The Canadian government’s response to foreign disinformation: Rhetoric, stated policy intentions, and practices

Nicole J. Jackson
School for International Studies, Simon Fraser University, Vancouver, British Columbia, Canada

Abstract
In recent years, governments have considered how to respond to “disinformation.” However, there is little academic literature on Canada’s response in the area of security and foreign policy. This paper addresses this gap by analyzing how and why Canadian government foreign and security actors have “securitized” foreign disinformation. It argues that, since 2014, they have increased awareness about disinformation and transformed it into a matter of “security” through rhetoric and discursive framing, as well as stated policy intentions and actions. This has occurred in response to perceived threats, but without coherent policy. The findings suggest that challenges are linked to persistent difficulties in defining and understanding disinformation. The result has been fragmented actions, some of which may legitimate actions that deviate from “normal political processes.” The implications are that definitional challenges need to be addressed, the role of security actors assessed, and a clearly articulated and holistic strategy drawn.

Keywords
Disinformation, security, Canadian foreign policy, information warfare, securitization, resilience, hybrid threats, foreign interference

Corresponding author:
Nicole J. Jackson, School for International Studies, Simon Fraser University, Vancouver, British Columbia V6B 5K3, Canada.
Email: nicole_jackson@sfu.ca
Disinformation\textsuperscript{1} is a complex and contentious phenomenon that has become a major challenge at multiple levels worldwide. In recent years, governments, private sector entities, and members of the public have confronted issues and controversies about whether and how to respond to it. In Canada, a complex myriad of counter-disinformation efforts has been initiated by the government, the private sector, and civil society (including the technical community, academia, and non-governmental organizations). However, there has been little academic cataloguing and analysis of all that is being done, and little debate about its merits and drawbacks.

The purpose of this paper is to provide a case study on how the Canadian government has responded to foreign disinformation nationally and internationally in security and foreign policy. In doing so, it seeks to fill a significant gap in the academic literature,\textsuperscript{2} but also to inspire and contribute to a more robust public conversation about Canada’s emerging approach and its benefits and limits. It therefore provides an analytical overview of the government’s foreign and security actors’ rhetoric, policies, and actions.

“Securitization” is used as a framework to highlight the processes and ways in which these government actors have rhetorically addressed the Canadian public and practically considered and acted upon foreign disinformation as an existential “threat” and a matter of “security.” This framework clarifies how non-military threats are brought into the domain of security policy, raising their profile in the government’s agenda, mobilizing greater attention and resources to address them.\textsuperscript{3} This may enable “extraordinary” action (breaking established rules) in the name of security.\textsuperscript{4} In contrast, when an issue is “desecuritized,” it goes off the security agenda; it may fade away or more actively be removed. It is then no longer discussed in terms of security or perceived as a threat, and new measures are not seen as necessary to address it.

This is not a theory paper. Rather, its contribution is in its empirical analysis of the Canadian government’s overall approach (rhetoric and practice) to foreign disinformation in security and foreign policy. While assessments of the effectiveness of these

\begin{itemize}
  \item Academics today commonly define disinformation as the \textit{deliberate} dissemination of \textit{intentionally} false or inaccurate information. The ambiguity and contested nature of this term are explored in the paper.
  \item Chris Tenove and Heidi Tworek, “Managing Canadian elections into the future: Online disinformation and harmful speech: Dangers for democratic participation and possible policy responses,” \textit{Journal of Parliamentary and Political Law} 13 (2019): 215–232; Alex S. Wilner, “Cybersecurity and its discontents: Artificial intelligence, the Internet of Things and digital misinformation,” \textit{International Journal} 73, no. 2 (2018): 308–316. Canadian reports (as opposed to academic journal articles) are referred to below. A case study of Canadian practices can also be found in Jean-Baptiste Jeangène Vilmer, “Effective state practices against disinformation: Four country case studies,” Hybrid CoE research report no. 2, July 2021.
  \item Ole Waever, “Securitization and desecuritization,” in Ronnie D. Lipschutz, ed., \textit{On Security} (New York: Columbia University Press, 1995), 46–86; Barry Buzan, Ole Waever, and Jaap de Wilde, \textit{Security: A New Framework for Analysis} (Boulder: Lynne Rienner Publishers, 1998); Rita Floyd, \textit{The Morality of Security: A Theory of Just Securitization} (Cambridge: Cambridge University Press, 2019); Rita Floyd, “States, last resort, and the obligation to securitize,” \textit{Polity} 51, no. 2 (2019): 378–394.
  \item Buzan et al., \textit{Security: A New Framework for Analysis}, 25; Michael C. Williams, “Words, images, enemies: Securitization and international politics,” \textit{International Studies Quarterly} 47, no. 4 (2003): 511–531.
\end{itemize}
responses, and of Canada’s responses in general to foreign and domestic disinformation, and in relation to specific theatres of disinformation are of interest, they remain outside the scope of this paper.

From the large and complex ecosystem of counter-disinformation efforts, I reviewed sources that provide a broad overview of how Canadian federal government departments and agencies which deal with foreign and security challenges have portrayed and acted upon disinformation. In specific, I examined government rhetoric through major government reports from 2014 to 2020 that were designed to raise Canadian awareness about foreign disinformation, and supplemented this with major publications on the topic by Canadian thinktanks. Sources examined for domestic policy rhetoric (intentions and plans) include Canada’s defence policy and official cyber strategy documents, and more specifically Canada’s first plan to tackle “misinformation” (presented jointly by Canada’s ministers of Democratic Institutions, of Public Safety and Emergency Preparedness, and of National Defence). Details of actions taken by the government at home and abroad were found in public statements from a wide range of security actors (sometimes working alongside other government and non-government actors) focused on securing and regulating the electoral system and on building institutional and social resilience, as well as those involved in Canada’s major foreign initiatives within North Atlantic Treaty Organization (NATO), the G7, and the United Nations. The government’s plans and attempts to regulate platforms, protect privacy, and support new digital literacy programs and other media and educational initiatives are beyond the scope of this paper, although some overlap with them (and other civilian and private actors) is acknowledged.

The year 2014 was chosen as a starting point because since Russia used hybrid tactics in its annexation of Crimea that year, there has been an increasing amount of Canadian (and other) government discussion and initiatives on organized foreign disinformation (initially Russian, but also Chinese and Iranian, among others). However, securitization was a process; it did not happen overnight nor in a vacuum: rhetoric and action evolved in reaction to external events. Although Canada itself was not a major target of sophisticated

5. These reports come from Canadian cyber and intelligence agencies including the Communications Security Establishment (CSE) (and its Cyber Centre) and the Canadian Security and Intelligence Service (CSIS), as well as Canada’s House of Commons Standing Committee on Access to Information, Privacy and Ethics; the National Security and Intelligence Committee of Parliamentarians; and the Privy Council Office (PCO). The thinktanks include Canadian International Council (CIC); Macdonald Laurier Institute; CGAI/School for Public Policy Centre for the Study of Democratic Institutions, CGAI/Alliance for Democracies; and the NATO Association of Canada, Public Policy Forum (Digital Democracy Project).
6. Royal Canadian Mounted Police (RCMP), Global Affairs Canada (GAC), CSE, CSIS. I examine Elections Canada in so far as it has worked with security actors and arguably contributed to the rhetorical securitization of the issue.
7. I illustrate with examples that come from Public Safety Canada, Department of National Defence (DND), CSIS, CSE, and the RCMP.
8. Since this paper was written, the Public Health Agency has become in charge of COVID-related disinformation.
9. Philippe Bourbeau, “Moving forward together: Logics of the securitization process,” *Millennium Journal of International Studies* 43, no. 1 (2014): 187–206.
foreign-state-sponsored disinformation, Canadian officials’ awareness of the challenge increased significantly with the investigations into electoral interferences that began most prominently with the 2016 United States presidential election and the 2016 Brexit campaign in the United Kingdom, and grew with recognition of Canadian links in the 2018 Cambridge Analytical data breach scandal. Before 2014, foreign disinformation was not widely and publicly talked of as a significant, urgent threat. Nor was it accompanied by the same exceptional or “emergency” rhetoric, and fewer government actors were addressing it. Fewer security measures were also taken to counteract it.

This paper argues that many Canadian government departments and agencies rhetorically securitized disinformation, labelling it as a significant yet ambiguous security threat that justified new practices. Within a larger global and societal context, disinformation was framed broadly as part of an ambiguous “hybrid threat,” as a danger to democracy and the so-called “international order.” Government reports raised the Canadian public’s awareness about the issue. They often used ambiguous language, conflating disinformation with misinformation, to portray a simultaneously urgent, long-term, and potential threat, often linked to other challenges or “interferences.” Policy rhetoric and intentions framed in the language of security gave security actors (but not exclusively security actors) a prominent role and new funds to tackle the broader categories of hybrid, cyber, foreign interference, and misinformation. Furthermore, in practice, an increasingly wide range of government security (and other) actors took multiple ad hoc top-down measures in the name of “securing” Canada and Canadians. On the security side, these fragmented actions at home and abroad often loosely focused on preventing malign behaviour. They were designed to strengthen electoral but also institutional and social resilience, to help collaborate, detect, and share information and develop new norms. (At the same time, government also encouraged a societal approach focused on strengthening citizens’ abilities to discern disinformation, to build democratic resilience and trust—for example, through journalism and education.)

This paper has three parts. First, it briefly addresses major difficulties and controversies over how to define and understand disinformation that have appeared in academic and policy literature post 2014 and are fundamental to understanding how the government has securitized the challenge. Second, it highlights how government rhetoric in official reports and policy intentions and plans refers to disinformation as a security challenge, or threat, to Canada and Canadians. The final section of the paper analyzes Canada’s practical securitization of disinformation based on its overt domestic and foreign security actions.

The complexity and ambiguity of disinformation that informs government rhetoric and actions

Canada’s conundrums over how to respond to disinformation are not unique. To understand how government actors have responded, it is imperative to first address major definitional

10. Less prominent was focus on the 2014 Scottish referendum. In 2018, Canada’s House of Commons Standing Committee on Access to Information, Privacy and Ethics adopted a motion to study the privacy implications of platform monopolies and possible regulatory and legislative remedies.
controversies and related complexities of disinformation. This section therefore provides a brief review of key challenges in recent academic literature that reveal unresolved debates about the definition and scope of disinformation, “unknowns” about the actors and processes involved, and difficulties in identifying its effects or consequences.

Unresolved definitional debates have informed how disinformation has been addressed in official Canadian rhetoric and policy intentions and actions. Clarifying the complexities and ambiguities of disinformation further reveals why the Canadian government has taken a variety of actions from a security approach and encountered practical difficulties. It also helps to explain the fundamental challenges behind why a more unified approach has not been taken both within Canada and in the greater ecosystem of counter-disinformation initiatives.

**Challenge 1: How to define disinformation and identify actors and processes**

The first of several challenges for governments is how to define disinformation and identify and understand the array of actors and processes that may be involved. It is obviously difficult for them to respond to something with rhetoric and action if they can’t clearly define or identify it.

Disinformation is not new, and neither is its study. Although there is a spectrum of disinformation, and specific cases have varied over time, today actors and processes appear and evolve at an unprecedented rate, some almost instantaneous and with global reach. Within this context, academics and practitioners analyze and advocate for different responses to a range of disinformation. Yet, despite a recent proliferation of studies, the scholarly definition (and identification) of disinformation remains ambiguous and controversial.

There is some academic consensus that “disinformation” is best defined as the deliberate dissemination of intentionally false or inaccurate information, as opposed to “misinformation” which is the act of spreading false information unintentionally, including when intent cannot be determined. However, the well-known difficulties in identifying “false information” and in determining whether it is deliberately or

11. There is a huge amount of recent literature on this topic. For example, Shashi Jayakumar, Benjamin Ang, Nur Diyanah Anwar, eds., *Disinformation and Fake News* (London: Palgrave Macmillan, 2021); Joshua Tucker et al., “Social media, political polarization, and political disinformation: A review of the scientific literature,” Hewlett Foundation, March 2018, [https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf](https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf) (accessed 1 September 2019); Caroline Jack, “Lexicon of lies: Terms for problematic information,” *Data and Society Research Institute*, 2017, [https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf](https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf) (accessed 1 September 2019); Dean Jackson, “Issue brief: Distinguishing disinformation from propaganda, misinformation and ‘fake news,’” National Endowment for Democracy (NED), 17 October 2017, [https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/](https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/) (accessed 2 September 2019); Alexander Lanoszka, “Disinformation in international politics,” *European Journal of International Security* 4, no. 2 (2019): 227–248; Claire Wardle and Hossein Derakhshian, “Information disorder: Toward an interdisciplinary framework for research and policy making,” Council of Europe Report, 2017; Emily K. Vraga and Leticia Bode, “Defining misinformation and understanding its bounded nature: Using expertise and evidence for describing misinformation,” *Political Communication* 37, no. 1 (2020): 136–144.
intentionally false (and to what purpose—e.g., to deceive, for economic or political gain, or to harm) continue. Determining when information moves from “persuasion” to being “deliberately manipulative” or “deceptive” is often a matter of perspective and can be difficult or impossible to prove. Deliberate incidents of disinformation, as well as more coherent and coordinated “information operations” and long-term “information campaigns,” can also involve accurate information, misinformation, disinformation, or a mix of all three. Significantly, information can also be “laundered,” hiding sources and blurring the distinction between disinformation and misinformation and between foreign and domestic. Digital disinformation exists as part of the greater media ecosystem, where false or intentionally misleading information can spread rapidly through the “interconnectedness of the internet.” In the process, it may be legitimized through a network of intermediaries that may act to distort and amplify it while concealing the original source.

Scholars (and journalists) across disciplines study and analyze a wide range of state (and state-sponsored or state-inspired) and non-state actors and their processes of manipulating and shaping public discourse in a constantly evolving process.12 Scholars of “information warfare” have tended to examine disinformation as a tool or technique used by malicious actors (e.g., Russia, China, terrorists, or extremists) to harm adversaries.13 Disinformation has also been examined as collaborative work,14 thus moving from a focus on examining “bots” and “trolls,” for example, to considering the role of (witting or unwitting) online crowds. Still other scholars emphasize the importance of the cultural context of disinformation, how forged narratives are formed and deployed,15 and how disinformation may be visually disseminated,16 “performed” or acted out—for example, by diplomats or practitioners.17

12. Samantha Bradshaw and Philip N. Howard, “Challenging truth and trust: A global inventory of organized social manipulation,” The Computational Research Project, University of Oxford, July 2018.
13. For example, Martine Moore, Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age, (London, UK: Oneworld Publications, 2018); Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, Hostile Social Manipulation: Present Realities and Emerging Trends (Santa Monica: RAND National Defense Research Institute, 2019); Mark Hazen, Anthony Isenor, Francine Desharnais, and Tania Randall, Characteristics of Information Warfare: The Battle for the Narrative, Atlantic Research Centre, Defence Research and Development Canada, November 2017.
14. Kate Starbird, Ahmer Arif, and Tom Wilson, “Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations,” 2019, http://faculty.washington.edu/kstarbi/Disinformation-as-Collaborative-Work-Authors-Version.pdf (accessed 2 October 2020).
15. For example, Oliver Schmitt, “When are strategic narratives effective? The shaping of political discourse through the interactions between political myths and strategic narratives,” Contemporary Security Policy 39, no. 4 (2018): 487–511; Alisher Faizullayev and Jérémie Cornut, “Narrative practice in international politics and diplomacy: The case of the Crimean crisis,” Journal of International Relations and Development 20, no. 3 (2016): 578–604.
16. Viorela Dan, Britt Paris, Joan Donovan, Michael Hameleers, Jon Roozenbeek, Sander van der Linden, Christian von Sikorski, “Visual mis- and disinformation, social media, and democracy,” Journalism and Mass Communications Quarterly 98, no. 3 (2021): 641–664.
17. Iver Neumann, “Returning practice to the linguistic turn: The case of diplomacy,” Millennium Journal of International Studies 31, no. 3 (2002): 627–651; James Carey, Communication as Culture: Essays on Media and Society (New York and London: Routledge, 1988).
The point here is that the definition and identification of disinformation is contested. Both what is “false” and what is intended can be difficult to identify. This complexity and uncertainty surrounding disinformation, its many actors, relationships, and processes, inform the vague language often used to discuss disinformation and the scattered nature of responses.

**Challenge 2: What is the scope of disinformation? Are other activities involved?**

The second related and as-yet unresolved question that affects government actors’ rhetoric and practice concerns the scope of disinformation. The attempt to uncover the “intent” behind disinformation has led many academics to discover a range of specific and general case-specific motivations for promoting disinformation to different groups that vary over time.\(^{18}\) To uncover specific motives requires deep knowledge of the context, the specific “theatres” of disinformation, and the disinforming actor. This is because disinformation is often a political issue dependent on the relations between the disinforming actor and its targets.

Today, many states are focused on disinformation understood as organized intent beyond deception, to inflict harm on persons or an organization or country—an understanding closer to other activities such as influence operations or foreign interference.\(^{19}\) The literature on “information warfare” stresses that disinformation is part of a broader strategy, which may include other kinds of manipulations or “interferences” (e.g. cyberattacks, leaks, and corruption). For example, Herbert Lin and Jackie Kerr package together propaganda, leaks, and chaos-producing operations which they term “information/influence warfare and manipulation.”\(^{20}\) In an even broader conceptualization, Mikael Wigell classifies disinformation along with clandestine diplomacy and geo-economics as “hybrid interference.” He plausibly hypothesizes that “hybrid interference” exploits liberal values (state restraint, pluralism, and free media) to drive wedges (or divisions) through democratic societies.\(^{21}\)

Below we will see that government rhetoric reflects the difficulty of accurately identifying underlying strategies and related activities as well as responding to them. Disinformation is often assumed to be part of a bundle of malicious tactics,

---

18. Tom Buchanan, “Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation,” PLoS ONE 15.10, 2021.
19. Wardle and Derakhshan, “Information disorder,” 18.
20. Herbert Lin and Jackie Kerr, “On cyber-enabled information/influence warfare and manipulation,” in*Oxford Handbook of Cybersecurity* (Oxford: OUP, 2021).https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680 (accessed 20 May 2020).
21. Mikael Wigell, “Hybrid interference as a wedge strategy,” *International Affairs* 95, no. 2 (2019): 255–275.
which makes causality even more difficult to determine. Yet, related activities must be clearly identified to meet the challenge of any broader strategy. And whether a strategy is understood to undermine democracy and social cohesion, for example, or to destabilize and sow confusion, different measures may be needed to counteract it.

**Challenge 3: What are the effects of disinformation?**

Finally, there are unresolved academic questions about how to discover, understand, and measure the short- and long-term effects and outcomes of disinformation that inform government language and rhetorical securitization. Some analysts highlight that disinformation is a current phenomenon, while others are more concerned about potential disinformation. The concern about possible negative consequences is not just because of the ever-evolving nature of the actors and processes of disinformation and new technology. Research also shows that the “outcomes” (results) of disinformation are case-specific and thus highly variable. They often are not discernible or immediate. For example, a RAND study from 2019 concludes that Russia has had “an effect” in terms of measurable output—e.g., we can count numbers of tweets, Facebook likes, etc. However, similar to Alexander Lanoszka, it finds that there is “almost no meaningful empirical evidence on outcomes” such as beliefs, attitudes, and behaviour.

Nevertheless, a key concern is that, in the future, disinformation could have a greater negative influence on long-term outcomes, even while it may become more difficult or impossible to detect or measure in the short or medium term. Lack of evidence of effects on outcomes is now commonly explained by findings (and speculations) that foreign actors deliberately (or unintentionally) add to emotive and issue “polarization” (by amplifying extremist or emotive narratives) and/or increase confusion or mistrust in authorities (e.g., journalists and governments). Academic literature on disinformation highlights that such aims (and outcomes) are plausible but can be difficult to prove and thus to respond to, especially when considering future hypothetical scenarios. The point here is that there are many difficulties concerning how to understand and measure current and potential effects of disinformation, which we see reflected in the depiction of disinformation as an immediate, long-term, and potential threat.

In sum, this brief review reveals that there is a complex spectrum of disinformation. There are serious challenges in defining disinformation and identifying and understanding its scope, actors, processes, and consequences. Below I show that these are

22. Lanoszka, “Disinformation in international politics.”
23. Mazarr et al., *Hostile Social Manipulations*, xiii; italics added.
24. Where no evidence can be found, it may also be that actions taken have in fact deterred.
25. Starbird et al., “Disinformation as collaborative work.”
reflected in the Canadian government’s often ambiguous rhetoric and in its scattered range of actions in security and foreign policy.

**How disinformation has been rhetorically securitized to the Canadian public through government reports and policy signalling**

My research shows that, since 2014, many actors in the Canadian government have rhetorically securitized disinformation by referring to it as an existential threat, and have broadly framed it as a threat to democracy and national security. They have done this in two major ways. First, government reports have provided specific examples of disinformation to increase public awareness. These have contributed to increasing disinformation’s profile on the government agenda and explained the need for more funds and urgent action. The language used has considered disinformation alongside other “interferences,” and portrayed it simultaneously as an urgent, protracted, and potential danger to a broad range of referent objects. Second, Canada has articulated policy rhetoric (plans and intentions) to combat broad categories of misinformation, foreign interference, hybrid threats, and cybersecurity.

*Reports warn of the dangers of disinformation: The rhetorical securitization of disinformation as an urgent, protracted, and potential “threat” which is part of broader “interference”*

Since disinformation is technically not illegal under international law, Canadian government actors tend to define it as a policy term meaning the deliberate, deceptive dissemination of false information. However, key reports that give details about foreign state disinformation often also use other terms to conceptualize the challenge, which in turn reveal the challenges and ambiguities inherent in addressing disinformation. For example, they refer to it within the wider categories of misinformation, foreign interference, hybrid warfare, and cyber activities, which are portrayed as threats to democracy and national security. The labelling of disinformation as “foreign interference” is strategic given the prohibition under international law of “interference in the internal affairs of states.” However, the practical problems of how to delineate what is foreign or domestic, and what is acceptable versus what is unacceptable action by foreign states (and their proxies), and how to respond, remain. This is particularly true when examining the role of disinformation designed to influence public debate or sentiment.

Canadian cyber and intelligence agencies were relatively quick to produce studies warning of immediate disinformation challenges and consequences to a range of “referent objects” for allies and troops abroad, as well as Canadian society, institutions, and Canadians themselves. Prominent public reports include the Communications
Security Establishment (CSE)’s 2017 Cyber Threats to Canada’s Democratic Process\textsuperscript{26} (and its 2019 update), and Canada’s Centre for Cyber Security’s National Cyber Threat Assessments from 2018 and 2020.\textsuperscript{27} The 2018 National Cyber Threat Assessment examined “disinformation” amongst other activities and concluded that Canada’s adversaries have used cyber capabilities as well as traditional and social media globally to target elections, political parties, politicians, and citizens worldwide. The year 2019 was predicted to be a particularly “perilous” year for Canadian individuals, businesses, and institutions.\textsuperscript{28} Similarly, the CSE 2019 report warned that it was “very likely” that foreign adversaries would interfere in the October election through the digital information environment.\textsuperscript{29} The Canadian Security Intelligence Service (CSIS) also published a report in 2018 looking at the security challenges of disinformation.\textsuperscript{30}

However, it is not just Canada’s cyber and intelligence security agencies that have echoed such warnings and addressed disinformation as an urgent threat (thus rhetorically securitizing disinformation). Responding to the 2018 report of a data breach involving Cambridge Analytica and Facebook, Canada’s House of Commons Standing Committee on Access to Information, Privacy and Ethics adopted a motion to study the privacy implications of platform monopolies and possible regulatory and legislative remedies. Canadian links to the scandal included Christopher Wylie, the Canadian whistleblower, and a Canadian company, AggregateIQ. Although the role of platforms and the question of privacy are outside the scope of this paper, the point here is that this parliamentary committee worked with its UK counterpart, spawning an International Grand Committee which helped Canada to position itself at the centre of a collective effort to raise awareness, and search for global solutions to protect privacy and “defend democracies from interference.”\textsuperscript{31}

The 2019 annual report of the National Security and Intelligence Committee of Parliamentarians also packaged disinformation as part of foreign interference, including flattery, bribery, threats, and manipulation, which it calls a “great threat” to Canada and its institutions.\textsuperscript{32} Major Canadian thinktank publications also warned of Russia’s (and others’) “demonstrated ability” to interfere in Canada’s October

\textsuperscript{26} CSE, Cyber Threats to Canada’s Democratic Process, 2017, https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-e.pdf (accessed 2 May 2020); CSE, Cyber Threats to Canada’s Democratic Process, Update 2019, https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e. pdf (accessed 2 May 2020).

\textsuperscript{27} Canadian Centre for Cyber Security, National Cyber Threat Assessment 2018, https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018 (accessed 2 May 2020); Canadian Centre for Cyber Security, National Cyber Threat Assessment 2020, https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf (accessed 3 February 2020).

\textsuperscript{28} National Cyber Threat Assessment 2018, 14.

\textsuperscript{29} Cyber Threats to Canada’s Democratic Process, Update 2019, 1.

\textsuperscript{30} CSIS, Who Said What? The Security Challenges of Modern Disinformation, February 2018.

\textsuperscript{31} Canada, House of Commons, Standing Committee on Access to Information, Privacy and Ethics, 42nd Parliament, 1st Session, 22 March 2018, Minutes of Proceedings.

\textsuperscript{32} National Security and Intelligence Committee of Parliamentarians, “Annual Report, 2019,” https://www.nsicop-cpsnr.ca/reports/wp-2020-03-12-ar/intro-en.html (accessed 1 March 2020).
2019 federal election, and gave recommendations for how Canada could respond.\textsuperscript{33} These documents all provide examples of Russian and/or “foreign” use of digital and other disinformation, as well as broader interference, which specifically targets, or may target, Canadian businesses, Canada’s society, individuals, and interests. The reports agree that disinformation is one of several often-interrelated actions, and that cyber is often directly or indirectly related to (or accompanied by) disinformation.

The rhetorical securitization of disinformation continued after reports later concluded that the threat of interference in the 2019 federal election was “overblown” and found no evidence of impact due to coordinated disinformation campaigns or coordinated behaviour to manipulate or interfere with the election.\textsuperscript{34} Thus, despite acknowledged methodological limitations (including data access and such a short-time period), the Digital Democracy Project research echoed other studies and found that disinformation, defined as “false information related to political issues disseminated with the intent to mislead the Canadian public, disrupt public democratic dialogue and potentially affect the outcome of the vote,” was rare, not coordinated from abroad, and had limited impact. The conclusions of an RCMP-led task force similarly reported no “observed” activities that affected Canada’s ability to have a free and fair election.\textsuperscript{35} The rhetoric securitization now focused on the negative potential of disinformation for Canada. A post-election briefing paper to the Privy Council Office (PCO) warns that “[f]oreign adversaries and competitors are increasingly targeting Canada to advance

\textsuperscript{33} Samantha Bradshaw, “Securing Canadian elections: Disinformation, computational propaganda, targeted advertising and what to expect in 2019,” Behind the Headlines (CIC) 66, no. 3 (2018); Marcus Kolga, “Stemming the virus: Understanding and responding to the threat of Russian disinformation,” Macdonald-Laurier Institute, 2019; Sergey Sukhankin, “The Western alliance in the face of Russian (dis)information machine: Where does Canada stand?,” SPP Research Paper 12, no. 26, CGAI/School for Public Policy, September 2019; Markus Kolga, Jakub Janda, and Nathalie Vogel, “Russia-proofing your elections: Global lessons for protecting Canadian democracy against foreign interference,” Macdonald-Laurier Institute, July 2019; Chris Tenove, “Digital threats to democratic elections: How foreign actors use digital techniques to undermine democracy,” Centre for the Study of Democratic Institutions, UBC, January 2018; CGAI/Alliance for Democracies, “Election risk monitor Canada,” 2019, \url{https://www.cigionline.org/publications/election-risk-monitor-canada} (accessed 22 May 2020). Also see Christian Picard, “Online disinformation threats in the 2019 Canadian federal election: Who is behind them and why?” in Joseph McQuade, ed., Disinformation and Digital Democracies in the 21st Century (NATO Association of Canada, Fall 2019), 5–30; Elizabeth Dubois and Fenwick McKelvey, “Political bots: Disrupting Canada’s democracy,” Canadian Journal of Communication Policy Portal 44, no. 2 (2019): 27–33; Edward Greenspoon and Taylor Owen, “Democracy divided: Countering disinformation and hate in the digital public sphere,” Public Policy Forum, August 2018, \url{https://ppforum.ca/publications/social-marketing-hate-speech-disinformation-democracy/} (accessed 2 July 2020).

\textsuperscript{34} Digital Democracy Project, “Lessons in resilience: Canada’s digital media ecosystem and the 2019 election,” Public Policy Forum, May 2020; Roberto Rocha, “Fears of election meddling on social media were overblown, say researchers,” CBC, 3 November 2019, \url{https://www.cbc.ca/news/canada/social-media-bots-trolls-canadian-election-2019-1.5343210} (accessed 4 May 2020).

\textsuperscript{35} Rachel Aiello, “Feds unveil plan to tackle fake news, interference in 2019 elections,” CTV News, 30 January 2019, \url{https://www.ctvnews.ca/politics/feds-unveil-plan-to-tackle-fake-news-interference-in-2019-election-1.4274273} (accessed 4 May 2020).
their own economic and national security interests,” and that “Canada, like the majority of Western democracies, is a target of foreign state efforts to interfere with or damage our democratic processes (cyber and non cyber).”

Securitizing disinformation through policy rhetoric: Stated government intentions and plans in cyber, defence, and misinformation

While the “threat” of disinformation has been addressed (in detail and through broad frames) in these reports, there is little Canadian policy that mentions disinformation. On the other hand, there are clear intentions, framed in the language of security and backed by significant new funds, to give security actors (but not only security actors) a more prominent role in responding to digital disinformation and the broader categories of hybrid threats, misinformation, and foreign interference. This can be seen in Canada’s defence policy, official cyber strategy documents (and, to a lesser extent in several non-legal documents), and in Canada’s plan to tackle misinformation and safeguard the 2019 election. This lumping together of disinformation with wider challenges reflects the uncertainty and complexity of the phenomenon which has no simple definition or solutions. It also explains the methodological difficulties in parsing out government policies, rhetoric, and actions within the complex counter-disinformation ecosystem.

Canada’s defence policy, Strong, Secure, Engaged (June 2017), directly outlined, for the first time, the challenges of detecting, attributing, and responding to the broader categories of “hybrid” threats, and allocated significant new resources to responding to cyber operations, intelligence, and information operations. The prioritization of the digital aspect of disinformation naturally occurred as part of a growing focus on cyber generally, which began as early as 2010 when Canada adopted a National Cyber Security Strategy. For example, in preparation to protect the 2019 federal election from foreign interference, Canada’s National Cyber Security Strategy 2018 strengthened security and intelligence actors by allotting an unprecedented $431 million over ten years to secure government systems, develop partnerships outside the federal government, and help Canadians be more secure online. More recently, the 2019–

36. Catharine Tunney, “Foreign enemies increasingly targeting Canada’s Privy Council warns new minister,” CBC News, 2 February 2020, https://www.cbc.ca/news/politics/foreign-interference-increasingly-targeting-canada-leblanc-warned-1.5446134 (accessed 19 May 2020); italics added.

37. Disinformation is labelled as a threat which the government should urgently tackle with a wide variety of responses. For example: the Paris Call for Trust and Security in Cyberspace (2018) agreement, with Canada taking the lead on principle 3, “to protect electoral process”; the “Christchurch Call,” which commits governments and technology companies to eliminate terrorist and violent extremist content on the internet; and Canada’s Digital Charter (May 2019) designed to build safer online spaces. In 2019, Canada also voted at both the G7 and G20 summits to adopt documents to work to counter violent propaganda and “fake news” and adopted Canada’s Declaration of Electoral Integrity Online (2019).

38. Department of National Defence, Strong, Secure, Engaged: Canada’s Defence Policy, 2017.

39. Public Safety Canada, National Cyber Security Strategy, Her Majesty the Queen in Right of Canada, 2018.
2024 National Cyber Action Plan calls for increasing the security and resilience of IT systems as well as increased research, collaboration, and international leadership on cyber security generally.\(^{40}\)

Canada’s minister of democratic institutions was eventually given the mandate to work with domestic and international partners to strengthen preparedness for, and resilience to, evolving threats to democracy and online disinformation.\(^{41}\) In January 2019, the minister of democratic institutions, along with the ministers of public safety and emergency preparedness, and national defence jointly unveiled the first “plan” to tackle misinformation and safeguard Canada’s 2019 election. The actions taken are outlined in the next section of the paper, but the plan promised to tackle the broad category of “misinformation” through four pillars: civilian preparedness, organizational readiness, combatting foreign interference, and setting expectations for social media.

Thus, on 23 April 2019, Canada’s then–minister of democratic institutions, Karina Gould, took the lead and explained that the goals were “educating Canadians on the dangers and prevalence of ‘misinformation’ online; improving organizational readiness within the government to quickly identify threats or weaknesses; combating foreign interference via Canada’s security agencies; and expecting social media platforms to increase transparency, authenticity and integrity on their systems.”\(^{42}\) A key understanding underlying the plan was that “combatting foreign interference” is a national security issue and therefore security organizations ought to be “first” among other responders (i.e., that the response should be “securitized”).

The plan included other non-security assumptions including that enhancing citizen and institutional/bureaucratic preparedness and building new expectations for social media companies are the “best defence.”\(^{43}\) This was an explicit acknowledgement of the importance of civilians and private actors in responding to disinformation, and was later followed by concrete actions. (For example, Canadian Heritage, and later others such as McGill University’s Media Ecosystem Observatory, were called upon to support digital, news, and civil literacy awareness and training, as well as broader research. Discussions between the Ministry of Democratic Institutions and social media companies resulted in the Canada Declaration on Electoral Integrity Online.) However, it remained a top-down approach to private and civil actors framed in the language of security. Overall, security issues dominated the plan, including the outlining of whom national security actors would inform of a possible threat, and how they would do so;

\(^{40}\) Public Safety Canada, *National Cyber Security Action Plan, 2019-2024*, Her Majesty the Queen in Right of Canada, 2019.

\(^{41}\) Since 2019, there has been a democratic institutions secretariat within the PCO.

\(^{42}\) James Jackson, “Minister assesses the cyber threat to Canada’s upcoming election,” *The Record*, 23 April 2019 [https://www.therecord.com/news-story/9298715-minister-assesses-the-cyber-threat-to-canada-s-upcoming-federal-election/](https://www.therecord.com/news-story/9298715-minister-assesses-the-cyber-threat-to-canada-s-upcoming-federal-election/) (accessed 4 June 2020); italics added.

\(^{43}\) “Enhancing citizen preparedness: Backgrounder,” Government of Canada website, 2019, [https://www.canada.ca/en/democratic-institutions/news/2019/01/enhancing-citizen-preparedness.html](https://www.canada.ca/en/democratic-institutions/news/2019/01/enhancing-citizen-preparedness.html) (accessed 2 June 2020). These assumptions have been acted upon, but this is beyond the scope of this paper.
how decision-makers would be informed of the risk of foreign interference by security actors; and the announcement of a new security task force to “combat” foreign interference by building awareness and preparedness.

In sum, government reports and policy rhetoric (as opposed to policy output) contributed to the rhetorical “securitization” of disinformation, which had been widely portrayed as a threat to democracy and national security. The key definitional challenges of disinformation’s scope, actors, processes, and consequences help to explain the rhetorical securitization which included ambiguous language, particularly a conflation of disinformation and misinformation, the portrayal of disinformation as linked to other “interferences,” and its depiction as an immediate, long-term, and potential threat.

**The practice of securitizing disinformation: Fragmented actions at home and abroad**

Beyond rhetoric and policy signalling, the securitization of disinformation has also occurred in practice by state-led actions at home and abroad. Overall, Canada’s security and foreign policy actors have assumed a greater role in countering disinformation than previously, working with a range of actors in a complex ecosystem of counter-disinformation efforts. Domestically, the focus is on protecting Canada’s elections and increasing “resilience.” Canadian government departments that are involved in confronting disinformation now include traditional security actors such as CSIS, the CSE, the Department of National Defence (DND), Global Affairs Canada (GAC), the PCO, the RCMP, but also Elections Canada and Heritage Canada. Foreign efforts involve Canada’s participation in wider state-led networks, most prominently with NATO, the G7, and the UN, to share information, increase collaboration, and discuss the development of possible new norms.

**Securitizing elections**

Domestically, many actions have focused on strengthening the electoral system and deterring foreign interference and breaking down bureaucratic silos. In advance of the October 2019 federal election, the government created a new RCMP-led task force, Security and Intelligence Threats to Elections (SITE), including GAC, the CSE, and CSIS, to build awareness and prepare the government to prevent and respond to “covert, clandestine or criminal attempts to interfere with the electoral process.” SITE analyzed foreign social media and coordinated responses with the G7 Rapid Response Mechanism. The government also initiated the Critical Elections Incident Public Protocol, under which five senior bureaucrats were to be informed of any potential

44. Government of Canada, “Security and Intelligence Threats to Elections (SITE) TASK FORCE,” [https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html](https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html) (accessed 14 October 2019).
interference during the 2019 federal election, in order to determine whether the incidents were serious enough to inform Canadians. (None were.) Also, the CSE and CSIS joined Elections Canada to track and analyze big data to share with other G7 members, and conducted simulations to identify vulnerabilities. Although institutional innovations that specifically focused on the 2019 elections have since been dismantled, further funds were given to the Royal Canadian Mounted Police (RCMP) Foreign Actor Interference Investigative Team to continue investigations to disrupt “interference.”

Steps have also been taken in the area of electoral regulation. In 2017, Bill C-59 was introduced to revamp Canada’s national security infrastructure and give the CSE the power to defend elections if they come under cyberattack. The bill, which received royal assent in June 2019, granted the CSE wide-ranging power to engage in “defensive cyber operations” and “active cyber operations” to “degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to Canada’s defence, security or international affairs.” In other words, for the first time, Canada could launch its own cyberattacks, an “extraordinary measure” as presented in the “securitization” framework. The threat of possible Canadian counterattacks (including against the digital information environment) is meant to deter attacks, but it is argued that Canada could also “proactively shut down the source of a possible attack against Canada.” The Elections Modernization Act (enacted in December 2019 and fully effective in June 2019) also introduced new provisions aimed at deterring or preventing “foreign interference,” although critics argue that “gaps” in the new rules remain and may be circumvented by creative actors.

45. Government of Canada, “Critical Elections Incident Protocol,” https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html (accessed 14 October 2019). Canada, House of Commons, Standing Committee on Access to Information, Privacy and Ethics: Evidence, 42nd Parliament, 1st Session, 26 February 2019, 1545, https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-138/evidence (accessed 4 February 2020).

46. Charlie Pinkerton, “Government releases blueprint for protecting election from interference,” iPolitics, 30 January 2019; Government of Canada, Democratic Institutions, “Combating foreign interference: Backgrounder,” 2019, https://www.canada.ca/en/democratic-institutions/news/2019/01/combating-foreign-interference.html (accessed 3 March 2020).

47. Government of Canada, The National Security Act 2017, https://www.canada.ca/en/services/defence/nationalsecurity/our-security-our-rights.html (accessed 2 March 2020).

48. Waever, “Securitization and desecuritization”.

49. Public Safety Canada, “New cyber security strategy bolsters cyber safety, innovation and prosperity,” June 2018, https://www.canada.ca/en/public-safety-canada/news/2018/06/new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity.html (accessed 2 August, 2019); Kolga et al., “Russia-proofing your election,” 26.

50. Anna Reepschlager and Elizabeth Dubois, “New election laws are no match for the internet,” Policy Options 2, January 2019, https://policyoptions.irpp.org/magazines/january-2019/new-election-laws-no-match-internet/ (accessed 2 May 2020).
Securitizing resilience from the top down

Beyond elections, government actors have acted to build institutional and social resilience in areas as diverse as cyber resilience, strategic communications, monitoring narratives, and public safety programs to respond to this threat. This wide range of responses once again reflects the ambiguities and complexities of disinformation explained at the beginning of this paper: the perceived urgency and protracted nature of the challenge, and the reality of constantly evolving actors and processes and their effects. It may also result from the perennial scramble for resources in the face of newly articulated threats.

To give a few examples, the DND, Public Safety, CSIS, and the CSE have continued to work to develop greater internal IT capacity and institutional resilience. The DND has worked to improve strategic communications, to identify trends in narratives which many recognize as potentially decisive factors in future conflicts, and to consider how to address emerging technologies such as “deep fakes” and increase research and awareness about these issues. Reflecting the concern that disinformation may be part of a broader phenomenon of violent transnational movements, based locally, but inspired internationally, the RCMP has been looking at how foreign actors intersect with domestic extremism. Similarly, Public Safety has explored links between communities, extremism, and disinformation.51

Collective securitization abroad: Countering disinformation as part of a network that shares information, coordinates, and develops new norms

Abroad, Canadian foreign and security actors have addressed disinformation as a security threat through a wide range of actions as part of a growing intergovernmental network, most prominently through NATO, GAC, and the UN. NATO has championed the strengthening of domestic security, but also institutional and social resilience, and taken a broad top-down governance approach as opposed to a purely military framework. To a large extent, Canada’s military and Department of Defence have mirrored that approach. NATO has encouraged allies to enhance domestic ministries of interior, to strengthen public protections to deal with “hybrid threats,” and to make ministries of defence and foreign affairs and others part of a broader “whole-of-government” effort to deter disinformation. In line with this effort, Canada’s military has engaged with its allies on “deterrence” responses ranging from electronic warfare to information warfare.52

As a NATO member, Canada also addresses disinformation through strategic communications and works with civil society to raise awareness, research, and

51. Candyce Kelshall and Victoria Dittmar, Accidental Power: How Non-State Actors Hijacked and Re-shaped the International System (Burnaby: SFU Library and CASIS, 2018).
52. Nicole J. Jackson, “Deterrence and hybrid wars: The case of Canada and NATO,” The Journal of Military and Strategic Studies 19, no. 4 (2019): 104–125.
education—for example, with the Strategic Communications Centre of Excellence in Latvia or the joint NATO-EU European Centre for Excellence for Countering Hybrid Threats. Possibly Canada’s most unified (and most effective) response was Canada’s Task Force Latvia and the local Canadian embassy’s use of public outreach efforts to counter malicious narratives that targeted Canada’s military personnel in Latvia and the merits of NATO’s involvement in the region.\(^53\)

Global affairs Canada has also addressed disinformation and related “foreign interference” through building information sharing and partnerships with the G7 and EU among others. The aim has been to position Canada at the centre of collective cyber defence by coordinating roles and sharing best practices. For example, Canada is network coordinator of the cyber Rapid Response Mechanism (RRM), created to identify and share regular reports about evolving and potential foreign threats to democracy, including disinformation, and to consider possible responses, although it has been critiqued for operating in an unclassified mode.\(^54\) The RRM leads G7 meetings on threats and practices, shares information, and attempts to coordinate a whole-of-government approach. GAC’s Centre for International Digital Policy also houses the Digital Inclusion Lab, which examines the relations between foreign policy and digital technology more widely.\(^55\)

Finally, the Canadian government has also engaged with other governments to develop international law and “big norms” to govern state behaviour in response to various activities in cyberspace, including disinformation.\(^56\) The major example is Canada’s involvement in intergovernmental negotiations at the UN, to create a new global cybersecurity architecture to protect digital information and the infrastructure on which it resides.\(^57\) These discussions have taken place in consecutive United Nations Groups of Governmental Experts (UN GGE) and more recently in the Open-ended Working Group (OEWG) processes. The 2015 UN GGE report outlined voluntary non-binding peacetime norms of state behaviour in cyberspace. The 2019 OEWG was tasked with promoting their implementation. Although the authorizing resolution of the OEWG (A/RES/73/27) directly raises the problem of disinformation as “interference”—“[r]ealising the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be

\(^{53}\) Alexander Lanoszka, Christian Leuprecht, and Alexander Moens, “Lessons from the Enhanced Forward Presence, 2017–20,” Rome, NDC Research Paper no. 14, November 2020.

\(^{54}\) G7 Rapid Response Mechanism, https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html (accessed 2 July 2020).

\(^{55}\) Howard Solomon, “Canada co-leading effort to fight election disinformation,” IT World Canada, 26 May 2020, https://www.itworldcanada.com/article/canada-co-leading-effort-to-fight-election-disinformation/431219 (accessed 3 July 2020).

\(^{56}\) As opposed to “small norms,” i.e., non-state efforts to create best practices and standards.

\(^{57}\) The subsequent General Assembly unanimously adopted a resolution that states should be guided by these norms. UN (2015) A/70/174, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accessed 2 July 2020).
interpreted as interference in the internal affairs of other States”—proceedings stalled, partly due to the growing hostility between Russia, China, and the US.

Within this UN process, Canada has provided guidance on how the agreed norms could be operationalized. The March 2021 OEWG report includes a proposal to create a permanent UN forum to consider cyber security issues which would allow the cyber conduct of states to be regularly examined and cooperative measures negotiated. Most recently, the 2021 UN GGE consensus report discusses disinformation as an “emerging threat” defined as “states’ malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another state.”58 However, it is not further mentioned in the section on international law or norms. Overall, because of definitional, legal (according to international law it cannot rise to the equivalent of an armed attack), political, and other concerns (e.g., on freedom of speech), disinformation has continued to be sidelined, or reframed as electoral interference. Thus, definitional and other persistent difficulties in countering disinformation continue to inform Canada’s domestic and international discussions.

Conclusion and discussion

To conclude, government security and foreign policy actors have rhetorically and practically securitized foreign disinformation, labelling and responding to it as a threat to democracy and national security. This paper first exposed the ambiguities and complexities that are fundamental to understanding government rhetoric. These include controversies over the definition, scope, actors, process, and effects that have shaped government rhetoric and responses. There is no one common definition of disinformation. It is multifaceted, and this helps to explain the government’s multifaceted responses. Different kinds of disinformation have been addressed with different kinds of measures. Yet the practical problems of how to identify “what is true and false,” how to delineate acceptable versus malign behaviour by foreign states (or other actors), and how to respond to them (and related concerns for freedom of speech and human rights), remain.

My research shows that government reports designed to raise awareness about disinformation have portrayed it as an urgent, persistent, and potential threat, legitimizing it as a key challenge that requires more serious responses. Government security actors (and others) have consistently portrayed disinformation as a significant yet ambiguous security challenge within the wider categories of misinformation, hybrid foreign interference, and cyber. Policy plans and intentions have given security actors (but not only security actors) more prominent roles and new funds in the name of “securing” Canada and Canadians.

In practice, there has been an increasing number of ad hoc measures taken both at home and abroad. These efforts also reflect the blurred line between domestic and

58. Paul Meyer, “The rules of war on the internet,” Open Canada, 17 February 2021, https://opencanada.org/the-rules-of-war-on-the-internet/ (accessed 19 February 2021).
foreign. The domestic focus was on elections and strengthening social and institutional “resilience.” Abroad, the focus was on developing new coalitions to share and co-ordinate information (G7), to develop new norms (UN), and to institutionalize a range of practices (NATO). Some of these may increase security actors’ power—for example, to launch preventative cyberattacks.

This securitization of disinformation, in rhetoric and in practice, is relatively new. A decade ago, there was less heightened and exceptionalist rhetoric or urgency expressed about disinformation. Few policies or actions were taken, and few funds spent, to confront it. Academic research into the process of securitization generally shows that it may be uneven, contested, and evolving over time. In this case, a period of insecurity (in which a threat is perceived, but no measures taken) was followed by a period of securitization in which the threat was widely communicated, with varying degrees of urgency, and many initiatives spawned in response. However, while the focus in this paper was on security and foreign policy actors, their actions have not always fit into neat boxes. Some have overlapped with other government, private, and civilian actors; security issues were often tied into questions of cyber, democracy, and hybrid; and even distinguishing “foreign” from “domestic” could be contentious. Nevertheless, even non security and military government actors (e.g., Elections Canada) used the language of threat and urgency, and sometimes worked with security actors in new whole-of-government efforts. And at the same time, traditional security actors (e.g., CSIS or NATO) initiated whole-of-government responses and highlighted the benefits of working with civil society actors in a wider “whole-of-society” approach.

Finally, it is apparent that there has been no clearly articulated, coherent strategic policy on foreign disinformation (or disinformation generally) that could unify security and foreign policy responses (let alone coordinate them with other government, and government-sponsored, responses not examined here—including regulation of platforms and initiatives in privacy, journalism, and public education). The result of the government’s domestic security and foreign policy efforts is continuing fragmented and overlapping actions that cause concern about federal effectiveness. This may be unsurprising in the face of disinformation’s many complexities and definitional ambiguities. Yet the challenges of how to reconcile and delineate largely state-led security responses with civil-society-led human rights efforts (focused on strengthening democratic values and countering mistrust), and private sector initiatives (in regulating platforms), remain.

This paper fills a gap in the academic literature concerning Canada’s broad and evolving approach in the areas of national security and foreign policy, including its rhetoric, policy plans, and actions. Specific responses in specific theatres of disinformation, or comparisons with the EU, or the provincial and local levels, for example, were outside the scope of this study. They could be pursued fruitfully in future research, as could an assessment of the effectiveness of Canada’s approach, and the benefits, drawbacks, unintended consequences and morality of securitizing disinformation. Another question that emerges from this review is what the role of government actors should be in relation to private (big tech) and civilians (ordinary people) within the
wider galaxy of counter-disinformation efforts. As Canada continues to discuss and develop its responses, its approach deserves further scrutiny.

Acknowledgements
I thank the anonymous referees for their helpful comments, and Paul Meyer for his review of an earlier draft.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD
Nicole J. Jackson  https://orcid.org/0000-0002-4108-2650

Author biography
Nicole J. Jackson is Associate Professor and Graduate Chair in the School for International Studies, Simon Fraser University.