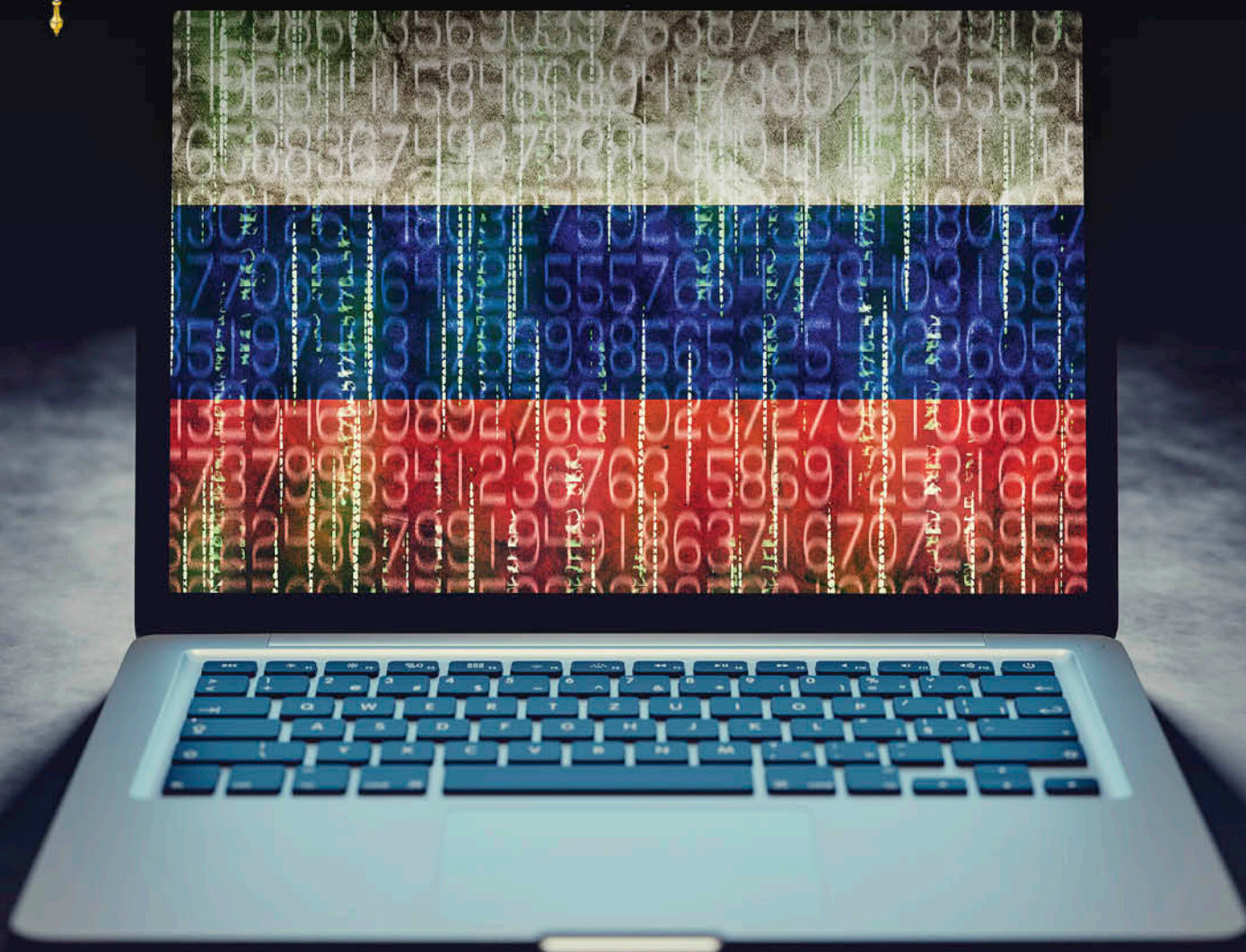




SENATE
SÉNAT
CANADA

APRIL 2026



RUSSIA'S **DISINFORMATION**

Understanding the Challenge, Strengthening Canada's Response

Report of the Standing Senate Committee
on National Security, Defence and Veterans Affairs

The Honourable Hassan Yussuff, Chair
The Honourable Mohammad Al Zaibak, Deputy Chair



For more information, please contact us by:

Email: SECD@sen.parl.gc.ca

Mail: The Standing Senate Committee on National Security, Defence and Veterans Affairs
Senate of Canada, Ottawa, Ontario, Canada, K1A 0A4

This report can be downloaded at: sencanada.ca

The Senate is on X: @SenateCA

follow the committee using the hashtag #SECD

Ce rapport est également offert en français.

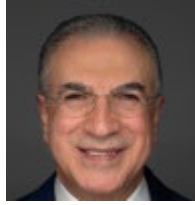
Table of Contents

The Committee Membership	2
Order of Reference	4
Executive Summary.....	6
Chapter One: The Context for Disinformation	6
Chapter Two: Russia’s Dissemination of Disinformation	6
Chapter Three: Ways to Address Russia’s Disinformation.....	7
Conclusion.....	8
List of Recommendations.....	9
Introduction	12
Chapter One: The Context for Disinformation	13
Disinformation as a public policy issue.....	13
Disinformation efforts, approaches and objectives by Russia and others.....	14
Some disinformation-related tools and platforms	15
Vulnerability to disinformation	16
Chapter Two: Russia’s Dissemination of Disinformation	17
Strategic objectives and principal “narratives”	17
Reliance on others and various tools	19
The use of disinformation against Ukraine.....	21
Disinformation targeting Canada	22
Some implications for Canada.....	23
Chapter Three: Ways to Address Russia’s Disinformation.....	25
The Government of Canada’s approach.....	25
A whole-of-society approach	28
Freedom of expression and disinformation	30
Legislative tools.....	31
Fact-checking and prebunking	33
Education	34
The Committee’s Conclusions and Recommendations	35
Appendix A – Witnesses	41
Appendix B – Documents	44

The Committee Membership



The Honourable
Hassan Yussuff
Chair



The Honourable
Mohammad Al Zaibak
Deputy Chair

The Honourable Senators



Dawn Anderson



Andrew Cardozo



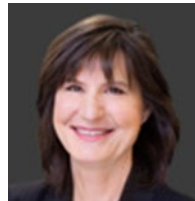
Claude Carignan, P.C..



Donna Dasko



Marty Deacon



Katherine Hay



Tony Ince



Stan Kutcher



John M. McNair



Judy A. White



Suze Youance

Ex officio members of the committee:

The Honourable Pierre Moreau, P.C., or the Honourable Patti LaBoucane-Benson
The Honourable Senator Leo Housakos or the Honourable Senator Yonah Martin
The Honourable Senator Raymonde Saint-Germain or the Honourable Senator
Bernadette Clement (until January 4, 2026)
The Honourable Senator Lucie Moncion or the Honourable Senator Joan Kingston
(since January 5, 2026)
The Honourable Senator Scott Tannas or the Honourable Senator Rebecca Patterson
(until January 4, 2026)
The Honourable Senator Flordeliz (Gigi) Osler or the Honourable Senator Robert
Black (since January 5, 2026)
The Honourable Senator Brian Francis or the Honourable Senator Judy A. White

Other senators who have participated in the study:

The Honourable Senator Gwen Boniface (retired)
The Honourable Senator Peter M. Boehm
The Honourable Senator Jean-Guy Dagenais (retired)
The Honourable Senator Tony Dean
The Honourable Senator Clément Gignac
The Honourable Senator Rebecca Patterson
The Honourable Senator David Richards (retired)
The Honourable Senator Duncan Wilson

Library and Research Services, Library of Parliament:

Ariel Shapiro, Analyst
Anne-Marie Therrien-Tremblay, Analyst

Senate Committees Directorate:

Ericka Paajanen, Committee Clerk
Debbie Larocque, Administrative Assistant

Senate Communications, Broadcasting and Publications Directorate:

Sabryna Lemieux, Communications Officer

Order of Reference

Extract from the Journals of the Senate of Thursday, February 10, 2022:

The Honourable Senator Dean moved, seconded by the Honourable Senator Dasko:

That the Standing Senate Committee on National Security and Defence be authorized to examine and report on matters relating to national defence and security generally, including veterans' affairs, as stated in rule 12-7(15); and

That the committee submit its final report no later than June 30, 2023, and that the committee retain all powers necessary to publicize its findings until 180 days after the tabling of the final report.

The question being put on the motion, it was adopted.

Interim Clerk of the Senate

Gérald Lafrenière

Extract from the Journals of the Senate of Thursday, April 27, 2023:

The Honourable Senator Dean moved, seconded by the Honourable Senator Omidvar:

That, notwithstanding the order of the Senate adopted on Thursday, February 10, 2022, the date for the final report of the Standing Senate Committee on National Security, Defence and Veterans Affairs in relation to its study on matters relating to national defence and security generally, including veterans' affairs, as stated in rule 12-7(17), be extended from June 30, 2023, to December 31, 2025.

The question being put on the motion, it was adopted.

Interim Clerk of the Senate

Gérald Lafrenière

Extract from the Journals of the Senate of Wednesday, October 8, 2025:

The Honourable Senator Yussuff moved, seconded by the Honourable Senator Kingston:

That the Standing Senate Committee on National Security, Defence and Veterans Affairs be authorized to examine and report on the impacts of Russia's disinformation on Canada;

That the papers and evidence received and taken, and the work accomplished by the committee on the topic of disinformation, in December 2024, April 2024, and May 2023 during the First Session of the Forty-fourth Parliament under its order of reference relating to national defence and security generally, including veterans affairs, be referred to the committee;

That the committee be permitted, notwithstanding usual practices, to deposit its report on this study with the Clerk of the Senate, if the Senate is not then sitting, and that the report be deemed to have been tabled in the Senate; and

That the committee submit its final report to the Senate no later than April 30, 2026, and that the committee retain all powers necessary to publicize its findings until 180 days after the tabling of the final report.

The question being put on the motion, it was adopted.

Clerk of the Senate

Shaila Anwar

Extract from the Journals of the Senate of Thursday, April 16, 2026:

The Honourable Senator Yussuff moved, seconded by the Honourable Senator Kingston:

That, notwithstanding the order of the Senate adopted on Wednesday, October 8, 2025, the date for the final report of the Standing Senate Committee on National Security, Defence and Veterans Affairs in relation to its study on the impacts of Russia's disinformation on Canada be extended from April 30, 2026, to June 30, 2026.

The question being put on the motion, it was adopted.

Clerk of the Senate

Shaila Anwar

Executive Summary

During the 44th Parliament and the 45th Parliament, the Standing Senate Committee on National Security, Defence and Veterans Affairs (the committee) held a total of five meetings to examine the impacts of Russia's disinformation on Canada. This report summarizes the witnesses' testimony on three themes: the context for disinformation; Russia's dissemination of disinformation; and ways to address Russia's disinformation.

Chapter One: The Context for Disinformation

Disinformation – the deliberate dissemination of false information – is not a new phenomenon, but its volume, its reach and the speed at which it spreads have increased significantly in recent years. As such, it is a complex and rapidly evolving challenge. Witnesses emphasized that disinformation – particularly from Russia and other hostile states – is an urgent public policy issue for Canada and other countries.

Several states produce and disseminate disinformation with differing approaches and objectives, but witnesses characterized Russia as among the most prolific states in this regard. Witnesses asserted that Russia's approach largely consists of overwhelming target populations with large quantities of disinformation, often exploiting existing societal and other divisions, in order to erode trust in information and institutions.

Artificial intelligence (AI), online platforms and social media algorithms are key enablers of disinformation, with AI increasingly used to produce fake content, including “deep fakes.” Witnesses expressed skepticism about social media platforms' effectiveness in moderating disinformation, which allows it to spread rapidly.

Several societal factors appear to make individuals and groups vulnerable to disinformation. Witnesses contended that disinformation is most effective in environments where confidence in institutions and media is weak.

Chapter Two: Russia's Dissemination of Disinformation

Russia's disinformation is part of a broad strategy designed to accomplish several objectives, such as undermining Western democracies and their support for Ukraine, and weakening the unity of the North Atlantic Treaty Organization, or NATO. Witnesses noted that, to achieve its objectives, Russia employs narratives that may be linked to existing vulnerabilities and divisions within target populations.

Disinformation is part of the hybrid tool kit that Russia uses to advance its geopolitical and military interests.

To disseminate disinformation, Russia relies on various entities and tools. Witnesses drew particular attention to state-controlled media, proxies, influencers and online platforms, emphasizing that influencers and certain media outlets help to promote narratives, and give them credibility. Witnesses held differing views about the degree of sophistication of Russia's disinformation.

Disinformation has been integral to Russia's military strategy against Ukraine. Witnesses cited several examples of Russia's disinformation narratives aimed at weakening Ukraine, which have reached populations outside of Ukraine. These narratives include portraying Ukraine as "neo-Nazi" and spreading false claims about bioweapons or nuclear risks. According to witnesses, Russia has also been using disinformation to target Ukrainian populations directly to cause confusion about its military operations.

Canadians' exposure to Russia's disinformation is significant. Witnesses identified a number of false narratives involving Canada's military and political figures, as well as specific issues that have been the focus of Russia's disinformation narratives targeting Canada, including in the context of the COVID-19 pandemic.

Although measuring the impact of disinformation is challenging, witnesses linked disinformation to polarization, violent extremism and declining support for Ukraine. In the view of witnesses, Russia's global disinformation efforts also affect Canada by destabilizing the liberal international order and undermining democracy.

Chapter Three: Ways to Address Russia's Disinformation

Multiple federal entities – including Global Affairs Canada and Rapid Response Mechanism Canada, the Canadian Centre for Cyber Security at the Communications Security Establishment, the Canadian Security Intelligence Service, the Privy Council Office and Public Safety Canada – play roles in addressing disinformation in Canada. Witnesses discussed the Government of Canada's current approach to address disinformation through these entities, the resources allocated to them, the transparency of the Government's efforts and the role of the Government in exposing disinformation.

A whole-of-society approach to addressing disinformation, with coordination among governments, communities, academic institutions, civil society organizations and the private sector, may be effective. According to witnesses, such an approach should comprise strategies that meet the particular needs of populations, including Indigenous communities and the residents of Canada's northern regions, and involve

international collaboration. Witnesses stressed the need to balance efforts in two areas – addressing disinformation and protecting the freedom of expression – and suggested that limiting certain entities’ ability to disseminate disinformation does not necessarily infringe on the freedom of expression. That said, in the view of witnesses, efforts to address disinformation must be transparent to establish and maintain trust.

Legislative tools can be central in addressing disinformation. Witnesses drew attention to several tools, such as Canada’s Foreign Influence Transparency Registry, sanctions on entities and individuals disseminating disinformation, and the regulation of online platforms that are used to disseminate disinformation.

Discussing various techniques for addressing disinformation, witnesses mentioned the effectiveness of fact-checking – the process of verifying the accuracy of information – and prebunking – the preventive process of preparing an audience before it encounters disinformation. In the opinion of witnesses, education – particularly media literacy skills and critical thinking skills – are foundational to addressing Russia’s disinformation, and the educational approach in Finland provides an example in this regard.

Conclusion

Russia’s disinformation has been growing and evolving at a rapid pace. Having heard the perspectives of Government of Canada officials, academics, journalists and representatives of civil society organizations, the committee is convinced that Russia’s disinformation poses an urgent threat to Canada’s national security, democratic institutions and social cohesion.

The Government of Canada has been making efforts to address disinformation. However, the extent of Russia’s disinformation exceeds Canada’s current capacity to address it effectively. Because disinformation affects all parts of society, addressing this threat requires a coordinated approach based on cooperation and collaboration among governments, academic institutions, civil society organizations, the private sector and international partners. To address Russia’s disinformation, Canada must act now to develop a strategic plan that leverages all available legislative, technical and policy tools, demonstrates transparency relating to the country’s responses to disinformation, and draws on best practices to improve resilience to disinformation within Canadian society.

List of Recommendations

Recommendation 1

That the Government of Canada develop, fund and implement a whole-of-government approach to address Russia's disinformation. The approach should include both a strategic plan and a requirement for an annual report to be presented in Parliament concerning the Government's disinformation-related activities and the results of the approach.

Recommendation 2

That the Government of Canada address the threats of, and responses to, Russia's disinformation in any national security strategy that is released during the 45th Parliament. In particular, the Government should ensure that any national security strategy outlines responses that are effective, comprehensive and coordinated.

Recommendation 3

That the Government of Canada enhance transparency about the nature, scope and impact of Russia's disinformation targeting Canada. In particular, the Government should consistently increase the amount of publicly available information about such disinformation, expand its activities designed to raise awareness about Russia's disinformation relating to that country's war against Ukraine, and review its practices relating to the security classification and protection of national security-related information.

Recommendation 4

That the Government of Canada, in collaboration with the Ukrainian community in Canada and civil society organizations, develop and implement measures to address Russia's disinformation aimed at reducing Canada's support for Ukraine. Entities monitoring Russia's disinformation in the context of that country's war against Ukraine should receive financial and other resources to facilitate their efforts.

Recommendation 5

That the Government of Canada lead the development of, provide funding for, and ensure the implementation of a whole-of-society approach to addressing disinformation, including from Russia. Any such approach should involve cooperation between and among the federal government and provincial, territorial, municipal and Indigenous governments, communities, academic institutions, civil society organizations and the private sector. In examining options for such an approach, consideration should be given to the elements of Finland’s model that would be appropriate for the Canadian context.

Recommendation 6

That the Government of Canada prioritize the strengthening of Global Affairs Canada’s Rapid Response Mechanism and contribute to any efforts by Group of Seven (G7) leaders to improve the G7 Rapid Response Mechanism. The Government should consider allocating additional financial, human and other resources, and should encourage other G7 governments to do the same.

Recommendation 7

That the Government of Canada establish an independent expert panel to review Canada’s approach to addressing disinformation, including in relation to online platforms and artificial intelligence.

Recommendation 8

That the Government of Canada – through its involvement in the North Atlantic Treaty Organization, the Group of Seven, the Five Eyes alliance and other international entities – take a global leadership role in publicly condemning Russia’s disinformation and contributing to efforts designed to achieve a cohesive global approach to addressing such disinformation.

Recommendation 9

That the Government of Canada, when developing Canada's approach to disinformation, address the distinct vulnerabilities of Arctic communities – including Indigenous communities – to foreign disinformation. In particular, the approach should include Arctic-specific responses.

Recommendation 10

That the Government of Canada continue to develop and implement strategies to use artificial intelligence-based tools to monitor, detect, analyze and respond to foreign disinformation. These tools should be based on responsible and ethical principles.

Introduction

Every day, millions of Canadians use the Internet to learn about world events, undertake business and other transactions, and communicate with loved ones, friends and coworkers. Some information that they see online is false, and some of that false information is disseminated deliberately by foreign state and non-state actors to accomplish certain objectives, which are often to the detriment of Canada, its allies and other partners. “Disinformation” is generally considered to be the deliberate dissemination of false information, and it differs from “misinformation,” which refers to the unintentional dissemination of such information.

A range of governmental and non-governmental sources identify Russia as among the most prolific producers and disseminators of disinformation. For example, according to Global Affairs Canada, Russia has “long spread disinformation and propaganda to achieve its objectives.”¹ The Communications Security Establishment (CSE), which characterizes Russia as a “hostile state,” notes that Russia’s dissemination of disinformation is a component of its efforts to “push beyond the boundaries of acceptable international behaviour.”² As well, according to the Canadian Security Intelligence Service (CSIS), Russia’s foreign interference activities – which include the dissemination of disinformation – “aim to disrupt and undermine Western democracies.”³

During the 44th Parliament, under its general order of reference, the Standing Senate Committee on National Security, Defence and Veterans Affairs (the committee) held three public meetings on the topic of Russia’s disinformation. In the current Parliament, the Senate adopted an order of reference authorizing the committee to “examine and report on the impacts of Russia’s disinformation on Canada,” and to consider – as part of the current study – the evidence from those three meetings.⁴ Two additional public meetings were held.

In both Parliaments, the committee’s study of Russia’s disinformation occurred at a time when disinformation and foreign interference were receiving significant attention in Canada, the country’s allies and other partners. As Russia’s war of aggression against Ukraine continues, some observers – including witnesses who appeared before the committee – are expressing alarm about Russia’s attempts to use disinformation as part of hybrid warfare operations designed to accomplish several objectives, such as: weakening Ukraine’s resolve; reducing the unity of the North Atlantic Treaty Organization (NATO) and its support for Ukraine; and

¹ Global Affairs Canada, *Countering disinformation with facts – Russian invasion of Ukraine*.

² Communications Security Establishment, *Communications Security Establishment Annual Report 2024-2025*, 27 June 2025, p. 18.

³ Canadian Security Intelligence Service, *CSIS Public Report 2024*, 18 June 2025, p. 29.

⁴ Senate, *Journals*, 8 October 2025.

undermining social cohesion in democratic countries. Furthermore, as the committee's study was under way, many countries around the world – including Canada – had national elections. As well, the increasing capabilities and widespread use of artificial intelligence (AI) provide new and expanded opportunities to produce and disseminate disinformation.

During its five meetings on the topic of Russia's disinformation, the committee heard from 27 witnesses, including Government of Canada officials, academics, journalists and representatives of civil society organizations. In this report, witnesses are identified with the professional titles that they had at the time of their appearance before the committee.

This report summarizes the witnesses' testimony on three themes: the context for disinformation; Russia's dissemination of disinformation; and ways to address Russia's disinformation. The report ends with the committee's conclusions and recommendations.

Chapter One: The Context for Disinformation

In providing a context for disinformation, which the Government of Canada defines as "false information that is deliberately intended to mislead,"⁵ witnesses' comments to the committee focused on four areas: disinformation as a public policy issue; disinformation efforts, approaches and objectives by Russia and others; some disinformation-related platforms and tools; and vulnerability to disinformation.

Disinformation as a public policy issue

Witnesses emphasized the importance of considering disinformation as a public policy issue, including for Canada. Nicole Jackson, Associate Professor at Simon Fraser University, portrayed disinformation as a "complex, rapidly evolving, transnational challenge that poses significant dilemmas for Canadian decision makers and Canadians who rely on accurate information," and – similarly – Farhaan Ladhani, Chief Executive Officer at Digital Public Square, characterized disinformation as a "complex, wicked problem."⁶ The Honourable Chris Alexander, P.C., Distinguished Fellow at the Macdonald-Laurier Institute, described disinformation – particularly from Russia – as a "core issue" for Canada.⁷ Nicole Jackson and Svitlana Matviyenko, Associate Professor at Simon Fraser

⁵ Government of Canada, [Online disinformation](#).

⁶ See SECD, [Evidence](#), 1 May 2023 (Nicole Jackson); and SECD, [Evidence](#), 1 May 2023 (Farhaan Ladhani).

⁷ SECD, [Evidence](#), 27 October 2025 (The Honourable Chris Alexander, P.C.).

University, observed that the producers of disinformation often intend to mislead public opinion or cause harm.⁸

As well, witnesses noted that the Government of Canada – and Canadians – are concerned about disinformation as a public policy issue. Officials from CSIS stated that disinformation is a “complex issue” that Canada and other countries are confronting.⁹ Francis L. Graves, President of EKOS Research Associates, asserted that Canadians are five times more likely to be concerned about disinformation than about misinformation, and added that their impacts can be similar because individuals may not know whether false information was disseminated intentionally or unintentionally.¹⁰

Disinformation efforts, approaches and objectives by Russia and others

Acknowledging that deliberately disseminating false information is not a new phenomenon, witnesses commented that the volume and reach of disinformation have markedly increased in recent years, partly due to the Internet and Russia’s full-scale invasion of Ukraine in February 2022. According to officials from CSIS, “a growing number of foreign states [are] building and deploying programs dedicated to undertaking online influence as part of their daily business,” and “Russia is chief among them.”¹¹ Edward Lucas, Senior Fellow and Senior Advisor at the Center for European Policy Analysis, underscored that the Internet “has brought an immediacy and frictionless quality to information warfare, which we didn’t have during the Cold War.”¹² As well, Nicole Jackson suggested that, since Russia’s invasion of Ukraine, “there has been a dramatic change in how information is produced, manipulated and distributed,” which has “amplified and extended the reach of mis- and disinformation.”¹³

Witnesses also discussed the speed with which disinformation spreads. Farhaan Ladhani asserted that a piece of content – including disinformation – receives half of its total number of views and other interactions within 24 to 80 minutes after being posted online.¹⁴ Jean-Christophe Boucher, Associate Professor at the University of Calgary, contended that “the first person in the information space to spread the

⁸ See SECD, [Evidence](#), 1 May 2023 (Nicole Jackson); and SECD, [Evidence](#), 15 April 2024 (Svitlana Matviyenko).

⁹ SECD, [Evidence](#), 9 December 2024 (Peter Madou).

¹⁰ SECD, [Evidence](#), 9 December 2024 (Francis L. Graves).

¹¹ SECD, [Evidence](#), 9 December 2024 (Peter Madou).

¹² SECD, [Evidence](#), 3 November 2025 (Edward Lucas).

¹³ SECD, [Evidence](#), 1 May 2023 (Nicole Jackson).

¹⁴ SECD, [Evidence](#), 1 May 2023 (Farhaan Ladhani).

message wins the information war. ... [I]t is very difficult after the fact to verify the information or change the narrative with the same momentum.”¹⁵

Recognizing that disinformation is often difficult to attribute to a particular entity, witnesses noted differences in the ways in which various states disseminate large amounts of disinformation, and their objectives in doing so. Edward Lucas and Justin Ling, who is an investigative journalist, cited a 2016 report from the RAND Corporation when referring to Russia’s approach to disinformation as a “firehose of falsehood” because the country spreads large quantities of disinformation to foreign populations.¹⁶ Officials from Public Safety Canada pointed out that China uses disinformation to “portray a positive image of itself,” particularly among diaspora communities.¹⁷ Marcus Kolga, Director of DisinfoWatch and Senior Fellow at the Macdonald-Laurier Institute, added that China and Iran primarily disseminate disinformation in those countries’ languages, which differs from Russia’s approach of disseminating disinformation in English and several other languages.¹⁸

Witnesses highlighted a particular objective for states’ dissemination of disinformation: reduce the levels of trust within target populations. According to officials from CSIS, some states disseminate disinformation to “discredit Canadian narratives and advance their own,” to “sow divisions among allies and other partners,” and to “erode Canadian values and faith in democracy.”¹⁹ Simon Hogue, Professor at the Université du Québec à Montréal, commented that the objective of disinformation is to “[tear] apart the fabric of Canadian society,” rather than to influence the outcome of a specific election.²⁰ In the view of Anthony Seaboyer, Director of the Centre for Security-Armed Forces and Society at the Royal Military College of Canada, much of the disinformation that Russia and other states disseminate is intended to overwhelm the target population with a quantity of disinformation that is sufficiently large that trust in information is generally undermined.²¹

Some disinformation-related tools and platforms

Witnesses drew attention to the role of AI, online platforms and social media algorithms in enabling the dissemination of disinformation. Officials from the Canadian Centre for Cyber Security at CSE stated that “Russia and other countries

¹⁵ SECD, [Evidence](#), 9 December 2024 (Jean-Christophe Boucher).

¹⁶ See Christopher Paul and Miriam Matthews, [The Russian “Firehose of Falsehood” Propaganda Model](#), RAND Corporation, 11 July 2016; SECD, [Evidence](#), 27 October 2025 (Justin Ling); and SECD, [Evidence](#), 3 November 2025 (Edward Lucas).

¹⁷ SECD, [Evidence](#), 9 December 2024 (Sébastien Aubertin-Giguère).

¹⁸ SECD, [Evidence](#), 9 December 2024 (Marcus Kolga).

¹⁹ SECD, [Evidence](#), 9 December 2024 (Peter Madou).

²⁰ SECD, [Evidence](#), 27 October 2025 (Simon Hogue).

²¹ SECD, [Evidence](#), 15 April 2024 (Anthony Seaboyer).

have incorporated artificial intelligence into their disinformation campaigns,” and noted that Russia uses AI to produce fake content and “deep fakes.”²² Jānis Sārts, Director of the NATO Strategic Communications Centre of Excellence, characterized AI as “the future of the information ecosystem,” adding that both Russia and China use AI to disseminate disinformation.²³ Anthony Seaboyer indicated that “AI-enabled applications are significantly enhancing the effectiveness of information attacks on democracies,” including by analyzing data and then “micro-targeting” groups of users to find the most effective message.²⁴ Marcus Kolga warned that “[d]isinformation campaigns that once took years to execute now take minutes with the help of social media, [AI] and an army of pro-Kremlin influencers.”²⁵ Cody Buntain, Assistant Professor at the University of Maryland, College Park, described the ways in which social media algorithms promote “anti-social negative messages” in a process called “algorithmic amplification,” with this process facilitating the spread of disinformation.²⁶

Regarding the role of social media platforms in enabling the dissemination of disinformation, witnesses expressed skepticism about the ability or willingness of those platforms to monitor and remove disinformation. Brian McQuinn, Assistant Professor at the University of Regina, pointed out that “[content] [m]oderation, for all intents and purposes ... simply [is not] happening.”²⁷ Cody Buntain focused on the absence of government regulation of online platforms, which facilitates the dissemination of disinformation.²⁸ Farhaan Ladhani underscored the ease with which disinformation can be disseminated and the ineffectiveness of online platforms’ moderation of content, explaining that several platforms have disbanded their “trust and safety” teams, which had been responsible for moderating content.²⁹

Vulnerability to disinformation

Witnesses discussed factors that make some societies more vulnerable than others to disinformation. Jean-Christophe Boucher described disinformation and other forms of foreign interference as “crime[s] of opportunity” that require a “suitable target.”³⁰ Pekka Kallioniemi, Non-Resident Research Fellow at the International Centre for Defence and Security in Estonia, observed that disinformation – notably

²² SECD, [Evidence](#), 9 December 2024 (Bridget Walshe).

²³ SECD, [Evidence](#), 3 November 2025 (Jānis Sārts).

²⁴ SECD, [Evidence](#), 15 April 2024 (Anthony Seaboyer).

²⁵ SECD, [Evidence](#), 15 April 2024 (Marcus Kolga).

²⁶ SECD, [Evidence](#), 1 May 2023 (Cody Buntain).

²⁷ SECD, [Evidence](#), 9 December 2024 (Brian McQuinn).

²⁸ SECD, [Evidence](#), 1 May 2023 (Cody Buntain).

²⁹ SECD, [Evidence](#), 1 May 2023 (Farhaan Ladhani).

³⁰ SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

from Russia – is most effective in “low-trust environments,” which are environments in which individuals have low levels of trust in journalists, politicians and institutions.³¹ According to Farhaan Ladhani, alongside the “supply” of disinformation, there is also a “demand” for disinformation, particularly among people “with low trust in institutions and in traditional media” or “with high levels of fear and grievance.”³²

As well, witnesses identified certain groups within Canadian society that are more vulnerable to viewing and believing disinformation than are others. In Francis L. Graves’s opinion, in Canada, young men are “four to five times” more vulnerable to disinformation than are young women.³³ Jean-Christophe Boucher mentioned Canadian survey results that found that young people, residents of rural communities and those with low levels of education have difficulties identifying disinformation, and asserted that the people who are the most vulnerable to disinformation often have “legitimate grievances.”³⁴ Anthony Seaboyer suggested that between 15% and 25% of the Canadian population “want to believe disinformation,” and Farhaan Ladhani contended that between 20% and 25% of Canadians “may have an increased vulnerability to disinformation,” including in relation to the COVID-19 pandemic and Russia’s war against Ukraine.³⁵

Chapter Two: Russia’s Dissemination of Disinformation

In their appearance before the committee, witnesses highlighted Russia’s dissemination of disinformation. In particular, their comments addressed five areas: strategic objectives and principal “narratives”; reliance on others and various tools; the use of disinformation against Ukraine; disinformation targeting Canada; and some implications for Canada.

Strategic objectives and principal “narratives”

Witnesses drew attention to Russia’s dissemination of disinformation as part of a strategy designed to accomplish several objectives. Officials from Global Affairs Canada stated that Russia uses “state-sponsored disinformation as part of a broader hybrid tool kit to achieve its geopolitical and military objectives,” adding that these

³¹ SECD, [Evidence](#), 9 December 2024 (Pekka Kallioniemi).

³² SECD, [Evidence](#), 1 May 2023 (Farhaan Ladhani).

³³ SECD, [Evidence](#), 9 December 2024 (Francis L. Graves).

³⁴ See SECD, [Evidence](#), 9 December 2024 (Jean-Christophe Boucher); and SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

³⁵ See SECD, [Evidence](#), 1 May 2023 (Farhaan Ladhani); and SECD, [Evidence](#), 15 April 2024 (Anthony Seaboyer).

objectives include “erod[ing] trust in democratic institutions and processes ... and creat[ing] and amplify[ing] divisions in our societies.”³⁶ As well, officials from Public Safety Canada noted that Russia’s main objectives include undermining both Western democracies and their support for Ukraine, as well as weakening NATO’s unity.³⁷ In the view of officials from the Canadian Centre for Cyber Security at CSE, Russia uses cyber espionage and disinformation to promote the country’s “global status and reinforce pro-Russian narratives, to erode trust in democratic institutions, [and] to generate popular support for Russia’s war efforts.”³⁸ Marcus Kolga observed that Russia’s objectives – to “distract, distort and divide democratic societies” – have been consistent for several decades.³⁹

As well, witnesses indicated that Russia’s objectives for its disinformation efforts vary across time horizons. In Jean-Christophe Boucher’s opinion, Russia’s objectives are to support its war against Ukraine in the short term and to “erode citizens’ trust in Western democratic institutions” in the medium term. According to Jean-Christophe Boucher, in the long term, Russia seeks to increase its status in the world, “redefine the distribution of power in world politics,” undermine NATO and “reclaim the place [it] lost under the Soviet Union.”⁴⁰ However, agreeing that Russia continues to use disinformation to “destabilize Western societies” in the long term, Pekka Kallioniemi emphasized that – since February 2022 – Russia’s priority with its disinformation and influence operations is to “stop any kind of military aid to Ukraine.”⁴¹

Witnesses also highlighted Russia’s approach to selecting the narratives that form the basis of its disinformation, with such narratives sometimes linked to existing vulnerabilities and divisions within target populations.⁴² Pekka Kallioniemi argued that Russia’s rationale for exploiting divisions within target populations is that “any country that is focusing on domestic disputes has, in general, a weaker foreign policy.”⁴³ Anayit Khoperiya, Deputy Head of the Center for Countering Disinformation at the National Security and Defence Council of Ukraine, explained that Russia “searches for vulnerabilities in each country – social divisions, political tensions and economic fears – and then uses those vulnerabilities against societies

³⁶ See SECD, [Evidence](#), 15 April 2024 (Tara Denham); and SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

³⁷ SECD, [Evidence](#), 9 December 2024 (Sébastien Aubertin-Giguère).

³⁸ SECD, [Evidence](#), 9 December 2024 (Bridget Walshe).

³⁹ SECD, [Evidence](#), 1 May 2023 (Marcus Kolga).

⁴⁰ SECD, [Evidence](#), 9 December 2024 (Jean-Christophe Boucher).

⁴¹ SECD, [Evidence](#), 9 December 2024 (Pekka Kallioniemi).

⁴² The European External Action Service defines a “disinformation narrative” as “an overall message, communicated through texts, images, metaphors and other means,” that is used to “foster distrust.” See European Union (EU), European External Action Service, “[5 Common Pro-Kremlin Disinformation Narratives](#),” *EUvsDisinfo*, 2 April 2019.

⁴³ SECD, [Evidence](#), 9 December 2024 (Pekka Kallioniemi).

themselves.”⁴⁴ Officials from Global Affairs Canada and Jean-Christophe Boucher commented on Russia’s “equal opportunity” approach to disinformation, noting the country’s willingness to promote whatever message – including from the far right or far left – is most likely to further its objectives.⁴⁵

Furthermore, witnesses discussed other issues, groups and regions that have been the focus of Russia’s disinformation narratives. According to officials from Global Affairs Canada, Russia promotes the narrative that its full-scale invasion of Ukraine in 2022 was a response to NATO’s “encroachments.”⁴⁶ In Jean-Christophe Boucher’s view, Russia is “promoting illiberal values, intolerance toward immigrants, racialized people, LGBTQ members, and ultimately trying to erode citizens’ trust in Western democratic institutions.”⁴⁷ Marcus Kolga mentioned Russia’s efforts to “exploit” the COVID-19 pandemic to “advance its interests” and “polarize our society,” including by promoting “anti-vaccination and anti-lockdown narratives.”⁴⁸ Chris Alexander, Pekka Kallioniemi and Justin Ling focused on Russia’s efforts to use disinformation to support pro-Russia candidates in recent elections in Moldova and Romania.⁴⁹ Additionally, Anthony Seaboyer described Russia’s disinformation targeting Germany, Justin Ling emphasized Russia’s efforts to spread disinformation narratives throughout Africa, and Chris Alexander pointed out Russia’s support for “White supremacists” and “anti-Ukrainian and anti-Semitic propaganda” in Canada.⁵⁰

Reliance on others and various tools

Witnesses mentioned that, in addition to its own efforts, Russia relies on other entities to disseminate disinformation.⁵¹ Officials from Global Affairs Canada indicated that Russia “goes to great lengths to obfuscate its involvement in the spreading of narratives or the fomenting of discord.”⁵² Farhaan Ladhani explained that, in addition to disseminating disinformation themselves, some states – such as Russia – also use other state or non-state actors, which are sometimes called “proxies,” to disseminate disinformation, with individuals then sharing that

⁴⁴ SECD, [Evidence](#), 3 November 2025 (Anayit Khoperiya).

⁴⁵ See SECD, [Evidence](#), 9 December 2024 (Jean-Christophe Boucher); and SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

⁴⁶ SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

⁴⁷ SECD, [Evidence](#), 9 December 2024 (Jean-Christophe Boucher).

⁴⁸ SECD, [Evidence](#), 1 May 2023 (Marcus Kolga).

⁴⁹ See SECD, [Evidence](#), 27 October 2025 (The Honourable Chris Alexander, P.C.); SECD, [Evidence](#), 9 December 2024 (Pekka Kallioniemi); and SECD, [Evidence](#), 27 October 2025 (Justin Ling).

⁵⁰ See SECD, [Evidence](#), 27 October 2025 (The Honourable Chris Alexander, P.C.); SECD, [Evidence](#), 27 October 2025 (Justin Ling); and SECD, [Evidence](#), 15 April 2024 (Anthony Seaboyer).

⁵¹ For an overview of the ways in which Russia disseminates disinformation, see EU, European External Action Service, [3rd EEAS Report on Foreign Information Manipulation and Interference Threats](#), March 2025.

⁵² SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

disinformation with others.⁵³ Marcus Kolga suggested that a particular false narrative might be broadcast on Russian state media before appearing on international social media platforms, with traditional media outlets in Canada then sharing the false narrative and elected officials and other policymakers then repeating it, thereby influencing public policy.⁵⁴ Brian McQuinn underlined a study's conclusion that Russia's disinformation operations rely on "average Canadians" promoting the disinformation to their social media followers.⁵⁵

As well, witnesses described some tools of Russia's disinformation. Justin Ling identified the state-owned RT (Russia Today) and Sputnik News – an international television channel and an online news service, respectively – as key tools that Russia uses to disseminate its narratives around the world.⁵⁶ According to Jean-Christophe Boucher, Telegram, TikTok, Reddit, Facebook and YouTube are tools in Russia's "information arsenal."⁵⁷ Anatoliy Gruz, Professor at Toronto Metropolitan University, asserted that Russia uses "bots, trolls, hackers and other proxies to create a more favourable environment for [its] information operation[s]."⁵⁸ Anayit Khoperiya observed that Russia's ability to use AI in its disinformation efforts has improved since 2022.⁵⁹

Moreover, witnesses focused on the role of "influencers" – including in Canada, Europe and the United States – in promoting Russia's disinformation and helping Russia reach international populations. Officials from Global Affairs Canada stated that, "whenever Russia's messages are repeated by influencers and people of authority, they take on credibility."⁶⁰ Justin Ling contended that "Western outlets that are either happy to take the propaganda or get paid for it" promote Russia's disinformation.⁶¹ Officials from Global Affairs Canada, as well as Marcus Kolga and Justin Ling, drew attention to Tenet Media, a Canadian company that the United States Department of Justice alleges had used money – possibly from Russia – to fund right-wing influencers so that they could disseminate pro-Russian disinformation.⁶² Aengus Bridgman, Assistant Professor at McGill University, elaborated that right-wing influencers in both Canada and the United States

⁵³ SECD, [Evidence](#), 1 May 2023 (Farhaan Ladhani).

⁵⁴ SECD, [Evidence](#), 15 April 2024 (Marcus Kolga).

⁵⁵ SECD, [Evidence](#), 9 December 2024 (Brian McQuinn).

⁵⁶ SECD, [Evidence](#), 27 October 2025 (Justin Ling).

⁵⁷ SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

⁵⁸ SECD, [Evidence](#), 15 April 2024 (Anatoliy Gruz).

⁵⁹ SECD, [Evidence](#), 3 November 2025 (Anayit Khoperiya).

⁶⁰ SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

⁶¹ SECD, [Evidence](#), 27 October 2025 (Justin Ling).

⁶² See SECD, [Evidence](#), 9 December 2024 (Larisa Galadza); SECD, [Evidence](#), 9 December 2024 (Marcus Kolga); and SECD, [Evidence](#), 27 October 2025 (Justin Ling).

allegedly received money from Tenet Media, and described the influencers as “useful idiots” who enabled Russia’s information operation.⁶³

Witnesses also provided their views about the sophistication of Russia’s disinformation-related efforts. Officials from Public Safety Canada portrayed those efforts as “pervasive, well funded and guided by the Kremlin ... carried out by a large, distributed network of actors across multiple jurisdictions.”⁶⁴ Pekka Kallioniemi characterized Russia’s disinformation operations as “the most effective in the world.”⁶⁵ However, Justin Ling contended that Russia’s efforts are “slapdash,” and added that the Russian government relies on “the work of oligarchs or business interests” to disseminate disinformation because it is “wildly corrupt [and] often completely incompetent.”⁶⁶

The use of disinformation against Ukraine

Witnesses commented on Russia’s use of disinformation to advance its military objectives against Ukraine, both in the lead-up to the full-scale invasion and throughout the subsequent war. Officials from the Canadian Centre for Cyber Security at CSE noted that Russia uses disinformation to support cyber and military attacks against Ukraine, and officials from Global Affairs Canada pointed out that Russia “conceals, blurs and fabricates information to gain military advantage, demoralize Ukrainians, divide allies and garner domestic and international support for its illegal invasion.”⁶⁷ Anayit Khoperiya asserted that Russia’s “[d]isinformation became an operational weapon that was launched before tanks and missiles and was used to justify aggression, divide allies and weaken public trust.”⁶⁸ Additionally, Simon Hogue emphasized that Russia’s objectives in disseminating its disinformation include “undermin[ing] Ukrainian courage and seek[ing] to have Ukraine’s defeat accepted as a fact.”⁶⁹

As well, witnesses provided specific examples of Russia’s use of disinformation against Ukraine, and the impacts of that disinformation. Nicole Jackson contended that Russia has used social media both to deny its attacks against Ukraine and to announce that it will not attack a certain area before it does so, with such disinformation “caus[ing] people to ... be completely confused.”⁷⁰ Anthony Seaboyer

⁶³ SECD, [Evidence](#), 27 October 2025 (Aengus Bridgman).

⁶⁴ SECD, [Evidence](#), 9 December 2024 (Sébastien Aubertin-Giguère).

⁶⁵ SECD, [Evidence](#), 9 December 2024 (Pekka Kallioniemi).

⁶⁶ SECD, [Evidence](#), 27 October 2025 (Justin Ling).

⁶⁷ See SECD, [Evidence](#), 15 April 2024 (Tara Denham); and SECD, [Evidence](#), 15 April 2024 (Sami Khoury).

⁶⁸ SECD, [Evidence](#), 3 November 2025 (Anayit Khoperiya).

⁶⁹ SECD, [Evidence](#), 27 October 2025 (Simon Hogue).

⁷⁰ SECD, [Evidence](#), 1 May 2023 (Nicole Jackson).

described a Russian-affiliated entity's creation of a "deep fake" that made it appear that Ukrainian President Volodymyr Zelenskyy was ordering Ukrainian troops to surrender.⁷¹ In Svitlana Matviyenko's view, due to the "scope, intensity and nature" of Russia's disinformation against Ukraine since 2022, "disinformation" may no longer be the most appropriate term.⁷² According to Svitlana Matviyenko, Russia's dissemination of disinformation to deny its attacks against Ukrainian civilians could be considered terrorism, with the goal of undermining Ukrainians' "human dignity" and "their ability to resist the aggressor."⁷³

Witnesses outlined Russia's disinformation narratives aimed at weakening and discrediting Ukraine to populations around the world. Officials from Global Affairs Canada emphasized that, before the February 2022 invasion, Russia disseminated a narrative about "Ukraine being overrun by Nazis."⁷⁴ Moreover, the officials stated that, after the invasion, Russia disseminated disinformation that blamed Ukraine for a worldwide shortage of wheat, when – in reality – Russia was blockading wheat shipments and had attacked Ukrainian farms and infrastructure.⁷⁵ In Marcus Kolga's opinion, among the most prominent of Russia's disinformation narratives is the claim that the Ukrainian government is "neo-Nazi," which it uses to "justify the war and to attack the credibility of Ukraine's government."⁷⁶ Justin Ling discussed Russia's dissemination of disinformation relating to "bioweapons" in Ukraine, and Svitlana Matviyenko noted that Russia uses disinformation to exploit fears relating to the use of nuclear weapons or the possibility of accidents at nuclear power plants.⁷⁷

Disinformation targeting Canada

Witnesses provided observations about Russia's dissemination of disinformation targeting Canada. According to Anatoliy Gruzd, 51% of Canadians have been exposed to "pro-Kremlin information," with 30% of Canadians believing Russia's narrative that the "Ukrainian nationalism movement is neo-Nazi."⁷⁸ Portraying Russia's dissemination of disinformation targeting Canada as "strategic," Jean-Christophe Boucher argued that Russia has a "clear understanding of Canadian audiences, in fact, probably better than the Canadian government itself," and added that Russia's disinformation primarily targets both the far right and the far left in

⁷¹ SECD, [Evidence](#), 15 April 2024 (Anthony Seaboyer).

⁷² SECD, [Evidence](#), 15 April 2024 (Svitlana Matviyenko).

⁷³ Ibid.

⁷⁴ SECD, [Evidence](#), 15 April 2024 (Tara Denham).

⁷⁵ Ibid.

⁷⁶ SECD, [Evidence](#), 1 May 2023 (Marcus Kolga).

⁷⁷ See SECD, [Evidence](#), 27 October 2025 (Justin Ling); and SECD, [Evidence](#), 15 April 2024 (Svitlana Matviyenko).

⁷⁸ SECD, [Evidence](#), 15 April 2024 (Anatoliy Gruzd).

Canada, and includes messaging in English and in French.⁷⁹ According to Jean-Christophe Boucher, Russia's disinformation seems to be more present in the far right information ecosystem, partly because this ecosystem is "starting to converge" with that in the United States.⁸⁰ Brian McQuinn asserted that Russia's disinformation targeting Canada increased "fourfold" in the three months prior to Russia's invasion of Ukraine.⁸¹

As well, witnesses indicated that some of Russia's disinformation involves Canada's military and political figures. Officials from the Canadian Centre for Cyber Security at CSE stated that, with the goal of providing the false impression that Canadian military members were fighting against Russia and committing war crimes, Russian-controlled media "have been ordered to include doctored images of members of the Canadian Armed Forces deployed on the front line" in Ukraine.⁸² In Marcus Kolga's view, during the COVID-19 pandemic, "Russian state media in Latvia tried to promote a story about [the Canadian Armed Forces] spreading COVID in Latvia to try to erode Latvian support for the mission."⁸³ As well, Nicole Jackson and Justin Ling referred to Russia's disinformation that focused on the Honourable Chrystia Freeland, P.C., former Deputy Prime Minister of Canada.⁸⁴

Some implications for Canada

Witnesses pointed out that the effectiveness of disinformation – targeting Canada or other countries – often cannot be completely evaluated. Officials from Global Affairs Canada stressed that it is difficult to measure the impact of disinformation.⁸⁵ Similarly, Anthony Seaboyer contended that "[w]e cannot effectively measure behavioural change based on disinformation," and explained that researchers can observe the number of times that narratives are viewed and shared, but they cannot measure the extent to which an individual "actually changes ... behaviour" as a consequence.⁸⁶ Aengus Bridgman suggested that data are limited concerning the effectiveness of Russia's disinformation-related interference in Canada, noting that it is "incredibly challenging for any citizen, parliamentarian or policy-maker to look at the information ecosystem and understand what's going on."⁸⁷ However, Aengus

⁷⁹ SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

⁸⁰ SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

⁸¹ SECD, [Evidence](#), 1 May 2023 (Brian McQuinn).

⁸² SECD, [Evidence](#), 15 April 2024 (Sami Khoury).

⁸³ SECD, [Evidence](#), 1 May 2023 (Marcus Kolga). Members of the Canadian Armed Forces are deployed to Latvia in support of the North Atlantic Treaty Organization's deterrence and defence measures. See Department of National Defence, [Operation REASSURANCE](#).

⁸⁴ See SECD, [Evidence](#), 1 May 2023 (Nicole Jackson); and SECD, [Evidence](#), 27 October 2025 (Justin Ling).

⁸⁵ SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

⁸⁶ SECD, [Evidence](#), 15 April 2024 (Anthony Seaboyer).

⁸⁷ SECD, [Evidence](#), 27 October 2025 (Aengus Bridgman).

Bridgman added that Canada is affected even when only a small number of Canadians view and believe Russia's disinformation.⁸⁸

That said, witnesses identified several consequences of disinformation, including that which Russia disseminates in relation to Canada. Officials from CSIS linked disinformation to a rise in violent extremism, including among youth, and Farhaad Ladhani drew attention to disinformation's "destabilizing effect on social cohesion."⁸⁹ In Brian McQuinn's opinion, one consequence is polarization, which is "the goal of many foreign influence operations."⁹⁰ Francis L. Graves asserted that the high levels of polarization within Canada are "connected directly to disinformation, which is now being wielded as a tool of statecraft and being amplified and reinforced in North America," adding that – in some cases – disinformation can affect people's "issue preference" and "partisan choices" during elections.⁹¹

Witnesses discussed the impacts of Russia's disinformation on support for Ukraine within Canada. Francis L. Graves highlighted that, because of disinformation, "[t]he incidence of people who have negative views on Ukraine and our involvement in NATO is still a minority but it's growing."⁹² Marcus Kolga pointed to a growing number of incidents of violence against Ukrainian, Central European and Eastern European communities in Canada resulting from Russia's "hate-based disinformation,"⁹³ and observed that – partly due to disinformation – there was an increase in the number of Canadians who "believed that Canada is giving too much to Ukraine."⁹⁴

As well, witnesses underscored that Russia's disinformation that targets other countries has impacts on Canada. Justin Ling argued that Canada is affected by such disinformation because "the more Russia can use propaganda and disinformation to finance its war machine, undermine democracy abroad and recruit new allies for its illiberal bloc, the more hostile and unsafe the world becomes."⁹⁵ Simon Hogue stated that Russia's disinformation targeting Europe or the United States "is also threatening Canadian interests" because the disinformation threatens the "liberal international order."⁹⁶ Moreover, in Justin Ling's view, Russia's extensive

⁸⁸ Ibid.

⁸⁹ See SECD, [Evidence](#), 1 May 2023 (Farhaan Ladhani); and SECD, [Evidence](#), 9 December 2024 (Peter Madou).

⁹⁰ SECD, [Evidence](#), 1 May 2023 (Brian McQuinn).

⁹¹ See SECD, [Evidence](#), 9 December 2024 (Francis L. Graves).

⁹² SECD, [Evidence](#), 9 December 2024 (Francis L. Graves).

⁹³ SECD, [Evidence](#), 1 May 2023 (Marcus Kolga).

⁹⁴ SECD, [Evidence](#), 15 April 2024 (Marcus Kolga).

⁹⁵ SECD, [Evidence](#), 27 October 2025 (Justin Ling).

⁹⁶ SECD, [Evidence](#), 27 October 2025 (Simon Hogue).

disinformation operations in Africa “could easily be replicated to target Canada.”⁹⁷ Aengus Bridgman emphasized the “interdependence” between Canada and the United States, and suggested that pro-Russia disinformation targeting – or emanating from – the United States affects Canada.⁹⁸

Witnesses commented that Russia has succeeded in accomplishing some of its disinformation-related objectives. Cody Buntain noted that, regardless of the effectiveness of specific pieces of disinformation in changing individual behaviour, Russia’s disinformation has been successful overall because the country has been able to spread the narrative that it can influence foreign populations, including in Canada.⁹⁹ In Brian McQuinn’s opinion, Russia’s significant financial investments in disseminating disinformation is evidence that the country believes that its disinformation – including that which targets Canada – is effective, “otherwise, [it] wouldn’t be doing it at the scale [that it is].”¹⁰⁰ Marcus Kolga asserted that some of Russia’s disinformation “appear[s] to be working,” constituting an “attack” on Canada’s “cognitive sovereignty.”¹⁰¹

Chapter Three: Ways to Address Russia’s Disinformation

When speaking to the committee about ways to address Russia’s disinformation, witnesses commented on the Government of Canada’s approach and the merits of a whole-of-society approach, as well as the balance between a government’s efforts to address disinformation and respect for the freedom of expression. As well, they discussed tools that can be used to address disinformation, noting legislative measures, efforts to fact-check and prebunk, and education.

The Government of Canada’s approach

Witnesses pointed out that a number of federal entities play a role in addressing disinformation in Canada, including – but not limited to – Global Affairs Canada, CSE, CSIS, the Privy Council Office and Public Safety Canada. Officials from Global Affairs Canada underlined their own disinformation-related efforts and the advice offered to other federal entities regarding the impacts of, and any responses to, disinformation. Providing an example, the officials said that Global Affairs Canada has publicly denounced Russia’s disinformation through producing video exposés,

⁹⁷ SECD, [Evidence](#), 27 October 2025 (Justin Ling).

⁹⁸ SECD, [Evidence](#), 27 October 2025 (Aengus Bridgman).

⁹⁹ SECD, [Evidence](#), 1 May 2023 (Cody Buntain).

¹⁰⁰ SECD, [Evidence](#), 1 May 2023 (Brian McQuinn).

¹⁰¹ SECD, [Evidence](#), 9 December 2024 (Marcus Kolga).

publishing fact-based content, condemning media outlets like RT – now “an arm of Russian intelligence” – and exposing “the Kremlin’s funding of firms like the Social Design Agency and Structura.”¹⁰²

As well, officials from Global Affairs Canada drew attention to Rapid Response Mechanism Canada, which is “housed” within Global Affairs Canada and serves as the secretariat for the Group of Seven (G7) Rapid Response Mechanism (RRM). The officials mentioned that the RRM uses open-source data to “detect, correct and call out the Kremlin’s malign activities.”¹⁰³ According to Marcus Kolga, Global Affairs Canada and the RRM have become “extraordinarily effective and courageous in calling out Russian disinformation narratives, explaining them and breaking them down for Canadians so they become digestible.”¹⁰⁴ Anthony Seaboyer advocated “far more funding” for the RRM.¹⁰⁵

Officials from the Canadian Centre for Cyber Security at CSE stated that the Canadian Centre for Cyber Security – which focuses on intelligence, cyber security and support for defence and national security – is responsible for collecting foreign intelligence relating to Russia’s disinformation. The officials indicated that the Centre has “monitored for malicious Russian cyber activity against Canada, Ukraine and NATO [and has] shared cyber-threat information with key partners,” including with the other Five Eyes countries.¹⁰⁶

Furthermore, officials from CSIS explained that CSIS investigates disinformation when it meets the legal threshold of “foreign interference,” which is outlined in the *Canadian Security Intelligence Service Act*.¹⁰⁷ The officials added that, although most of CSIS’s work – such as investigations and briefings provided to federal entities – involves classified information, CSIS shares unclassified information with other levels of government, academics and various groups.¹⁰⁸ The officials stressed that, ultimately, resilience to disinformation depends on public trust in authoritative sources, and highlighted that the “best way to counter disinformation is to have ... trusted sources of information, the government included.”

¹⁰² See SECD, [Evidence](#), 9 December 2024 (Tara Denham); and SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

¹⁰³ SECD, [Evidence](#), 9 December 2024 (Larisa Galadza).

¹⁰⁴ SECD, [Evidence](#), 9 December 2024 (Marcus Kolga).

¹⁰⁵ SECD, [Evidence](#), 15 April 2024 (Anthony Seaboyer).

¹⁰⁶ SECD, [Evidence](#), 15 April 2024 (Sami Khoury).

¹⁰⁷ SECD, [Evidence](#), 9 December 2024 (Peter Madou). Section 2(b) of the *Canadian Security Intelligence Service Act* defines the term “foreign interference” as “foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person.”

¹⁰⁸ SECD, [Evidence](#), 9 December 2024 (Peter Madou).

Officials from the Privy Council Office underlined that the Democratic Institutions secretariat within the Privy Council Office has a “policy development” role. As well, the officials said that, in 2022, the Government of Canada established the Protecting Democracy Unit within the Privy Council Office “to coordinate, develop and implement government-wide measures designed to combat disinformation and protect democracy.”¹⁰⁹

Moreover, officials from Public Safety Canada characterized Public Safety Canada as a “policy-coordination department.”¹¹⁰ The officials noted that Public Safety Canada “work[s] with other partners in Canada to come up with responses, good policies and legislation to combat any national security issue.” The officials particularly mentioned foreign interference.¹¹¹

Witnesses questioned the effectiveness of the Government of Canada’s approach to addressing disinformation, including that which Russia disseminates. In Jean-Christophe Boucher’s view, federal public servants do not have the tools or financial resources needed to address disinformation, indicating that Russia spends \$3 billion or \$4 billion annually to disseminate disinformation and Canada spends \$20 million or \$30 million yearly to address it.¹¹² Nicole Jackson supported current federal efforts to raise awareness about misinformation and disinformation, urged the Government “to articulate a balanced, responsible and transparent approach,” and proposed that new national defence and security policy updates should address foreign misinformation and disinformation “holistically.”¹¹³

Furthermore, witnesses contrasted the Government of Canada’s approach to addressing disinformation with the more centralized approaches in other countries. Officials from the Privy Council Office, Chris Alexander, Jean-Christophe Boucher and Marcus Kolga provided examples of government entities that address disinformation, such as Sweden’s Psychological Defence Agency, France’s VIGINUM and the European Union’s EUvsDisinfo, as well as government-funded initiatives, such as Australia’s Strategic Policy Institute.¹¹⁴ Drawing on Ukraine’s experience, Anayit Khoperiya suggested that efforts to address disinformation should not be “fragmented across ministries or left to reactive initiatives.”¹¹⁵ Aaron Erlich, Associate Professor at McGill University, underlined that many Eastern European

¹⁰⁹ SECD, [Evidence](#), 9 December 2024 (Sarah Stinson).

¹¹⁰ SECD, [Evidence](#), 9 December 2024 (Sébastien Aubertin-Giguère).

¹¹¹ Ibid.

¹¹² SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

¹¹³ SECD, [Evidence](#), 1 May 2023 (Nicole Jackson).

¹¹⁴ See SECD, [Evidence](#), 27 October 2025 (The Honourable Chris Alexander, P.C.); SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher); SECD, [Evidence](#), 15 April 2024 (Marcus Kolga); and SECD, [Evidence](#), 9 December 2024 (Sarah Stinson).

¹¹⁵ SECD, [Evidence](#), 3 November 2025 (Anayit Khoperiya).

countries have created ministries or subministries dedicated to addressing disinformation.¹¹⁶

Witnesses advocated greater transparency concerning the Government of Canada's efforts to address disinformation. Simon Hogue contended that "Canada needs to be much more transparent when it comes to all defence security issues, including disinformation."¹¹⁷ Similarly, Justin Ling argued that there is "no reason" that would justify the Government's decision not to "disclose and attribute" disinformation, and indicated that the current approach to addressing disinformation mirrors the way in which the Government conducts national security investigations.¹¹⁸ Focusing on Ukraine, Anayit Khoperiya asserted both that transparency builds trust and that "[c]itizens are more resilient when governments communicate clearly and openly."¹¹⁹

Furthermore, witnesses commented on the limits of the Government of Canada's role in addressing disinformation. Officials from Global Affairs Canada acknowledged that the Government should not "say what is truthful or not," but recognized that the Government should provide information about the ways in which it responds to disinformation.¹²⁰ The officials underscored that "no government can tackle [disinformation] alone, so [it is] important to work with civil society and academia."¹²¹

A whole-of-society approach

Witnesses called for an approach to addressing disinformation that relies on coordination among governments, communities, academic institutions, civil society organizations and the private sector. Officials from the Privy Council Office said that "protecting democracy requires a government-wide whole-of-society approach," and highlighted the Privy Council Office's coordination with other federal entities, provincial, territorial and municipal governments, civil society organizations and academics to address disinformation.¹²² Supporting such an approach, Nicole Jackson stated that disinformation "poses a transnational set of challenges that demands holistic responses" both internationally and "domestically with provincial governments, civil society and private actors across all of Canada."¹²³ Simon Hogue emphasized that even "the best institutional coordination" is insufficient to address

¹¹⁶ SECD, [Evidence](#), 15 April 2024 (Aaron Erlich).

¹¹⁷ SECD, [Evidence](#), 27 October 2025 (Simon Hogue).

¹¹⁸ SECD, [Evidence](#), 27 October 2025 (Justin Ling).

¹¹⁹ SECD, [Evidence](#), 3 November 2025 (Anayit Khoperiya).

¹²⁰ SECD, [Evidence](#), 15 April 2024 (Tara Denham).

¹²¹ Ibid.

¹²² SECD, [Evidence](#), 9 December 2024 (Sarah Stinson).

¹²³ SECD, [Evidence](#), 1 May 2023 (Nicole Jackson).

disinformation and protect democracy because “[t]he problem is societal and requires a societal response.”¹²⁴

Moreover, witnesses proposed that a whole-of-society approach to addressing disinformation should consider the needs of particular regions, communities and groups. Officials from Global Affairs Canada noted that *Canada’s Arctic Foreign Policy*¹²⁵ “recognizes the vulnerability to disinformation in the North,” highlighting Russia’s “narrative ... of a hostile, unfriendly West, used in part to justify militarization of the Arctic.”¹²⁶ Furthermore, officials from the Canadian Centre for Cyber Security at CSE indicated that, although the Canadian Centre for Cyber Security works with all provincial and territorial governments, information sharing with Canada’s northern governments is “prioritize[d].”¹²⁷ Nicole Jackson pointed out Indigenous-specific vulnerabilities to disinformation, and stressed that approaches to addressing disinformation must be “specifically designed to engage Indigenous communities.”¹²⁸ Aaron Erlich encouraged the allocation of more resources for non-governmental organizations to help them “target hard-to-reach populations” with their efforts to address disinformation.¹²⁹

Witnesses suggested that a whole-of-society approach to addressing disinformation may increase trust in the responses to disinformation. Nicole Jackson urged the creation of “an interdisciplinary whole-of-society hub for discussion, research and policy ... to develop trust between society and government and a culture of national security resilience.”¹³⁰ Advocating collaboration between the Government of Canada and non-governmental entities to address disinformation, Farhaan Ladhani asserted both that “a single person, individual or institution [cannot] be the arbiter of truth,” and that the Government should be “a party to the conversation with other actors.”¹³¹

Furthermore, witnesses described Taiwan’s approach to addressing disinformation, which involves whole-of-society coordination among the government, civil society organizations and online platforms.¹³² Farhaan Ladhani explained that, in Taiwan,

¹²⁴ SECD, *Evidence*, 27 October 2025 (Simon Hogue).

¹²⁵ Global Affairs Canada, *Canada’s Arctic Foreign Policy*, December 2024.

¹²⁶ SECD, *Evidence*, 9 December 2024 (Larisa Galadza).

¹²⁷ SECD, *Evidence*, 9 December 2024 (Bridget Walshe).

¹²⁸ SECD, *Evidence*, 1 May 2023 (Nicole Jackson).

¹²⁹ SECD, *Evidence*, 15 April 2024 (Aaron Erlich).

¹³⁰ SECD, *Evidence*, 1 May 2023 (Nicole Jackson).

¹³¹ SECD, *Evidence*, 1 May 2023 (Farhaan Ladhani).

¹³² Taiwan addresses disinformation in four ways: identifying disinformation through media literacy, fact-checking disinformation through cooperation with civil society organizations, combating the dissemination of disinformation through online platforms’ regulation of content, and punishing perpetrators of disinformation. See Government of Taiwan, Executive Yuan, *Anti-Disinformation Policy Overview*, 2019.

civil society organizations monitor disinformation and alert the government and online platforms, as required. As well, Farhaan Ladhani added that the online platforms then reduce the visibility of the identified disinformation, and the government may respond by “‘prebunking’ narratives within an hour of being alerted” about the disinformation.¹³³

Moreover, witnesses identified coordination with international partners – including through NATO – as an essential part of a whole-of-society approach to addressing disinformation. In Anayit Khoperiya’s opinion, because “Russia’s narratives adapt across languages and platforms,” international coordination is central in “exposing” those narratives.¹³⁴ Jānis Sārts emphasized NATO’s growing role in addressing Russia’s disinformation, indicating that NATO increased the resources dedicated to “developing capabilities in this area.”¹³⁵ Pekka Kallioniemi agreed that NATO’s collaboration in addressing disinformation is “very crucial.”¹³⁶

Freedom of expression and disinformation

Witnesses discussed the balance between efforts in two areas: protecting the freedom of expression and addressing disinformation. Nicole Jackson argued that the Government of Canada should not be “policing speech,” and advocated collaboration among diverse entities to build trust in efforts designed to address disinformation.¹³⁷ Aengus Bridgman highlighted the role of online platforms in disseminating disinformation, observing that “any demanding of transparency, accountability and adjustment of platforms is seen as an infringement on freedom of speech ... [but] these platforms are not neutral actors.”¹³⁸

As well, when urging Canada to defend democratic principles vigorously, witnesses suggested that limiting certain entities’ ability to disseminate disinformation does not necessarily infringe on the freedom of expression. Marcus Kolga proposed that such countries as China, Iran and Russia should be “blocked” from Canada’s information environment “whenever possible,” and contended that protecting the freedom of expression does not preclude the Government of Canada from taking actions to address disinformation.¹³⁹ Jean-Christophe Boucher commented that

¹³³ Ibid.

¹³⁴ SECD, [Evidence](#), 3 November 2025 (Anayit Khoperiya).

¹³⁵ SECD, [Evidence](#), 3 November 2025 (Jānis Sārts).

¹³⁶ SECD, [Evidence](#), 9 December 2024 (Pekka Kallioniemi).

¹³⁷ SECD, [Evidence](#), 1 May 2023 (Nicole Jackson).

¹³⁸ SECD, [Evidence](#), 27 October 2025 (Aengus Bridgman).

¹³⁹ SECD, [Evidence](#), 15 April 2024 (Marcus Kolga).

Canada has become “gun-shy” about defending its values, and asserted that “there is a difference between censoring someone and defending your own values.”¹⁴⁰

Witnesses also provided their views about the effectiveness and risks of banning Russian state-controlled media from operating in certain countries. Nicole Jackson noted that the Government of Canada has imposed sanctions targeting Russian state-controlled media, and cautioned that the Government should be transparent when adopting a media ban, “otherwise it will continue to increase mistrust.”¹⁴¹ Acknowledging the existence of concerns about undermining the freedom of expression, Aaron Erlich cited research that concluded that banning Russian state-controlled television in Ukraine “has reduced support for [Russian President Vladimir] Putin and pro-Russian positions.”¹⁴²

Legislative tools

Witnesses described statutory tools that could help address disinformation. Officials from Public Safety Canada explained that the *Foreign Influence Transparency and Accountability Act* both created “a registration obligation for individuals acting on behalf of foreign principals” and introduced criminal offences for interference in Canadian politics.¹⁴³ Marcus Kolga encouraged “proper implementation” of the statute and the associated Foreign Influence Transparency Registry.¹⁴⁴ Officials from CSIS drew attention to Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts,¹⁴⁵ which would have established cyber security standards for critical sectors with the goal of strengthening Canada’s resilience against hybrid threats, including disinformation.¹⁴⁶

Moreover, witnesses pointed out that Canada’s sanctions regime allows the Government of Canada to impose sanctions on entities and individuals disseminating disinformation.¹⁴⁷ Officials from Global Affairs Canada said that

¹⁴⁰ SECD, [Evidence](#), 9 December 2024 (Jean-Christophe Boucher).

¹⁴¹ SECD, [Evidence](#), 1 May 2023 (Nicole Jackson).

¹⁴² SECD, [Evidence](#), 15 April 2024 (Aaron Erlich).

¹⁴³ SECD, [Evidence](#), 9 December 2024 (Sébastien Aubertin-Giguère). See [Foreign Influence Transparency and Accountability Act](#), S.C. 2024, c. 16, s. 113.

¹⁴⁴ SECD, [Evidence](#), 9 December 2024 (Marcus Kolga).

¹⁴⁵ [Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts](#), 44th Parliament, 1st Session.

¹⁴⁶ SECD, [Evidence](#), 15 April 2024 (Sami Khoury). Bill C-26 died on the Order Paper when the federal general election was called for 6 January 2025. On 18 June 2025, the bill was reintroduced as [Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts](#), in the 45th Parliament, 1st Session.

¹⁴⁷ The Government of Canada imposes sanctions through the regulatory authority granted by three statutes: the *United Nations Act*; the *Special Economic Measures Act*; and the *Justice for Victims of*

“Canada has applied sanctions to target entities and individuals involved in Russian disinformation operations” in the context of Russia’s war against Ukraine.¹⁴⁸ The officials stressed the need for coordination with allies and other partners when imposing sanctions, and indicated that “the power and potential impact of sanctions are increased when multiple countries impose them on the same individuals.”¹⁴⁹ Commenting on sanctions targeting Russian state-controlled media, Anatoliy Gruzd asserted that banning media like RT is only partially effective because Russia “circumvents such sanctions by copying content and disseminating it through other channels.”¹⁵⁰

Witnesses also discussed various jurisdictions’ regulation of online platforms that are used to disseminate disinformation, including the approach in the European Union. Simon Hogue and Marcus Kolga suggested that Canada should consider the European Union’s *Digital Services Act*,¹⁵¹ and Farhaan Ladhani cited this statute as “one example of how governments are aiming to impose compliance and regulatory standards that are intended to promote safer online spaces.”¹⁵² However, Jānis Sārts cautioned against adopting an inflexible regulatory approach, and characterized the European Union’s statute as “a very extensive regulatory framework [that] stamps out innovation.”¹⁵³

Furthermore, witnesses provided their views about other possible requirements and ways to regulate online platforms. In Aengus Bridgman’s opinion, Canada has been “a laggard” in establishing transparency and accountability requirements for online platforms.¹⁵⁴ Edward Lucas supported an “active policy to protect [Canada’s] information system,” instead of an approach that would “rely on free speech [and] on the free market” to address Russia’s disinformation.¹⁵⁵ Suggesting that the focus should be regulating the amplification and monetization of disinformation rather than regulating speech, Jean-Christophe Boucher advocated mandatory transparency regarding the funding provided to influencers who profit from

Corrupt Foreign Officials Act (Sergei Magnitsky Law). The Governor in Council’s regulations made under these statutes outline prohibitions and restrictions in relation to individuals and entities in Canada, as well as Canadian citizens overseas. See Global Affairs Canada, [*Current sanctions imposed by Canada*](#).

¹⁴⁸ SECD, [*Evidence*](#), 15 April 2024 (Tara Denham).

¹⁴⁹ *Ibid.*

¹⁵⁰ SECD, [*Evidence*](#), 15 April 2024 (Anatoliy Gruzd).

¹⁵¹ See SECD, [*Evidence*](#), 27 October 2025 (Simon Hogue); and SECD, [*Evidence*](#), 15 April 2024 (Marcus Kolga). The European Union’s *Digital Services Act* establishes responsibilities for online services, including online platforms. It entered into force in November 2022. See Tambiama Madiaga, European Parliamentary Research Service, [*Digital services act*](#), Briefing, 17 November 2022.

¹⁵² SECD, [*Evidence*](#), 1 May 2023 (Farhaan Ladhani).

¹⁵³ SECD, [*Evidence*](#), 3 November 2025 (Jānis Sārts).

¹⁵⁴ SECD, [*Evidence*](#), 27 October 2025 (Aengus Bridgman).

¹⁵⁵ SECD, [*Evidence*](#), 3 November 2025 (Edward Lucas).

disseminating disinformation.¹⁵⁶ Brian McQuinn called for a requirement for online platforms to provide researchers with access to data, warning that platforms' refusal to share data is preventing researchers from monitoring disinformation networks.¹⁵⁷

Fact-checking and prebunking

Witnesses provided their views about the effectiveness of fact-checking – the process of verifying the accuracy of information – to address disinformation.¹⁵⁸ Cody Buntain contended that fact-checking alone is not “particularly useful at changing people’s beliefs,” adding that it does “suppress some [sharing of incorrect information], but [does not] change the underlying mindset that leads to that sharing.”¹⁵⁹ Jean-Christophe Boucher agreed that “fact checking actually doesn’t work. ... If we think it works, it actually makes other people more entrenched in their views.”¹⁶⁰

That said, witnesses also stressed that fact-checking can reduce the impacts of disinformation, especially when it occurs on a large scale and with the support of online platforms. Anatoliy Gruzd recalled that, during the COVID-19 pandemic, “labelling and fact checking ... were implemented across many platforms” and YouTube “demonetized” anti-vaccine videos, which reduced exposure to such videos.¹⁶¹ Marcus Kolga underscored that fact-checking undertaken by entities that monitor disinformation, such as DisinfoWatch, can be “useful” to journalists.¹⁶²

Witnesses characterized prebunking – the process of preparing members of an “audience before they encounter disinformation by providing accurate information, evidence or context” – as more effective than fact-checking in relation to Russia’s disinformation.¹⁶³ Anatoliy Gruzd proposed the development of “proactive or prebunking strategies,” including public service announcements and educational games that incorporate known false information, that could reduce the effectiveness of disinformation.¹⁶⁴ Jean-Christophe Boucher outlined three types of information required for effective prebunking: the message to convey, such as why

¹⁵⁶ SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

¹⁵⁷ SECD, [Evidence](#), 9 December 2024 (Brian McQuinn).

¹⁵⁸ The process of debunking – “explicitly expos[ing] false information to make the facts clear” – often overlaps with the process of fact-checking. The two terms are sometimes used interchangeably. See Government of Canada, “[Debunking](#),” *Countering Disinformation: A Guidebook for Public Servants*, 2024.

¹⁵⁹ SECD, [Evidence](#), 1 May 2023 (Cody Buntain).

¹⁶⁰ SECD, [Evidence](#), 15 April 2024 (Jean-Christophe Boucher).

¹⁶¹ SECD, [Evidence](#), 15 April 2024 (Anatoliy Gruzd).

¹⁶² SECD, [Evidence](#), 15 April 2024 (Marcus Kolga).

¹⁶³ Government of Canada, “[Share accurate information with your audience ahead of time \(pre-bunking\)](#),” *Countering Disinformation: A Guidebook for Public Servants*, 2024.

¹⁶⁴ SECD, [Evidence](#), 15 April 2024 (Anatoliy Gruzd).

defending Ukraine aligns with Canada’s democratic values; insights into the targets of the disinformation, such as which online platforms they use and which media they consult; and an understanding of the targets’ concerns and the best methods for communicating with them, such as their main grievances.¹⁶⁵

Education

Witnesses described education as foundational to addressing Russia’s disinformation. Nicole Jackson emphasized that education that provides Canadians with the knowledge to understand “dangerous narratives” and the historical context in which they arise is essential for building resilience against such disinformation.¹⁶⁶ Svitlana Matviyenko illustrated the need for such context by explaining that, notwithstanding the prevalence of strong fact-checking skills among Ukrainians, Russia’s disinformation often appeals to emotions, and a broad understanding of context is needed to expose it effectively.¹⁶⁷

As well, witnesses commented on particular areas where education is needed to address disinformation, including media literacy skills and critical thinking skills. Officials from the Privy Council Office noted that media literacy is “one of the best defences” against disinformation.¹⁶⁸ Aaron Erlich underscored the existence of “good evidence” indicating that improving such skills and “reminding individuals to think critically about media” lead people to reduce their belief in disinformation and “does not harm trust in stories that are verifiably true.”¹⁶⁹ That said, Anatoliy Gruzd was concerned that an approach with media literacy skills and critical thinking skills at its core gives rise to the risk of putting “all responsibilities on individual users.”¹⁷⁰

Witnesses called for the integration of media literacy skills and critical thinking skills into academic curricula, from elementary school to postsecondary education. Chris Alexander urged Canada to “invest heavily in media literacy ... taught in schools.”¹⁷¹ Similarly, referencing the experiences of other NATO countries, Jānis Sārts supported the integration of media literacy skills into academic curricula, and Aaron Erlich pointed out Ukraine’s success in embedding critical thinking skills into such curricula, which helps Ukrainians identify Russia’s disinformation.¹⁷² Brian McQuinn

¹⁶⁵ SECD, [Evidence](#), 9 December 2024 (Jean-Christophe Boucher).

¹⁶⁶ SECD, [Evidence](#), 1 May 2023 (Nicole Jackson).

¹⁶⁷ SECD, [Evidence](#), 15 April 2024 (Svitlana Matviyenko).

¹⁶⁸ SECD, [Evidence](#), 9 December 2024 (Sarah Stinson).

¹⁶⁹ SECD, [Evidence](#), 15 April 2024 (Aaron Erlich).

¹⁷⁰ SECD, [Evidence](#), 15 April 2024 (Anatoliy Gruzd).

¹⁷¹ SECD, [Evidence](#), 27 October 2025 (The Honourable Chris Alexander, P.C.).

¹⁷² SECD, [Evidence](#), 15 April 2024 (Aaron Erlich); and SECD, [Evidence](#), 3 November 2025 (Jānis Sārts).

underscored the urgency of integrating critical thinking skills into educational systems, warning that Canadian universities often overlook these skills.¹⁷³

Drawing attention to successful educational models that help to address disinformation, witnesses highlighted Finland's approach of building resilience against Russia's disinformation.¹⁷⁴ Pekka Kallioniemi explained that, "[f]rom as early as preschool, Finnish children are taught through stories to critically analyze and evaluate information," and Marcus Kolga said that the Finnish model embeds digital media literacy skills and critical thinking skills into a range of academic courses.¹⁷⁵ Similarly, Edward Lucas noted Finland's success with embedding "information resilience" in academic curricula with the goal of "teaching kids about disinformation almost before [they have] learned to read and write properly."¹⁷⁶ However, Aaron Erlich cautioned that "what works [in Finland] might not" be effective in Canada, and suggested that Canada should study a variety of models before choosing an approach that is suitable for the Canadian context.¹⁷⁷

The Committee's Conclusions and Recommendations

Russia's disinformation is thought to be part of a deliberate strategy to undermine democratic institutions and increase social divisions in Canada and other democratic countries. Russia is known to use online platforms, such as social media, and other technologies, such as AI-based tools and bot farms, to disseminate false narratives rapidly and pervasively. The committee is troubled by Russia's disinformation, the associated impacts on Canada and its residents, and the reality that Canada's efforts are insufficient to address that disinformation. False content permeates Canada's information environment, and Russia and its proxies are producing and disseminating some of this content to destabilize Canadian society, reduce the country's support for Ukraine and weaken the bonds of NATO.

The modern information environment is complex, and vast quantities of content are produced every day. Although attempting to assess the nature and scope of Russia's disinformation with accuracy is difficult, the committee is convinced that Russia's

¹⁷³ SECD, [Evidence](#), 9 December 2024 (Brian McQuinn).

¹⁷⁴ Finland's media literacy policy outlines the objectives of a comprehensive, high-quality and systematic media literacy approach, covering all types of media and integrating media literacy across all levels of education. See Finland, Ministry of Education and Culture, [Media Literacy in Finland: National media education policy](#), 2019.

¹⁷⁵ SECD, [Evidence](#), 9 December 2024 (Pekka Kallioniemi); and SECD, [Evidence](#), 9 December 2024 (Marcus Kolga).

¹⁷⁶ SECD, [Evidence](#), 3 November 2025 (Edward Lucas).

¹⁷⁷ SECD, [Evidence](#), 15 April 2024 (Aaron Erlich).

disinformation is having significant negative effects on Canadian society, such as through contributing to polarization and distrust in governments and their institutions. Russia's disinformation poses significant threats to Canada that must be addressed immediately.

Many federal entities play a critical role in safeguarding Canada, Canadians and the country's democracy against disinformation. The committee acknowledges these entities' vital efforts and specifically notes Canada's leadership role in hosting the secretariat of the G7 RRM within Global Affairs Canada. However, the Government of Canada's current approach to addressing disinformation lacks coordination among federal entities and fails to provide a strategic plan to address Russia's disinformation. Canada would benefit greatly from the development and implementation of a coordinated approach to addressing disinformation.

Furthermore, Russia's disinformation targeting countries throughout the world – including Ukraine – threatens Canada's national security. Recognizing that the Government of Canada has made a commitment to publish a national security strategy every four years,¹⁷⁸ the committee feels that the next national security strategy must address the urgent threats that Russia's disinformation poses for Canada. Ideally, an accurate assessment of those threats would guide the development of a comprehensive and coordinated response to disinformation.

Enhanced transparency and the timely communication of accurate information contribute to improved resilience to disinformation, increased trust in governments, and strengthened democracies and democratic institutions. The committee believes that greater transparency about the Government of Canada's responses to disinformation, as well as better communication with the public about Russia's disinformation, are urgently needed. Because one of the main objectives of Russia's disinformation is to undermine the support that Canada and other Western democracies provide to Ukraine, including public support for military assistance, further efforts are needed to raise awareness about Russia's disinformation relating to that country's war against Ukraine.

Addressing disinformation effectively requires a whole-of-society approach comprising federal, provincial, territorial, municipal and Indigenous governments, as well as communities, academic institutions, civil society organizations and the private sector, including online platforms. The committee is certain that such an approach would enhance trust in the Government of Canada's response to disinformation. As well, greater information sharing among entities that monitor disinformation can significantly enhance efforts to address it.

¹⁷⁸ Department of National Defence, "[A Strategic Approach to National Security](#)," in *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, 2024.

Unlike civil society organizations in Finland, Taiwan and Ukraine, such organizations in Canada are not sufficiently involved in the country's approach to addressing disinformation, and they should play a larger role in monitoring and countering Russia's disinformation. The committee observes that online platforms seem to lack the willingness and ability to monitor and remove disinformation and believes that limiting certain entities' ability to disseminate disinformation does not necessarily infringe on freedom of expression. However, protecting freedom of expression should be central in any approach to regulating online platforms.

Moreover, because disinformation spreads across national borders, international cooperation and collaboration – including through the G7 and NATO – are required to achieve meaningful and durable results in addressing disinformation in Canada. The committee feels that joint international efforts are especially important when imposing sanctions against entities and individuals disseminating disinformation. They are also vital when designing regulatory frameworks for the online platforms that enable disinformation to be disseminated quickly and widely.

Canada's approach to addressing disinformation should consider the needs of specific regions, communities and groups, including northern and Indigenous communities. The committee is deeply concerned about Russia's disinformation narratives targeting the Canadian Arctic, which are often used to justify the militarization of the Russian Arctic. The Government of Canada should pay special attention to Russia's disinformation about the Arctic, monitor the nature and extent of this disinformation, and consider the particular needs of the Arctic and northern communities when developing responses to disinformation.

Finland's educational model, of which media literacy skills and critical thinking skills are key components, is thought to be effective in addressing disinformation. The committee is confident that enhancing skills in these areas – such as by embedding them in academic curricula – would not only improve the Canadian society's resilience to disinformation but would also contribute to the health of Canada's democracy. When combined with such other tools as fact-checking, debunking, prebunking, and the responsible and ethical use of AI-based tools, efforts in relation to education could be particularly important as disinformation grows and evolves.

Finally, disinformation is an ever-changing issue, with the objectives of the countries and entities that produce it evolving over time, and the scale, speed and methods used to disseminate it also changing. The committee notes that disinformation, its impacts on Canada and the most appropriate responses to it are areas that require additional study. In addition to Russia, other entities, some of which are identified in this report, also disseminate disinformation with the intent of causing harm. The risks posed by such disinformation – for Canadian society and the health of our democracy – demand our prompt attention.

In light of the foregoing, the committee recommends:

Recommendation 1

That the Government of Canada develop, fund and implement a whole-of-government approach to address Russia's disinformation. The approach should include both a strategic plan and a requirement for an annual report to be presented in Parliament concerning the Government's disinformation-related activities and the results of the approach.

Recommendation 2

That the Government of Canada address the threats of, and responses to, Russia's disinformation in any national security strategy that is released during the 45th Parliament. In particular, the Government should ensure that any national security strategy outlines responses that are effective, comprehensive and coordinated.

Recommendation 3

That the Government of Canada enhance transparency about the nature, scope and impact of Russia's disinformation targeting Canada. In particular, the Government should consistently increase the amount of publicly available information about such disinformation, expand its activities designed to raise awareness about Russia's disinformation relating to that country's war against Ukraine, and review its practices relating to the security classification and protection of national security-related information.

Recommendation 4

That the Government of Canada, in collaboration with the Ukrainian community in Canada and civil society organizations, develop and implement measures to address Russia's disinformation aimed at reducing Canada's support for Ukraine. Entities monitoring Russia's disinformation in the context of that country's war against Ukraine should receive financial and other resources to facilitate their efforts.

Recommendation 5

That the Government of Canada lead the development of, provide funding for, and ensure the implementation of a whole-of-society approach to addressing disinformation, including from Russia. Any such approach should involve

cooperation between and among the federal government and provincial, territorial, municipal and Indigenous governments, communities, academic institutions, civil society organizations and the private sector. In examining options for such an approach, consideration should be given to the elements of Finland's model that would be appropriate for the Canadian context.

Recommendation 6

That the Government of Canada prioritize the strengthening of Global Affairs Canada's Rapid Response Mechanism and contribute to any efforts by Group of Seven (G7) leaders to improve the G7 Rapid Response Mechanism. The Government should consider allocating additional financial, human and other resources, and should encourage other G7 governments to do the same.

Recommendation 7

That the Government of Canada establish an independent expert panel to review Canada's approach to addressing disinformation, including in relation to online platforms and artificial intelligence.

Recommendation 8

That the Government of Canada – through its involvement in the North Atlantic Treaty Organization, the Group of Seven, the Five Eyes alliance and other international entities – take a global leadership role in publicly condemning Russia's disinformation and contributing to efforts designed to achieve a cohesive global approach to addressing such disinformation.

Recommendation 9

That the Government of Canada, when developing Canada's approach to disinformation, address the distinct vulnerabilities of Arctic communities – including Indigenous communities – to foreign disinformation. In particular, the approach should include Arctic-specific responses.

Recommendation 10

That the Government of Canada continue to develop and implement strategies to use artificial intelligence-based tools to monitor, detect, analyze and respond to foreign disinformation. These tools should be based on responsible and ethical principles.

Appendix A – Witnesses

Monday, May 1, 2023

Farhaan Ladhani, Chief Executive Officer, Digital Public Square

Nicole Jackson, Associate Professor, School for International Studies, Simon Fraser University

Marcus Kolga, Director, DisinfoWatch, and Senior Fellow, Macdonald-Laurier Institute

Brian McQuinn, Assistant Professor, Co-Director, Centre for Artificial Intelligence, Data, and Conflict, University of Regina

Cody Buntain, Assistant Professor, College of Information Studies, College Park, University of Maryland

Monday, April 15, 2024

Tara Denham, Director General, Office of Human Rights, Freedoms and Inclusion

Kelly Anderson, Director, International Cyber Policy, Global Affairs Canada

Sami Khoury, Head, Canadian Centre for Cyber Security, Communications Security Establishment

Anthony Seaboyer, Director, Centre for Security-Armed Forces and Society, Royal Military College of Canada

Svitlana Matviyenko, Associate Professor, Critical Media Analysis, School of Communication, Simon Fraser University

Aaron Erlich, Associate Professor, Department of Political Science, McGill University

Jean-Christophe Boucher, Associate Professor, School of Public Policy, University of Calgary

Anatoliy Gruzdt, Professor and Co-Director, Social Media Lab, Toronto Metropolitan University

Marcus Kolga, Director, DisinfoWatch and Senior Fellow, Macdonald-Laurier Institute

Monday, December 9, 2024

Sébastien Aubertin-Giguère, Associate Assistant Deputy Minister, National Security and Cyber Security, Public Safety Canada

Bridget Walshe, Associate Head, Canadian Centre for Cyber Security, Communications Security Establishment Canada

Peter Madou, Assistant Deputy Minister, Operational Intelligence and Assessment Requirements, Canadian Security Intelligence Service

Larisa Galadza, Director General, Cyber, Critical Technology and Democratic Resilience Bureau, Global Affairs Canada

Sarah Stinson, Director of Operations, Democratic Institutions, Privy Council Office

Francis L. Graves, President, EKOS Research Associates Inc.

Jean-Christophe Boucher, Associate Professor, School of Public Policy, University of Calgary

Pekka Kallioniemi, Non-Resident Research Fellow, International Centre for Defence and Security

Marcus Kolga, Director, DisinfoWatch and Senior Fellow, Macdonald-Laurier Institute

Brian McQuinn, Co-Director, Centre for Artificial Intelligence, Data, and Conflict and Associate Professor, Department of Politics and International Studies, University of Regina

Monday, October 27, 2025

The Honourable Chris Alexander, P.C., Distinguished Fellow, Macdonald-Laurier Institute

Justin Ling, Investigative journalist

Simon Hogue, Professor, World politics of digital technologies, Department of Political Science, Université du Québec à Montréal

Aengus Bridgman, Director, Media Ecosystem Observatory and Assistant Professor (Research), Max Bell School of Public Policy, McGill University

Monday, November 3, 2025

Janis Sārts, Director, NATO Strategic Communications Centre of Excellence

Edward Lucas, Senior Fellow and Senior Advisor, Center for European Policy Analysis

Anayit Khoperiya, Deputy Head, Center for Countering Disinformation, National Security and Defence Council of Ukraine

Appendix B – Documents

The committee received the following documents:

Written response from the Communications Security Establishment
(March 20, 2023)

Written response from the Communications Security Establishment
(April 15, 2024)



sencanada.ca

