciting violent extremism, terrorism, or violence.[22] The bill, however, received substantial criticism from civil society and has not progressed in parliament since a debate at the second reading in September 2024—making its adoption unlikely in the near future.[23] Yet, even if the Online Harms Act were to become law, it would address, at best, a narrow slice of foreign disinformation.

Despite Canada's multifaceted approach to countering foreign disinformation, the Commission remains convinced, as do we, that additional measures must be taken to strengthen Canadian democracy and reduce the effects of foreign disinformation. While there is no silver bullet to this problem, we propose two areas in which Ottawa, with its provincial, territorial, and Indigenous counterparts, could invest: integrating media literacy into education curriculums, and more strongly regulating social media platforms responsible for circulating disinformation.

Strengthening resilience: Targeting the consumption and circulation of disinformation

Because exploiting national divisions is a key tactic of foreign interference, measures intended to improve democratic health will likely benefit national security. While some have argued that improving democratic resilience is insufficient and needs to be supplemented by more deterrent punitive measures,[24] we emphasize the importance of protecting Canada from the effects, rather than the existence, of foreign interference. We argue that incorporating stronger media literacy into education curriculums from an early age and imposing stricter regulations on social media platforms would yield significant long- and short-term benefits.

This position builds on the assumption that foreign disinformation is not simply a piece of content, but a process. The content is strategically created by malicious actors, then circulates through media technologies to reach its audience or consumers. As Mike Wigell notes, "Authoritarian regimes such as China, Iran, Russia, and Turkey

did not create the initial conditions of the current polarizing tendencies that make Western democracy vulnerable—they are merely seizing the moment to opportunistically foment these tendencies."[25] We argue that this notion of "opportunity" must be broadened. Disinformation may originate from malicious foreign agents, but its effectiveness relies on a wide array of structures exterior to the control of these agents: social media infrastructure, weak national regulations, the reproduction of populist and false discourses by public figures, and a susceptible networked public characterized by group-based fear and resentment and a general eroding trust in public institutions. Foreign agents hit the first domino and profit as the rest fall. While each of these dominos could warrant a full discussion,[26] we focus here on two key stages in the disinformation chain: consumption and circulation. This is an acknowledgment that, unfortunately, Canada has little control over the production of disinformation: the cost of producing it is low, and will likely remain so, decreasing further with advances in artificial intelligence. Given this reality, the soundest strategy is to target the points in the chain where intervention is actually possible.

Efforts to counter disinformation must target the reasons why consumers believe disinformation in the first place. Research shows a strong link between, on one side, pre-existing attitudes and beliefs, or partisanship and polarization, and, on the other side, acceptance of disinformation and resistance to debunking.[27] Therefore, once individuals are radicalized, it becomes difficult to challenge their alternate realities. This means acting upstream to prepare individuals to understand the mechanism of online radicalization before foreign influence campaigns strike. To reach this preventative goal, Ottawa could look to some of its allies. Finland, Sweden, the Netherlands, Latvia, and numerous American states have implemented pedagogical initiatives to teach media literacy to schoolchildren.[28] For example, in 2019, Finland adopted the National Media Education Policy, which integrates digital and information ecosystems into the regular school curriculum from pre-school through the full duration of public education. The programs teach children media literacy, digital skills, internet safety, and critical thinking to develop their capacity to identify falsehoods and understand how social media platforms function. The policy seeks to promote democratic participation and reduce polarization, and appears to be successful as the country repeatedly ranks first among European countries in resilience against misinformation.[29] Canada could follow suit.

Integrating media literacy and digital skills into school curriculums would also formalize the existing ad hoc initiatives funded through the DCI, and could institutionalize expertise developed by academia and civil society. Implementation, however, poses obvious difficulties: beyond political opposition, the Canadian constitutional context creates challenges to implementing a countrywide project, as education falls under provincial jurisdiction. Still, the federal government could work with the provinces and civil society to create a general framework that could be adapted to the local particularities of each education curriculum.

From a circulation perspective, the belief that the invisible hand of the information market will solve the problem plaguing the digital ecosystem is, at best, misguided and,

at worst, delusional. Indeed, social media platforms have demonstrated that self-regulation is insufficient, and may even run counter to their corporate interests. Canada must therefore strengthen its regulation of these platforms with obligations and penalties for non-compliance. This would supplement previous norm-based initiatives and extend the time frame of counter-disinformation measures beyond the electoral period, as suggested by the Commission (although its recommendation refers narrowly to the 2018 Elections Modernization Act).

Again, Europe inspires. After proposing revolutionary privacy protection with the General Data Protection Regulation—which has since been imitated around the world, including in Quebec's Law 25—the EU implemented the Digital Services Act (DSA) in 2023, which forces platforms to take content moderation seriously, and imposes additional obligations for "very large online platforms."[30] Under the DSA, these large online platforms must "identify, analyse, and assess any systemic risks" linked to their services, establish functions to mitigate these risks, and be audited by independent auditors. As such, the DSA does not determine how platforms will implement the new measures, but provides guidelines on where actions should be taken.[31] Notably, the DSA compels platforms to set up a dedicated internal team prior to each election and to adopt risk mitigation measures for electoral processes—such as easing access to official information; promoting media literacy initiatives; providing contextual analysis, including fact-checking labels; and labelling content from EU states, third countries, and their entities. Platforms must also ensure that their recommender systems limit the amplification of disinformation and demonetize disinformation content, among other actions outlined in the guidelines. In addition, the DSA promotes transparency and accountability by sharing data with public authorities and allowing researchers to access platform data. In parallel, the DSA introduces certified "trusted flaggers," which are civil society groups working to identify disinformation. The initiative continues existing collaborations between civil society and platforms, but with enhanced institutionalization and transparency.[32] Non-complying platforms can be fined up to 6 percent of their annual worldwide turnover, or up to 1 percent for the "supply of incorrect, incomplete or misleading information" or for the "failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection."[33]

Stronger regulation does not mean the end of free speech. Because strategies like deplatforming have a heavier toll on free expression,[34] the DSA concludes that other measures, like reducing the prominence of disinformation through the configuration of algorithmic recommender systems or demonetizing disinformation content, could help reduce the circulation, visibility, and effect of disinformation while preserving free expression. Canada could also look to Taiwan, which does not ban posts, but instead greys them out and informs users that the post contains mis/disinformation. Users must then click a button to acknowledge the message, after which a notice appears explaining why the post was flagged. This approach has two alleged advantages: free expression is not compromised since the post is not censored, and platforms can use the post to teach users how to identify disinformation.

Doubtless, implementing stronger regulations on platforms will be met with opposition. The opposition Conservative Party of Canada under Pierre Poilievre opposed the Online Harms Act and would likely do the same with a DSA-inspired regulation. A group of civil society organizations, including Amnesty International and the Canadian Civil Liberties Association, signed a joint letter to warn against, among other things, changes to the Criminal Code proposed by the Online Harms Act that "risk creating a serious chilling effect on lawful speech and debate."[35] However, stronger regulation of social media platforms would not seek to criminalize speech, but to limit the circulation and visibility of disinformation by imposing clear obligations and penalties.

No silver bullet: Developing the Canadian toolbox against foreign disinformation

Foreign interference and disinformation are widely recognized as threats to Canadian democracy. While Ottawa works to counter these threats, the Commission believes that more must be done. Bill C-70 effectively targets some interfering practices, but remains largely silent on disinformation. In seeking to strengthen democratic resilience, we have argued that Canada should integrate media and digital literacy into school curriculums and impose stronger regulations on social media platforms. These measures are not a fix-all solution: they do not address the particular experiences of Canadian diasporas, transnational repression and silencing, nor the rising use of encrypted messaging apps for political discussion. They also do not address the role of influential Canadians, including members of parliament, in the normalization of polarizing discourses. Yet, maintaining the status quo while hoping that foreign disinformation will somehow fade away is not only unrealistic; it is irresponsible. The two proposed measures would add to the existing ones by targeting two critical aspects of the disinformation process: its consumption and circulation. They also constitute areas where Canadian governments—federal, provincial, territorial, and Indigenous—have the power to intervene in practical and meaningful ways in order to create a more resilient democracy.

Acknowledgement

We want to thank the anonymous reviewers for their generous feedback and the Human-Centric Cybersecurity Partnership for its financial support.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: We acknowledge the 2023–2024 Human-Centric Cybersecurity Partnership (HC2P) mini-grant.

ORCID iDs

Simon Hogue https://orcid.org/0000-0001-5998-6765
Benjamin C.M. Fung https://orcid.org/0000-0001-8423-2906

Notes

1. Mikael Wigell, "Democratic deterrence: How to dissuade hybrid interference," *The Washington Quarterly* 44, no. 1 (2021): 49–67.
2. No relationship with author.
3. *Final Report, Volume 1: Report Summary*, Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (Ottawa, 2025), 5.
4. "Initial Report," Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (Ottawa, 2024), 150.
5. *Final Report, Volume 1*, 14.
6. Ibid., 37–39.
7. Ibid., 5
8. *First Report*, The Right Honourable David Johnston, Independent Special Rapporteur on Foreign Interference (Ottawa, 2023). For a discussion of the Johnston Report, see Simon Hogue, Magalie Lavallée, and Benjamin C. M. Fung, "L'ingérence chinoise au Canada au-delà de la myopie du Rapport Johnston: L'analyse acteur-réseau pour renforcer la résilience de la démocratie canadienne," in Jean-Vincent Holeindre and Julian Fernandez, eds, *Annuaire français de relations internationales* (Paris: Éditions Panthéon-Assas, 2024), 339–351.
9. *Final Report, Volume 1*, list of recommendations.
10. *Final Report, Volume 5*, "Chapter 19: Recommendations to better protect against foreign interference in Canada's democratic institutions and processes," Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (Ottawa, 2025), 41–47. Of the seven recommendations made to improve civic resilience, two (recommendations 47 and 49) are identified as urgent.
11. Canada, *Bill C-70: An Act Respecting Countering Foreign Interference*, 1st sess., 44th Parliament, introduced 6 May 2024, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-70/first-reading (accessed 18 June 2025).
12. *Final Report, Volume 2*, "Chapters 1–9: Context and Commission's mandate / The 2019 and 2021 general elections (Fact and Analysis)," Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (Ottawa, 2025), 144. See also Volume 4, Chapter 17, and Volume 6, Chapter 21.
13. Yasmin Dawood, "Protecting elections from disinformation: A multifaceted public-private approach to social media and democratic speech," *Ohio State Technology Law Journal* 16, no. 2 (2020): 641.

14. Government of Canada, "Canada's plan to protect democracy," 28 January 2025, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy.html (accessed 8 February 2025).
15. Government of Canada, "Protecting Canada's democratic institutions from foreign interference," 11 July 2024, https://www.canada.ca/en/democratic-institutions/news/2024/05/protecting-canadas-democratic-institutions-from-foreign-interference.html (accessed 8 February 2025).
16. Ibid.
17. Government of Canada, "Digital Citizen Contribution Program," 16 May 2024, https://www.canada.ca/en/canadian-heritage/services/online-disinformation/digital-citizen-contribution-program.html (accessed 8 February 2025)
18. Dawood, "Protecting elections from disinformation."
19. Ibid., 655.
20. Government of Canada, *Canada Declaration on Electoral Integrity Online*, 13 September 2024, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html (accessed 28 July 2025); Government of Canada, *Canada's Digital Charter*, 12 January 2021, https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world (accessed 28 July 2025)
21. Dawood, "Protecting elections from disinformation," 665.
22. Canada, *Bill C-63: An Act to Enact the Online Harms Act, to Amend the Criminal Code, the Canadian Human Rights Act and An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service and to Make Consequential and Related Amendments to Other Acts*, 1st sess., 44th Parliament, introduced 26 February 2024, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading (accessed 18 June 2025).
23. Amnesty International, "Joint letter urges justice minister to split the online harms act (Bill C-63)," 7 May 2024, https://amnesty.ca/human-rights-news/joint-letter-urges-justice-minister-to-split-the-online-harms-act-bill-c-63/ (accessed 28 July 2025)
24. Wigell, "Democratic deterrence."
25. Ibid., 63–64.
26. See Jon Bateman and Dean Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide* (Washington: Carnegie Endowment for International Peace, 2024)
27. Rubén Arcos et al., "Responses to digital disinformation as part of hybrid threats: A systematic review on the effects of disinformation and the effectiveness of fact-checking/debunking," *Open Research Europe* 2, no. 8 (2022): 1–19; Christian S.B. Overgaard et al. "Building connective democracy: Interdisciplinary solutions to the problem of polarisation," in Howard Tumber and Silvio Waisbord, eds., *The Routledge Companion to Media Disinformation and Populism* (New York: Routledge, 2021), 559–568.
28. Dawood, "Protecting elections from disinformation," 666.
29. OECD DIS/MIS Resource Hub, "Media Literacy Education System," 20 February 2023, https://oecd.org/stories/dis-misinformation-hub/webbooks/dynamic/gov-mis-information-case-studies/d067f517/pdf/media-literacy-education-system.pdf (accessed 17 June 2024); Jenny Gross, "How Finland is teaching a generation to spot misinformation," *The New York Times*, 10 January 2023, https://www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html (accessed 17 June 2024).

30. European Union, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, 27 October 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065 (accessed 28 July 2025)
31. European Union, *Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065*, 26 April 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277 (accessed 18 June 2025).
32. European Commission, "DSA: Very large online platforms and search engines," 21 February 2024, https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops (accessed 17 June 2024); European Commission, "Trusted flaggers under the Digital Services Act (DSA)," 13 June 2024, https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa (accessed 17 June 2024).
33. European Union, *Digital Services Act*, art. 52 (3)
34. Stefan D. McCabe et al., "Post-January 6th deplatforming reduced the reach of misinformation on Twitter," *Nature* 630, no. 8015 (2024): 132–140.
35. Amnesty International, "Joint letter urges justice minister to split the online harms act (Bill C-63)."

Author biographies

Simon Hogue is a professor of political science at the Université du Québec à Montréal. He is researcher-in-residence at the Observatoire des conflits multidimensionnels of the Chaire Raoul-Dandurand, and co-investigator with the Human-Centric Cybersecurity Partnership. His most recent publications focus on the use of digital technologies in the war in Ukraine and representations of algorithmic surveillance in popular culture.

Magalie Lavallée is a master's student in political science at the Université du Québec à Montréal. Her research focuses on the security dimensions of China's foreign policy, as well as regional strategic dynamics in Asia, more specifically centred on Chinese strategic thinking.

Benjamin C.M. Fung is Canada Research Chair in Data Mining for Cybersecurity, professor at McGill University's School of Information Studies (SIS), and associate editor of the Elsevier journal, *Sustainable Cities and Society* (SCS). Working closely with the national defence, law enforcement, transportation, and health sectors, he has published over 150 refereed papers covering the fields of data mining, machine learning, privacy, and cybersecurity.