Co-funded by
the European Union

KONRAD
ADENAUER
STIFTUNG

Countering Foreign Information Manipulation and Interference

Lessons from the 2024 European Elections

Aengus Bridgman
Ferdinand Gehringer
Taylor Owen
Alexander Romanishyn

This report was co-funded by the European Union, through the EU-Canada Policy Dialogues Support Facility, and Konrad Adenauer Stiftung. The content of this publication does not reflect the official opinion of the European Union and Konrad Adenauer Stiftung. Responsibility for the information and views expressed therein lies entirely with the author(s).

Executive Summary

This report, "Countering Foreign Information Manipulation and Interference – Lessons from the 2024 European Elections" assesses responses to foreign information manipulation and interference (FIMI) in the European Union (EU) and Canada. It highlights regulatory frameworks, best practices, and challenges to countering these threats, and offers valuable lessons for Canadian policymakers.

Key Findings:

1. **EU's Approach to FIMI**:
    - The EU has adopted numerous measures, including the Digital Services Act and the strengthened Code of Practice on Disinformation, to address FIMI.
    - Initiatives like EUvsDisinfo, European Digital Media Observatory (EDMO), and the Early Warning System offer examples of the benefits of coordinated, multi-stakeholder strategies.
    - The EU approach and response demonstrate the importance of regulatory frameworks, fact-checking infrastructure, and public awareness campaigns for mitigating the negative impacts of FIMI.
2. **Canadian Context**:
    - Canada faces significant and increasing threats from FIMI, particularly from China, Russia, India, and Iran.
    - Specific vulnerabilities include the exploitation of diaspora communities, digital infrastructure weaknesses, and a fragmented policy and political landscape.
    - Emerging tactics, such as generative AI, diaspora population targeting, and influencer-driven campaigns, pose evolving challenges.
3. **Comparative Insights**:
    - While Canada and the EU share common threats, Canada's responses are constrained by underdeveloped national frameworks and limited resources.
    - Lessons from the EU emphasize the need for continuous, long-term strategies, international collaboration, and adequate resourcing.
4. **Policy Recommendations**:
    - **Coordination**: Establish a national task force for FIMI detection and response while cultivating strong international partnerships.
    - **Research**: Develop a national observatory to monitor disinformation and support a scaled FIMI incident response protocol.
    - **Policy**: Expedite online harms legislation and adopt measures inspired by the EU's Code of Practice.
    - **Public Education**: Invest in media and information literacy programs to bolster societal resilience.

The report underscores the critical need for Canada to bolster its defences against FIMI. Drawing on the EU's successful strategies, Canada should implement a comprehensive, coordinated approach to safeguard its democratic processes. This includes enhanced regulation, cross-sector collaboration, and public engagement to mitigate the risks posed by FIMI.

Table of Contents

1 Introduction

This report, "Countering Foreign Information Manipulation and Interference – Lessons from the 2024 European Elections," aims to enhance the understanding of foreign information manipulation and interference (FIMI) threats to democracy, focusing on lessons that Canada can draw from the European Union's experiences. The purpose of the report is to help Canadian policymakers, civil society, and the media better understand and respond to the risks posed by foreign actors.

The report begins by examining the European Union's approach to countering FIMI. It highlights regulatory frameworks such as the Digital Services Act, the self-regulatory Code of Practice on Disinformation, and initiatives like the European External Action Service (EEAS) flagship EUvsDisinfo project. These coordinated efforts were implemented ahead of the 2024 European elections and offer insights into how disinformation and election interference can be addressed. The EU's experience provides examples of how regulatory measures, public awareness campaigns, and institutional coordination can strengthen democratic processes against FIMI.

The report then shifts focus to the Canadian context, beginning with a brief overview of the past two elections and the unique challenges faced in Canada. It highlights the heightened concern among Canadians regarding influence from China, Russia, India, and Iran, particularly through disinformation campaigns and influence over diaspora communities. The discussion then examines the key pathways for FIMI within Canada, reflecting tactics observed in Europe and emphasizing the global nature of FIMI threats. The section concludes with an overview of initiatives undertaken by Canadian institutions to prepare for, defend against, and mitigate FIMI.

In both the EU and Canada, FIMI activities represent coordinated attempts to undermine democratic processes, disrupt public trust, and exploit digital platforms. The report highlights parallels between the European and Canadian experiences, emphasizing how the lessons learned from the EU's robust responses can be applied to the Canadian context.

The final sections of the report offer actionable recommendations for Canada, informed by both EU and domestic experiences. These include stronger coordination between Canadian governmental institutions, improved media and information literacy, and a more robust monitoring and response infrastructure. The dual focus helps policymakers draw lessons from the 2024 European elections that are directly relevant to Canada and supports Canadian efforts to protect its democracy from similar foreign interference. The report concludes by stressing the critical need for Canada to bolster its defences against FIMI, drawing on the EU's successful strategies as a guide.

2 FIMI Threat Perception in Europe

The European Union faces significant threats from foreign information manipulation and interference, primarily orchestrated by state actors such as Russia and China. These threats aim to undermine public trust in democratic institutions, exacerbate polarisation and division within the EU, and impede the implementation of political measures both domestically and internationally. Additionally, FIMI often accompanies cyberattacks and other hybrid threats, further complicating the information environment. In conflict-prone regions, such manipulative activities can escalate political violence, thereby undermining EU and international peacekeeping efforts.

In recent years, the significant impact of digital platforms and social media on political discourse and voter behaviour has been underscored by the outcomes of major elections worldwide. 2024 has been a pivotal year for democracy, with elections in over 60 countries, whose combined GDP accounts for more than 50% of the global total, including more than 10 European nations. The challenges posed by politically driven disinformation are more pressing than ever, particularly in the context of the European Parliament elections.

FIMI attacks are global, with 49% of the cases detected and analyzed by the European External Action Service (EEAS) in their second FIMI threat report targeting countries or their representatives. Among the FIMI cases analyzed, in 2023, Ukraine was the most affected, with 160 incidents, followed by the USA (58), Poland (33), Germany (31), France (25), and Serbia (23). In total, 53 different countries were targeted. Additionally, 30% of cases were directed at 149 organizations, including the EU (19%), NATO (15%), and media outlets such as Euronews, Reuters, and Deutsche Welle.[1]

Among the FIMI cases analyzed, state-driven FIMI also targeted 59 individuals in 171 cases, with Ukrainian President Volodymyr Zelenskyy being the most frequent target, accounting for 40% of these cases. Other notable figures targeted included Josep Borrell, Ursula von der Leyen, and Emmanuel Macron, while celebrities like Elijah Wood and Margot Robbie were also impersonated in FIMI incidents. Gender-based and anti-LGBTIQ+ FIMI attacks were recorded, highlighting a troubling trend. In 2023, the European External Action Service (EEAS) began systematically coding FIMI incidents linked to specific events, with 160 cases tied to 94 events, such as political summits, elections, and crises like the Hamas attack on Israel and the coup in Niger.[2]

FIMI content is disseminated via social channels, with approximately 4,000 different channels identified. The most frequently used platforms were Telegram (496 instances) and X (formerly Twitter, 452 cases), along with Facebook, VKontakte, YouTube, and others.[3]

2.1 *Broader Structural Challenges*

Most of the negative externalities arising from the platform internet, including increased vulnerability to foreign interference, are not merely the result of individual bad actors but are instead embedded in the design of the digital infrastructure itself. They are structural, with four components.

[1] EEAS; 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, January 2024, p. 9, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf [visited on 21 November 2024]

[2] ibid.

[3] ibid.

First is the financial model. It is worth noting that for nearly a decade, there was no viable business model for social platforms. What Google, and then Facebook eventually landed on was a means of commodifying their core asset: the data they collected about their users. This is done in two ways. Data profiles are used to determine how best to hold users' attention, keep them on the platform for longer, and how best to incentivize them to engage with content. In this model, engagement is the primary metric of value. Platform algorithms prioritize entertainment, shock and radicalization over reliable information. In this model, their attention is the product. The second model, linked to the first, is advertising. Data is used to inform targeted advertising that is sold as a product intended to change users' behaviour. The more attention, the more advertising can be sold.

The second is scale. To make these two financial models work, platforms need a global user base. This means operating on a massive scale. The ability to scale without mass is one of the key advantages that digital platforms have over industrial-era companies. They can grow their customers exponentially without commensurate physical scaling. And this has allowed them to grow to truly remarkable sizes. The challenge is that this scale makes responsible moderation of content virtually impossible. Platforms rely on two forms of content moderation. Human content moderators, operating in opaque private content moderation operations, make decisions on whether flagged content breaches complex terms of use agreements. This process is disconnected from national context, culture and linguistic diversity. Platforms also increasingly rely on AI to flag and take down harmful and illegal content, including that from malicious foreign actors. However, these remain highly imperfect moderators of the complex digital ecosystem.

Third is market power. The dominant platforms behave like traditional monopolies, creating barriers for competitors, acquiring start-up challengers, buying new innovations, hiring the industry's top talent and entrenching their data advantages. Their market power is significant, and they are getting bigger. The dynamics of this market concentration are different for each company, but all have elements of concentrated market power. Meta has leveraged its market power and user data to buy potential competitors before they can grow. Amazon both controls a marketplace, and sells products based on the data it derives from it. Google dominates both the way users search and index the internet and sells preferential results within it.

Finally, a structural disconnect exists between the digital infrastructure that has been developed and the institutions of democratic governance. This disconnect has two key implications tied to the scale and complexity of this infrastructure. First, due to scale, platforms would rather have one policy for the whole world; and second, due to complexity, they are likely the most capable of 'governing' the infrastructure. But these companies are not embedded with the core principles of democratic accountability that the governments are. This contraction is simply not how systems of democratic governance work, leading to a structural democratic deficit and a fundamental lack of democratic accountability in how the public sphere is governed.

2.2 Some lessons learnt from Russian FIMI campaigns in the EU

The broad context outlined above creates a relatively safe environment for malicious actors. Russia has been the primary FIMI actor of concern in the EU. This section highlights Russian efforts and the EU's responses.

Russian FIMI campaigns heavily leverage digital platforms and social media to spread false narratives and manipulate public opinion. This strategy takes advantage of the vast reach and engagement-driven algorithms of these platforms. Key tactics applied: creating and amplifying fake news websites, using bots and troll farms to spread disinformation, exploiting platform algorithms to increase the visibility of misleading content[4].

Box 1

Example cases:

- The "Doppelganger" operation, uncovered in Germany, involved creating fake news websites mimicking legitimate outlets.
- In France, a wide-ranging Russian FIMI campaign aimed at undermining Western support for Ukraine involved spreading pro-Russian content, impersonating media and government websites, and coordinating fake accounts.
- Over 1 million German-language posts from over 50,000 fake accounts were discovered in a massive pro-Russia disinformation campaign targeting Ukraine support
- In Poland, approximately 60,000 negative articles and comments about Ukraine are published in Polish-language mass media every month.

Targeting specific countries with tailored narratives. Russian FIMI efforts are often tailored to exploit specific political, historical, and social contexts of target countries. They use the following tactics among others: exploiting historical grievances or national sensitivities; amplifying existing social and political divisions; promoting narratives that align with local far-right or anti-establishment sentiments[5].

Box 2

Example cases:

- In Poland, narratives exploit historical tensions between Poland and Ukraine, suggesting Poland has territorial claims on Western Ukraine.

[4] E. Malitskaya, "Fighting Russian Disinformation in Europe., ISE Group, 14 March 2024 accessed at https://ise-group.org/disinformation

[5] E. Malitskaya, "Fighting Russian Disinformation in Europe," ISE Group, 14 March 2024 accessed at https://ise-group.org/disinformation

- In Germany, FIMI campaigns target the country's energy dependency and economic concerns related to supporting Ukraine.
- In Austria, narratives exploit the country's historical neutrality to argue against support for Ukraine.
- In Poland, over 1,800 distinct disinformation narratives were discovered in 2023 alone.
- In Germany, 37.7% of the population sees more disadvantages than advantages in EU membership, an increase of 7% compared to 2022, partly influenced by disinformation narratives.

A key goal of Russian FIMI is to erode European support for Ukraine by portraying it negatively and questioning the impact of sanctions on Russia. Key tactics include demonizing the Ukrainian government and accusing it of Nazism and corruption, portraying Ukrainian refugees negatively, emphasizing the economic costs of supporting Ukraine for European countries[6].

Box 3

Example cases:

- In France, disinformation campaigns have spread false reports of French mercenaries fighting in Ukraine.
- In Austria, narratives portray Ukrainian refugees as "welfare tourists" burdening the state.
- Across Europe, narratives claim that sanctions against Russia harm European economies more than Russia's.
- Since February 2022, the EUvsDisinfo database has tracked more than 237 disinformation cases relating to Ukraine, and more than 5,500 total cases about Ukraine since 2015.

Promoting Russian dominance and shifting blame. Russian disinformation aims to legitimize Russia's actions and portray it as a victim of Western aggression. Key tactics used: justifying the annexation of Crimea as historically Russian, portraying NATO expansion as a threat to Russian security, framing Russia's actions as defensive responses to Western provocations[7].

Box 4

Example cases:

[6] E. Malitskaya, "Fighting Russian Disinformation in Europe," ISE Group, 14 March 2024 accessed at https://ise-group.org/disinformation

[7] E. Malitskaya, "Fighting Russian Disinformation in Europe," ISE Group, 14 March 2024 accessed at https://ise-group.org/disinformation

- In France, far-right politicians like Marine Le Pen have echoed Russian narratives claiming "Crimea was always Russian.
- In Germany, narratives suggest that the war in Ukraine is a "geostrategic war" to prevent Ukraine from becoming a US military outpost.
- A DW poll showed that nearly 40% of Russian speakers in Germany attribute blame for the war in Ukraine to Russia, while 15% hold Ukraine responsible, and 27% believe both parties share responsibility.

Russian FIMI increasingly utilizes artificial intelligence and other advanced technologies to create and spread false and misleading content more effectively. Key tactics include using AI to generate and amplify misleading content, creating deepfakes and manipulated media, and employing AI-driven targeting to reach specific demographics.

2.3 EU efforts to address FIMI

At the EU level, various initiatives aim to counter FIMI and reduce the spread of manipulative content.

Regulation and Code of Conduct

The EU's **Digital Services Act (DSA)** and the Strengthened Code of Practice on Disinformation (hereafter, **the Code of Practice**) are the two key components of the EU's strategy to combat disinformation. The DSA provides a legal framework for digital services, while the Code of Practice is a self-regulatory tool, through which signatories voluntarily commit to a set of practices to counter the spread of disinformation[8].

The DSA aims to ensure the transparency of content moderation practices and provide measures to tackle the presence of disinformation, harmful content and hate speech on online platforms such as social networks and content-sharing platforms. The DSA came into force for all platforms on 17 February 2024. The Act also provides a framework for cooperation between the Commission and law enforcement, and for monitoring the implementation of all its obligations[9]. Companies that fail to comply with the DSA's rules could face fines of up to 6% of their global turnover. To enhance the effectiveness of the DSA, a complementary Code of Practice was developed. This Code provides a detailed framework to help online platforms and other stakeholders combat disinformation, particularly in the context of the EU elections. The Code is a first-of-its-kind tool through which relevant players active in the online information ecosystem in the EU have agreed to self-regulatory standards to fight disinformation.

[8] Romanishyn, A. (2024). "Enhancing Election Integrity by Strengthening EU Defences Against Disinformation," European View, https://doi.org/10.1177/17816858241292435

[9] European Commission, "The Impact of the Digital Services Act on Digital Platforms" (3 November 2023).

A central tool in this effort is the **Code of Practice**, launched in 2018 and strengthened in 2022. This voluntary code commits major online platforms and advertisers to take comprehensive measures against disinformation. Key provisions include requirements for transparency in political advertising, limiting fake accounts, and reducing the spread of manipulatively generated information.[10]

The Code has proven to be an effective tool for raising platform awareness about the issue and increasing their accountability. Compliance with the agreed-upon measures is monitored through regular reports, ensuring continuous improvement.

The strengthened version of the Code from 2022 builds on the original 2018 Code and includes 44 commitments and 128 specific measures. These measures encompass **demonetization**, which cuts off financial incentives for disinformation spreaders. Other measures include **enhancing cooperation with fact-checkers** and **enabling better data access for researchers**.[11]

Another important element is the **Transparency Centre**, which provides the public with a clear overview of the policies implemented by the signatories and is regularly updated with relevant data. The Code is also recognized as a code of conduct under the **DSA**, further underscoring its significance and effectiveness.[12]

Overall, the EU Code of Practice on Disinformation represents a pioneering example of industry self-regulation and contributes to a more transparent, safer, and more trustworthy online environment.

Initiatives and Toolboxes

The **EU Action Plan Against Disinformation**, developed in 2018, was a response to the European Council's calls in June and October 2018 for a coordinated approach to tackle disinformation, especially in light of the upcoming European elections. The plan focuses on enhancing the capabilities of EU institutions and Member States to detect, analyze, and expose disinformation campaigns both within the EU and in its neighbourhood.[13]

A significant aspect of the Action Plan is the **Strategic Communication Task Forces** of the European External Action Service (EEAS), which play a crucial role in countering disinformation by improving strategic communication. The plan also emphasizes the importance of mobilizing the private sector to fulfil its commitments to combating disinformation and enhancing societal resilience against its impacts.

[10] Refer to the 2022 Code of Practice on Disinformation, available at: https://digital-strategy.ec.europa.eu/de/policies/code-practice-disinformation [visited on 21 November 2024]
[11] ibid.
[12] The Transparency Centre, available at: https://disinfocode.eu/ [visited on 21 November 2024]
[13] Refer to Together Against Disinformation, available at: https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/eu-desinformation-1875918 [visited on 21 November 2024]

Additionally, the Action Plan includes measures to strengthen coordinated and joint responses to disinformation, improve the detection and analysis of disinformation, and enhance public awareness and media literacy to build societal resilience.

The **FIMI Toolbox**[14] of the European Union is a crucial instrument in the fight against foreign information manipulation and interference. A central goal of the toolbox is to assist the EU and its member states in responding to manipulative information practices originating from both state and non-state actors. It encompasses a wide range of measures and strategies aimed at protecting the democratic processes of the EU and minimizing the impacts of FIMI.

The toolbox outlines various areas and instruments that together form a robust and comprehensive framework for combating foreign information manipulation and interference. It includes measures designed for the short, medium, and long term, ranging from preventive approaches to responses to incidents. This dynamic system is intended to adapt to the constantly evolving threats, allowing existing instruments to be supplemented by new ones as needed.

The toolbox should not be viewed as a complete list of instruments; rather, it provides an overview of the diversity of approaches across four dimensions. Additionally, it is meant to complement other toolboxes, particularly the EU's Hybrid Toolbox. Close cooperation across these domains is essential to fully leverage the potential of these instruments. To effectively combat FIMI, it is also important to collaborate with other stakeholders in the defense community, following a "whole-of-society" approach.

The instruments can be grouped into four dimensions:

1. *Situational Awareness*: A comprehensive understanding of the threat is a fundamental prerequisite for determining the most appropriate responses and actors.

2. *Resilience Building*: This includes strategic communication efforts, collaboration within the EU's Rapid Alert System, and ongoing initiatives to inform and raise public awareness.

3. *Disruption and Regulation*: Measures aimed at promoting trust, transparency, and safety in the information environment, such as the Digital Services Act, serve as permanent instruments that shape the conditions for responses to FIMI.

4. *Measures related to EU external action*: This dimension encompasses instruments in the area of foreign and security policy, including international cooperation, the G7 Rapid Response Mechanism, and sanctions against Kremlin-controlled media outlets like RT and Sputnik.

[14] Refer to – EAAS responses to foreign information manipulation and interference; available at https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en [visited on 21 November 2024]

A central element of the toolbox is the **Rapid Alert System** (RAS), which enables quick responses to FIMI incidents. This system promotes collaboration among member states and other relevant actors to efficiently exchange information and detect threats early.

Within the framework of the RAS, various stakeholders work together, including EU institutions, member states, academic institutions, and fact-checkers. This collaboration allows for comprehensive analyses of threats and timely responses to identified risks. For example, the RAS could be activated if a coordinated FIMI campaign is detected during an election period. In such a case, the system would rapidly disseminate information about the nature of the disinformation, the affected platforms, and the potential impacts, enabling member states to take immediate action.[15]

Additionally, the **Information Sharing and Analysis Centre** (FIMI ISAC)[16] plays a crucial role by providing a platform for sharing experiences and insights.

The toolbox aims not only to improve the identification of FIMI incidents but also to optimize the analysis and reporting of these incidents. Regular reports help develop a shared understanding of the threats and formulate appropriate countermeasures. Through this structured approach, the EU is empowered to take proactive action against disinformation and hold those responsible accountable.

Overall, the FIMI Toolbox represents an important step in the EU's strategy to address the challenges of the digital information landscape and defend democratic values. It underscores the importance of remaining vigilant in an increasingly interconnected world and working together to combat disinformation.

Another important initiative is **EUvsDisinfo**, an East StratCom Task Force campaign within the European External Action Service. This initiative aims to publicly expose and actively counter Russian disinformation campaigns, publishing regular reports and analyses to uncover disinformation content and shed light on the origins of such campaigns. Established in 2015, EUvsDisinfo identifies, documents, and debunks disinformation, with a database containing over 17,000 cases of pro-Kremlin disinformation. The initiative also provides training and briefings to EU institutions, Member State governments, journalists, and civil society organizations to enhance their resilience against disinformation. Additionally, EUvsDisinfo collaborates with international researchers and regularly publishes articles on new developments in disinformation tactics.[17]

In addition, the **European Digital Media Observatory (EDMO)** plays a key role. EDMO operates hubs in all EU countries and promotes collaboration among fact-checkers, researchers, and other stakeholders to combat disinformation and enhance media literacy among the public effectively. Established in 2020, EDMO supports an independent community dedicated to tackling disinformation through a

[15] Refer to – Factsheet: Rapid Alert System; available at https://www.eeas.europa.eu/eeas/factsheet-rapid-alert-system_en [visited on 21 November 2024]

[16] https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en [visited on 21 November 2024]

[17] Refer to Countering Disinformation, available at: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en [visited on 21 November 2024]

multidisciplinary approach. The Observatory coordinates the activities of 14 regional and national hubs, which engage in detecting and exposing online disinformation, organizing media literacy activities, and analyzing digital media ecosystems across 28 countries in the EU and the European Economic Area (EEA). EDMO also provides a platform for fact-checkers, academics, and media literacy experts to collaborate and share best practices, thereby strengthening the overall resilience against disinformation. Furthermore, EDMO offers training and resources to enhance the skills of media practitioners, teachers, and citizens in identifying and countering disinformation.[18]

The **EDMO Guidelines for Effective Media Literacy Initiatives**[19] are meticulously designed to significantly enhance the effectiveness of media literacy projects across Europe. Developed by EDMO's Working Group on Media Literacy Standards and Best Practices, these guidelines incorporate insights from 14 national and cross-national hubs and over 100 experts from more than 50 countries, aiming to fortify societal resilience against disinformation. Endorsed by over 60 organizations, including academic institutions, regulatory bodies, and civil society organizations, these guidelines cater to a diverse audience involved in media literacy initiatives, such as educators, policymakers, and professionals in the media and technology sectors. They offer adaptable recommendations suitable for various projects.

The core principles are categorized into three phases: *Development, Delivery* and *Review*. Development involves clearly defined goals and principles, Empowerment, Critical understanding of the media ecosystem, Consultative and relevant Evidence-based, Inclusive Ethical and accessible. Delivery covers Transparency, Preparation, Adaptability, and Review, including Sustainability Reflection, sharing, and evaluation. The comprehensive guidelines offer detailed explanations, pertinent resources, and exemplary practices.

European Parliament's Special Committee on Foreign Interference[20] (INGE) adopted a report with recommendations for protecting the 2024 European elections[21].
Key points include:

- Calling for a ban on TikTok on devices of EU institutions and national governments due to security concerns;
- Urging strengthened cybersecurity measures to prevent hacking and attacks on election-related infrastructure;
- Recommending the creation of a permanent body to monitor and counter foreign interference;
- Advocating for increased media literacy education;

[18] Refer to EDMO - European Digital Media Observatory, available at https://www.eui.eu/research-hub?id=european-digital-media-observatory-1 [visited on 21 November 2024]
[19] Refer to EDMO - The European Digital Media Observatory launches Media Literacy Guidelines, available at https://digital-strategy.ec.europa.eu/en/news/european-digital-media-observatory-launches-media-literacy-guidelines [visited on 21 November 2024]
[20] This committee, officially called the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE2)
[21] European Parliament, "Foreign interference: MEPs call for urgent protection of 2024 European elections," 25 May 2023, https://www.europarl.europa.eu/news/en/press-room/20230524IPR91908/foreign-interference-meps-call-for-urgent-protection-of-2024-european-elections

- Suggesting stricter regulations on political advertising online; and
- The committee emphasized the urgency of implementing these measures before the 2024 elections, given the increased risk of foreign interference and disinformation campaigns.

The EU has allocated funding to combat disinformation through various programs[22], but the approach has been criticized as fragmented and often insufficient.

- The European Digital Media Observatory (EDMO) received €11 million for 2020-2022 to support fact-checking networks and research
- The Creative Europe program includes some funding for media literacy projects
- Horizon Europe has allocated funds for research on disinformation

However, challenges include: many initiatives are short-term or project-based, limiting their long-term impact; funding is often spread across different EU bodies and programs, making it difficult to coordinate efforts; civil society organisations and independent media often struggle to access sustainable funding. The European Parliament has called for more coherent and substantial funding to support fact-checking and media literacy initiatives[23]. This fragmented approach to funding has been identified as a limitation in the EU's overall strategy to combat disinformation, particularly in the context of preparing for major events like the 2024 European elections.

3 Relevance of EU approach for Canada

The European Union has been actively combating FIMI within the Union for several years now. Some insights from recent years are also crucial for Canada. There are, of course, limitations to direct comparisons to EU and Canadian policy on foreign interference and disinformation. First and foremost, while there are overlapping threats, the breadth of the EU member states interests and roles in the world means the diversity of foreign threats faced by the EU is more multivarious than those directed at Canada. Second, policies developed through the EU represent a multinational governance approach and are ultimately applied by national legal and regulatory mechanisms. Canadian policy is largely national, making direct comparisons to drafting language, governance bodies and powers difficult.

3.1 Combating FIMI as a Long-Term Task and Not Just Before Elections

FIMI should not only be seen as a threat to the state and society in the run-up to elections and referendums. On the contrary: the mitigation and fight against FIMI should be seen as a long-term and ongoing task. The operations and attacks exerted by these foreign agents are designed to undermine democracies in the long run and do, therefore, not always target elections as isolated destabilizing opportunities. Their objectives are clear: to fundamentally influence political decisions, processes and actors over a sustained period.

[22] European Commission, "Fighting disinformation," https://digital-strategy.ec.europa.eu/en/policies/online-disinformation
[23] European Parliament, "EU efforts to fight disinformation," 22 March 2023, https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745686/EPRS_ATA(2023)745686_EN.pdf

In recent times, elections have pushed states to act. In the run-up to elections, states often begin to see an increased spread of FIMI, thus threatening the election campaign, the election process, and, subsequently, the election result. During these phases, states often invest more financial and personnel resources to reduce the possibilities of influence.

Against this background, states have begun to develop and implement continuous measures and strategies to combat FIMI both in the short- and in the long-run.

3.2 Committee on the Parliamentary Level

Already mentioned above, the European Parliament's Committee on Foreign Interference (INGE) has played a crucial role in addressing the growing threat of foreign interference and disinformation in Europe. It was established in 2020 and then relaunched with an updated name and responsibilities in 2023.[24]

This special committee has been at the forefront of investigating and countering foreign interference and disinformation campaigns targeting EU member states. INGE's mandate encompasses a wide range of activities, including analyzing foreign actors' attempts to manipulate public opinion, spread disinformation, and interfere with electoral processes. The committee has made significant strides in identifying vulnerabilities in EU democratic systems and proposing concrete measures to enhance resilience against foreign interference.

Key achievements of the INGE committee include:

1. The committee has produced detailed analyses of foreign interference tactics, providing valuable insights for policymakers and stakeholders.

2. INGE has proposed a series of measures to strengthen EU institutions and member states' capabilities in countering disinformation and foreign interference.

3. Through public hearings and engagement with the media, the committee has increased public understanding of the threats posed by foreign interference.

4. INGE has facilitated collaboration between EU institutions, national governments, and civil society organizations in combating disinformation.

The committee has issued several calls to action, urging EU institutions and member states to:

1. Enhance legislative frameworks to address foreign interference and disinformation.
2. Increase funding for research and development of tools to detect and counter disinformation.

[24] In 2023 the name was changed to Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation. Refer to: https://www.europarl.europa.eu/news/en/press-room/20230210IPR74716/special-committee-on-foreign-interference-to-deal-with-corruption-allegations [visited on November 22, 2024]

3. Strengthen media literacy programs across the EU to build societal resilience against manipulation.
4. Improve coordination between EU bodies and national authorities in responding to foreign interference threats.
5. Develop stricter regulations for social media platforms to combat the spread of disinformation.

3.3 Targeted Operations for Diverse Information Spaces

Most foreign state actors, such as Russia, China, and Iran, strategically employ FIMI to sow instability in their target countries. These operations are tailored to the distinct regions and their specific characteristics. In the European Union (EU), there is not merely one single information space; rather, there are multiple very diverse information spaces that exist due to the multitude of member states that make up the EU and are each characterized by their own distinct history and political reality. This, in turn, means that the architects of FIMI attacks cannot apply a single approach to destabilize the EU as a whole.

Rather, they need to take the different historical, socioeconomic, religious, and political realities in their target country into account in order to assess what the most vulnerable segments of society are to successfully spread mis- and disinformation narratives.

The actors exploit the specificities of these spaces to enhance the success prospects of FIMI. Manipulated information and narratives that resonate within one information space in society or parts of society may have little to no impact in others.

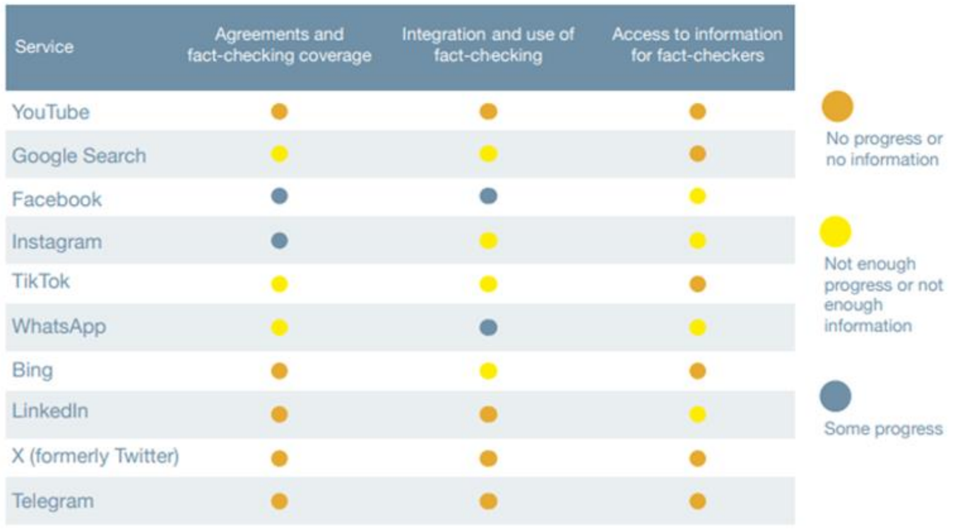
3.4 Access to data for analysts and scientists

Both the DSA and, particularly, the Code of Practice encourage multi-stakeholder cooperation between online platforms and fact-checkers to combat disinformation. However, the effectiveness of this cooperation depends on the willingness and ability of these parties to engage in these efforts.

For instance, the key commitments of the Code of Practice regarding cooperation between online platforms and fact-checkers include setting up agreements, integrating and using fact-checking services, and providing access to data. However, an analysis by the European Fact-Checking Standards Network (EFCSN) revealed that most very large online platforms and search engines are still far from fulfilling their promises of cooperation and do not have effective risk-mitigation measures against disinformation in place, as required by the DSA.[25]

Figure 1: Compliance of VLOPs at glance.

[25] EFCSN, "The EFCSN Reviews Big Tech's Implementation of the EU Code of Practice on Disinformation."



Service	Agreements and fact-checking coverage	Integration and use of fact-checking	Access to information for fact-checkers
YouTube	🟠	🟠	🟠
Google Search	🟡	🟡	🟠
Facebook	🔵	🔵	🟡
Instagram	🔵	🟡	🟡
TikTok	🟡	🟡	🟠
WhatsApp	🟡	🔵	🟡
Bing	🟠	🟡	🟠
LinkedIn	🟠	🟠	🟡
X (formerly Twitter)	🟠	🟠	🟠
Telegram	🟠	🟠	🟠

🟠 No progress or no information

🟡 Not enough progress or not enough information

🔵 Some progress

Source: EFCSN, *Fact-Checking and Related Risk-Mitigation Measures for Disinformation in the Very Large Online Platforms* (January 2024), reproduced with permission.

The DSA imposes a range of obligations on digital service providers, with particular emphasis on very large online platforms (VLOPs). These obligations include measures to remove or restrict access to illegal content, including disinformation. The Act also establishes a framework for cooperation between the European Commission and law enforcement agencies to monitor the implementation of its provisions. Companies that fail to comply with the DSA's rules could face substantial fines of up to 6% of their global turnover, underscoring the EU's commitment to enforcing these regulations.

However, the DSA faces several challenges in its implementation and effectiveness in this regard. One significant issue is the lack of a clear legal definition of disinformation within the Act. This ambiguity could lead to fragmented application across EU member states, potentially undermining the DSA's effectiveness in combating disinformation during critical periods such as elections. The absence of a precise definition also raises concerns about potential over-censorship or inconsistent enforcement.

Another limitation of the DSA is its primary focus on VLOPs, while smaller platforms that also contribute to the spread of disinformation may not be subject to the same level of scrutiny. This disparity in regulatory oversight could create loopholes in the fight against disinformation. Additionally, the implementation of the DSA requires significant resources from platforms to modernize their internal processes and compliance mechanisms, which may pose challenges for smaller entities.

The DSA's provisions related to content removal have also sparked debates about potential regulatory overreach. There are concerns that the requirement for platforms to swiftly remove or restrict access to illegal content could lead to the over-removal of legitimate political speech and debate, potentially chilling free expression during election periods.

Furthermore, the DSA's impact on artificial intelligence-based amplification of disinformation may be limited. While the Act focuses on transparency, it may not be sufficient to counteract the speed and scale at which AI can disseminate false information. The DSA's current provisions might not be robust enough to effectively prevent or counteract targeted disinformation campaigns, especially those originating from foreign actors or conducted through covert methods.

Despite these challenges, the DSA represents a significant step forward in regulating digital platforms and combating disinformation. Its implementation, alongside complementary measures such as the Code of Practice on Disinformation, demonstrates the EU's commitment to addressing the complex issues surrounding online content moderation and the spread of false information. As the digital landscape continues to evolve, ongoing assessment and refinement of the DSA will be crucial to ensure its effectiveness in safeguarding the integrity of online information ecosystems, particularly during critical democratic processes such as elections.[26]

3.5 Fact-Checking Infrastructure and Initiatives in Europe

The European landscape of fact-checking and disinformation combat has evolved significantly in recent years, particularly in response to Russian disinformation campaigns. A key player in this field is the European Fact-Checking Standards Network (EFCSN), which plays a crucial role in reviewing the implementation of the EU Code of Practice on Disinformation by major digital platforms. The EFCSN has been critical of some platforms for not fully implementing measures they committed to and for misrepresenting their policies in reports.

Several countries have developed specific initiatives to address disinformation. In Poland, the Demagog Association specializes in fact-checking and debunking disinformation. Germany has invested approximately 2.3 million euros to support ten journalism projects, with a particular focus on fact-checking initiatives. These country-specific efforts highlight the growing recognition of the need for localized approaches to combat disinformation.

Multi-stakeholder cooperation has emerged as a key strategy in the fight against disinformation. There is an increasing emphasis on collaboration between online platforms, fact-checkers, and other stakeholders to effectively combat the spread of false information.

3.6 Overcome Language Barriers

Despite these efforts, several challenges persist in the fact-checking landscape. One significant issue is the language barrier. There is a recognized need for improved content assessment capabilities in all EU languages to effectively combat disinformation across the diverse linguistic landscape of Europe.

The algorithms used by digital platforms pose another challenge. Fact-checkers have highlighted difficulties in ensuring that platform algorithms prioritize fact-based, independent journalism over sensational or false information. This algorithmic bias towards engaging content often works against the dissemination of factual information.

[26] Romanishyn, A. (2024). “Enhancing Election Integrity by Strengthening EU Defences Against Disinformation.” European View, https://doi.org/10.1177/17816858241292435

Resource allocation remains a critical issue. While some funding is available for fact-checking initiatives, it is often fragmented and project-based. This approach can dilute the impact of media literacy projects and limit the long-term effectiveness of fact-checking efforts.

The sheer scale and speed of disinformation, especially on social media platforms, present significant challenges for fact-checkers to keep up. The volume of content being produced and shared makes comprehensive fact-checking a daunting task.

3.7 Technological Advancements and Policy Framework

To address these challenges, there is growing interest in using AI-driven tools to detect and filter out disinformation content at scale. Some proposals suggest using blockchain technology to create immutable records of political advertising and content moderation decisions.

As explained in detail above, the Digital Services Act (DSA) provides a legal framework for digital services and aims to ensure transparency of content moderation practices. It imposes obligations on platforms to combat disinformation. The Code of Practice on Disinformation serves as a self-regulatory tool for platforms, including commitments related to fact-checking and cooperation with fact-checkers.

3.8 International Cooperation and Public Engagement

There is increasing recognition of the need for international cooperation in fact-checking, especially for addressing disinformation campaigns that target multiple countries. Fact-checkers across Europe are encouraged to share best practices and methodologies.

4 Foreign Information Manipulation and Interference Threats to Canada and the National Response

Canada, like other advanced democracies, faces growing threats from foreign information manipulation and interference. Throughout 2023 and 2024, the Canadian public, policy-makers, and those tasked with defending the country from interference have become acutely aware of these threats, and in many ways, these issues are now top of the policy agenda.[27] These efforts by foreign actors seek to disrupt Canadian democratic processes, erode trust in institutions, and exploit societal vulnerabilities. Adversaries are employing various tactics to achieve their strategic objectives, all of which take advantage of structural vulnerabilities in the information ecosystem.

[27] https://www.cbc.ca/news/politics/foreign-interference-trudeau-poilievre-india-1.7356434 and https://www.ctvnews.ca/politics/public-inquiry-grapples-with-definition-of-foreign-interference-in-its-final-week-1.7081249 [visited on 21 November 2024]

4.1 2019 and 2021 Canadian federal elections

While FIMI occurs both in and outside election periods, the 2019 and 2021 federal elections in Canada are instructive regarding the evolving threat of FIMI. These elections illustrate a growing prevalence of disinformation and increasing concern about its impact on democratic processes. While the 2019 election revealed emerging vulnerabilities in Canada's democratic systems, the 2021 election demonstrated a significant escalation in the complexity and influence of FIMI efforts.

While disinformation and misinformation were present in the 2019 federal election, they did not significantly impact the election's outcomes. A high-profile review concluded that incidents of foreign interference were relatively limited and insufficient to necessitate public notification under the Critical Election Incident Public Protocol (CEIPP).[28] However, the election revealed vulnerabilities in Canada's democratic processes, particularly in the areas of online disinformation and social media manipulation.

One significant concern during the 2019 election was the amplification of domestic political tensions by foreign actors. While no direct foreign involvement was conclusively identified in key disinformation campaigns, concerns emerged regarding how foreign states might exploit Canada's divisive political environment in the future. Social media platforms played a prominent role, with mechanisms such as trending algorithms and virality aiding in the rapid dissemination of misinformation, even when it originated domestically. The election highlighted the lack of coordination between federal agencies and the insufficient capacity to monitor and respond to emerging threats on digital platforms. Despite these challenges, public confidence in the integrity of the election process remained high.[29]

By the 2021 federal election, the threat landscape had shifted significantly, with foreign interference becoming a more prominent concern. The preliminary findings of the Hogue Commission indicated that disinformation campaigns, particularly those related to COVID-19, were amplified by both domestic actors and foreign states such as China and Russia.[30] Protesters fuelled by misinformation disrupted campaign events, pushing pandemic-related issues to the forefront of public discourse. While these incidents were not necessarily driven by organized foreign interference, the influence of global disinformation narratives, particularly those originating from the U.S., played a notable role in shaping public perceptions.

The Hogue Commission and Rosenberg reports also noted the emergence of cohesive misinformation networks that transcended borders, linking Canadian communities with global conspiratorial movements. Foreign states leveraged these networks to undermine trust in Canada's democratic institutions. For example, narratives about voter fraud—though unsubstantiated—circulated widely and echoed claims from the 2020 U.S. presidential election.[31] Despite the growing sophistication of FIMI efforts, the election process itself is perceived to remain secure, with no evidence of foreign

[28] https://www.canada.ca/en/democratic-institutions/services/reports/report-assessment-2021-critical-election-incident-public-protocol.html [visited on 21 November 2024]
[29] https://meo.ca/work/digital-democracy/canada2019 [visited on 21 November 2024]
[30] https://foreigninterferencecommission.ca/news/article/foreign-interference-commission-releases-initial-report [visited on 21 November 2024]
[31] https://meo.ca/work/election-misinfo/canada2021 [visited on 21 November 2024]

interference altering results. Public perceptions of the threat of foreign interference have grown significantly and there is concern about the long-term erosion of trust in Canadian democracy.

4.2 Canadian vulnerabilities

A combination of structural, demographic, and technological factors shapes Canada's vulnerabilities to foreign interference. While the country prides itself on openness, diversity, and inclusiveness, these very characteristics have been exploited by foreign actors seeking to manipulate Canadian institutions, influence political outcomes, and undermine public trust. Below are some of the most critical vulnerabilities that make Canada particularly susceptible to FIMI.

Canada's multicultural landscape, while a strength in many respects, has also become a target for foreign influence. With large diaspora communities, particularly Chinese, Iranian, Indian Sikhs, Indian Hindus and Russians, foreign states frequently attempt to manipulate these populations by exerting pressure on their members in Canada. Chinese, Iranian, and Indian operatives have been known to monitor, intimidate, and harass activists or critics of their home governments, sometimes leveraging familial ties abroad as leverage.[32]

For example, members of the Chinese diaspora have been pressured by the Chinese Communist Party (CCP) to suppress criticisms of China's human rights record or its policies on Taiwan and Hong Kong. This vulnerability is further magnified by the lack of resources in Canadian security agencies to effectively monitor and respond to these activities. A similar dynamic has emerged with India's foreign influence efforts targeting Sikh activists advocating for the Khalistan movement.[33]

Two other vulnerabilities are present: vulnerabilities in cybersecurity infrastructure. Despite Canada's advanced cybersecurity infrastructure, state-sponsored cyber actors, particularly from China, Russia, and North Korea, continue to exploit vulnerabilities. Many critical infrastructure operators, such as those in the energy, finance, and healthcare sectors, may lack the resources, personnel, and expertise to defend themselves against sophisticated cyberattacks. Further complicating matters, these cyberattacks are often multi-pronged. Foreign actors not only seek to steal intellectual property and intelligence but also to disrupt communications and spread disinformation through cyber channels. For example, Russia has been linked to ransomware campaigns that target Canadian public services and businesses, while China has engaged in more covert cyber espionage efforts. Given the high dependence on digital infrastructure, Canada's vulnerability to cyberattacks presents a clear national security risk. These efforts often compound FIMI vulnerabilities and enable more sophisticated operations.

Finally, Canada's political landscape is characterized by a certain degree of fragmentation, particularly between federal and provincial jurisdictions. This division can sometimes hinder coordinated responses to FIMI threats, as seen during the investigations into foreign interference in the 2019 and 2021 federal elections. Furthermore, public awareness of foreign interference until recently was low,

[32] https://globalnews.ca/news/9954415/michael-chong-foreign-interference-testimony/ [visited on 21 November 2024]
[33] https://www.bbc.com/news/articles/c89lne2k87vo [visited on 21 November 2024]

and improvement has been slow. Many Canadians are unaware of the extent to which foreign states actively seek to manipulate public discourse or influence political outcomes. The Critical Election Incident Public Protocol was established to notify Canadians of significant foreign interference during elections, but it has been criticized for not being transparent enough in its decision-making processes, leading to underreporting of interference threats. This lack of transparency leaves the public vulnerable to manipulation, especially during politically sensitive periods.

Building on this context, the report assesses current Canadian perspectives on FIMI, focusing on two dimensions: 1) country-specific threats and 2) emergent or harmful types of FIMI. Each dimension is addressed in turn, followed by an overview of Canada's response to FIMI to date.

4.3 Country-Specific Foreign Interference Threats in Canada

In the Canadian context, China, Russia, India, and Iran have advanced distinct strategies to manipulate public discourse, interfere in democratic processes, and influence policy.

China

China is one of the most persistent and sophisticated actors in Canada's foreign interference ecosystem. The People's Republic of China has engaged in a range of activities, including espionage, cyberattacks, and the use of disinformation to sway political and public discourse. China's interference focuses heavily on the Chinese diaspora, with tactics that include the surveillance of activists, attempts to silence critics of the Chinese Communist Party, and pressure on Chinese Canadian politicians. The harassment of Conservative MP Michael Chong[34] and the disinformation spread about incumbent Kenny Chiu during the 2021 Canadian federal election[35] are two notable examples (among many) of how Chinese influence extends into Canadian politics.

In addition to targeting individuals, China seeks to influence broader political outcomes. Intelligence reports suggest that the CCP attempted to sway the 2019 and 2021 federal elections by supporting specific candidates and undermining others, often through covert and deceptive means.[36] These tactics are part of a broader strategy to ensure that Canadian policy remains favourable to China's interests, especially regarding Taiwan, the Uyghurs, and Hong Kong.

Russia

Russia's approach to interference is rooted in its broader strategy of disrupting democratic institutions and undermining the Western-led international order. Russian tactics in Canada primarily focus on cyberattacks, disinformation campaigns, and the exploitation of societal divisions. Russia's disinformation apparatus is particularly adept at amplifying polarising narratives, often playing on themes of immigration, social justice, and national security to exacerbate tensions. Russia has used

[34] https://globalnews.ca/news/9954415/michael-chong-foreign-interference-testimony/ [visited on 21 November 2024]
[35] https://nationalpost.com/news/conservatives-saw-voting-anomalies-in-same-ridings-they-suspected-foreign-interference-in-2021-election-otoole [visited on 21 November 2024]
[36] https://www.reuters.com/world/americas/canada-spies-found-china-interfered-last-two-elections-probe-hears-2024-04-08/?utm_source=chatgpt.com [visited on 21 November 2024]

disinformation to attempt to delegitimize Canadian support for Ukraine and has targeted both critical infrastructure and public institutions through cyberattacks.[37]

The cyber capabilities of Russian actors, coupled with their sophisticated use of social media, make them a persistent and dangerous threat. In one instance, Russian-linked media organizations were found to have funded Canadian influencers to spread narratives aligned with Russian geopolitical interests during the U.S. election.[38] Although the direct impact on Canada has not yet been as overt as in other countries, Russia's ongoing efforts to weaken trust in democratic institutions are concerning.

India

India's foreign interference in Canada has come under intense scrutiny recently, particularly following accusations that Indian operatives were involved in the assassination of Sikh leader Hardeep Singh Nijjar in British Columbia in June 2023. The Canadian government responded by expelling several Indian diplomats in relation to the alleged operation, marking a significant escalation in tensions between the two countries. The case highlighted India's ongoing efforts to monitor and target members of the Sikh community in Canada, particularly those advocating for the Khalistan movement, which calls for an independent Sikh state in Punjab. According to recent reports, Indian agents, operating under diplomatic cover in consulates across Canada, have recruited local informants, often through coercion or financial incentives, to gather intelligence on Sikh activists and other opponents of the Modi government. These operatives have allegedly engaged in activities ranging from surveillance to violent crimes, including shootings and arson attacks, aimed at silencing or eliminating critics of the Indian government.[39] The involvement of organized crime groups in executing some of these violent acts further underscores the scale and severity of India's foreign interference in Canada.

Iran

Iran has been implicated in surveillance and intimidation efforts directed at Iranian-Canadian activists, particularly those who criticize the Iranian regime or advocate for reform. This interference primarily targets individuals involved in political activism, including those who support women's rights, oppose the regime's treatment of dissidents, or criticize its foreign policies. Iranian operatives have reportedly monitored protests, compiled information on attendees, and used this intelligence to intimidate or harass activists in Canada.[40] These activities seek to silence critics of the regime and create a climate of fear within the Iranian diaspora community in Canada. Such actions are part of a broader Iranian strategy of suppressing dissent beyond its borders through a combination of surveillance, intimidation, and disinformation.

[37] https://www.canada.ca/en/global-affairs/news/2024/10/global-affairs-canada-statement-on-russian-disinformation.html [visited on 21 November 2024]
[38] https://www.cdmrn.ca/russian-funding-canadian-influencers [visited on 21 November 2024]
[39] https://globalnews.ca/news/10811118/indian-government-agents-canada-modi-opponents/ [visited on 21 November 2024]
[40] https://ici.radio-canada.ca/rci/en/news/1933800/spy-agency-investigating-credible-death-threats-from-iran-against-individuals-in-canada [visited on 21 November 2024]

4.4 Notable Pathways for FIMI

Generative AI and deepfakes

Generative AI, including deepfake technologies, are quickly becoming a significant tool in the foreign interference arsenal. With generative AI, state and non-state actors can produce highly realistic content—whether in the form of text, images, videos, or audio clips—that can be used to mislead, distort, or manipulate public perception. The rise of deepfake technology, which allows for the creation of fabricated videos that appear convincingly real, presents significant challenges in discerning truth from falsehood, particularly when targeting political figures or public debates.

In the Canadian context, generative AI was used to produce coordinated posts related to political events, such as the bot-generated posts following Pierre Poilievre's rally in Kirkland Lake.[41] These bots, driven by generative AI models, highlighted the growing risk of AI-generated disinformation. Generative AI could also easily be used to create deepfakes targeting political leaders, further undermining public trust. This appears to be happening in Canada already for crypto scams.[42]

FIMI-enabling cyberattacks

Cyberattacks remain a key tactic in FIMI efforts, with foreign state actors, particularly Russia and China, frequently targeting Canadian infrastructure, businesses, and government systems. With regard to FIMI, the capacity of foreign actors to use cyberattacks for intelligence gathering is particularly troubling. For instance, Russia has been implicated in multiple cyber incidents aimed at compromising Canadian digital infrastructure, including attempts to breach election-related systems. The rise in ransomware attacks and phishing campaigns targeting key Canadian institutions adds to this threat.[43]

Social media and the influencer class

The recruitment of social media influencers by foreign states has become a highly effective, albeit covert, form of interference. Platforms like X (formerly Twitter) and YouTube have seen an increase in influencer-driven content that, at times unknowingly, promotes state-aligned disinformation. Social media influencers, even those with modest followings, have been targeted to disseminate polarising content aimed at deepening societal divisions. In Canada, foreign states like Russia have sought to exploit such influencers to push narratives that align with geopolitical objectives or undermine public trust in democratic institutions.[44]

Private channels

Private communication channels such as encrypted messaging apps and closed social media groups have been documented to facilitate the spread of disinformation, with foreign actors attempting to

[41] https://www.cdmrn.ca/kirkland-lake-bot-campaign [visited on 21 November 2024]
[42] https://www.thecanadianpressnews.ca/fact_checking/youtube-video-of-freeland-promoting-investment-scheme-is-a-fake/article_544ecbd9-5e5d-5705-ab6f-48c01b27b37c.html
[43] https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update [visited on 21 November 2024]
[44] https://www.cdmrn.ca/russian-funding-canadian-influencers [visited on 21 November 2024]

influence Canadian public opinion. Platforms like WhatsApp, Telegram, and WeChat are particularly vulnerable to this type of interference due to their encrypted nature. These platforms also serve as tools for surveillance and intimidation, with dissidents and activists in Canada reporting harassment through private communication channels.[45]

Linguistic minority targeting

Again, linguistic minority communities in Canada are increasingly targeted by foreign interference campaigns due to their use of non-English, non-French media and communication platforms. These communities often rely on foreign-language social media and news outlets that are susceptible to manipulation by foreign states, especially those with strong diaspora populations in Canada, such as China, India, and Russia. In the case of the Chinese Canadian community, WeChat has been utilized to disseminate disinformation that aligns with Beijing's geopolitical interests.[46] Similarly, Russian disinformation campaigns have exploited linguistic divisions to spread polarising narratives.[47]

4.5 Canada's Response to Foreign Interference

Canada's efforts to address foreign interference have evolved significantly over recent years. Numerous initiatives have been implemented to strengthen Canadian defences and improve resilience against the threats and pathways outlined above.

Digital Citizen Initiative

Canadian Heritage plays a key role in combating FIMI through the Digital Citizen Initiative, which funds projects aimed at raising awareness and building resilience against online disinformation. This includes support for research, digital literacy programs, and partnerships with civil society organizations to enhance Canadians' ability to recognize and respond to misinformation. The initiative emphasizes public engagement and supports a healthy information ecosystem to protect democracy from foreign influence.[48]

Media and information literacy

Media and information literacy efforts in Canada have been spearheaded by initiatives like the Digital Citizen Initiative, but much of the on-the-ground work is carried out by non-governmental organizations such as MediaSmarts, which provides digital literacy resources. These efforts aim to improve critical thinking and media analysis skills to help Canadians identify and counter misinformation and disinformation. While the initiative has seen moderate investment from the federal government, there is growing recognition that more resources are required to scale these programs.

[45] https://policyoptions.irpp.org/magazines/march-2024/democracy-disinformation/ [visited on 21 November 2024]
[46] https://www.cbc.ca/news/politics/wechat-disinformation-operation-chong-1.6931377
[47] https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng
[48] https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html [visited on 21 November 2024]

Critical Election Incident Public Protocol

The Critical Election Incident Public Protocol is an important part of Canada's election security framework. It established a senior panel to monitor potential foreign interference during elections and inform the public if necessary. While the panel did not find sufficient grounds to issue a public warning during the 2019 or 2021 elections, the structure remains a critical component of Canada's election integrity efforts.[49] However, the Protocol has come under heavy criticism for not being transparent enough in its decision-making processes, leading to underreporting of interference threats.

The Security and Intelligence Threats to Elections Task Force

The Task Force was created to monitor and address foreign interference during federal elections. Composed of representatives from key national security agencies—CSIS, the RCMP, CSE, and Global Affairs Canada—SITE operates as a central hub for information-sharing and threat mitigation.[50]

Rapid Response Mechanism

As part of the G7, Canada established the Rapid Response Mechanism, which monitors disinformation campaigns and coordinates responses with international partners. The RRM focuses on identifying state-sponsored disinformation activities and responding quickly to limit their spread.[51]

Canadian Digital Media Research Network

The CDMRN plays a vital role in countering disinformation by providing research, tools, and training to journalists and media professionals. This network, coordinated by Canadian Heritage, collaborates with academic institutions and tech companies to track disinformation campaigns and improve media literacy across the country.[52]

Foreign Interference Commission

In response to growing concerns about foreign interference, Canada established a Foreign Interference Commission to address the influence of foreign actors in its democratic processes. Led by Justice Marie-Josée Hogue, this commission is tasked with investigating foreign efforts, particularly those from China and Russia, to interfere in Canadian elections and political life. The commission aims to increase transparency and accountability, with an interim report already released and a final report to be released by December 2024.[53]

[49] https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html [visited on 21 November 2024]
[50] https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html [visited on 21 November 2024]
[51] https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide [visited on 21 November 2024]
[52] https://www.cdmrn.ca/ [visited on 21 November 2024]
[53] https://foreigninterferencecommission.ca/reports [visited on 21 November 2024]

An Act Respecting Countering Foreign Interference

This 2024 legislation aims to fill gaps in Canada’s ability to counter foreign influence by mandating transparency in activities linked to foreign governments and actors. In addition to the Foreign Influence Transparency Registry and Commissioner (described below), the bill also enhances the powers of Canadian law enforcement and intelligence agencies to investigate and prosecute acts of foreign interference, particularly in sensitive areas. This legislation builds upon existing security frameworks but introduces new tools to address non-traditional, covert, and insidious forms of interference. Some civil society groups have expressed concerns that the broad definitions within the bill could lead to unintended impacts on free expression, especially within diaspora communities.

Foreign Influence Transparency Registry and Commissioner

The Foreign Influence Transparency Registry, established through Bill C-70, is an essential recent measure taken in Canada's effort to combat FIMI. The bill was introduced to modernize Canada's legislative toolkit in addressing the growing concerns of foreign influence in domestic politics and decision-making processes. This registry mandates individuals and organizations acting on behalf of foreign governments to register their activities, aiming to increase transparency and accountability. It targets explicitly lobbying and other political activities conducted on behalf of foreign states or entities, ensuring that the public and policymakers are informed about foreign influence operations taking place within Canadian borders.[54]

Election law updates to better combat misinformation

The Canadian government has put forward a series of proposed amendments to the Canada Elections Act aimed at enhancing electoral integrity by targeting the spread of misinformation.[55] These updates are designed to address modern challenges posed by online disinformation, especially during elections. The proposed amendments prohibit the dissemination of false information intended to mislead voters about key aspects of the voting process, such as voting locations, dates, and voter eligibility. They also impose stricter penalties for anyone found to be deliberately spreading misinformation about candidates or political parties that could influence electoral outcomes. If passed, social media platforms would also be required to act more decisively against election-related misinformation, including implementing transparency measures to prevent foreign actors from exploiting online platforms. Sub-national jurisdictions such as British Columbia have already enacted similar provisions prohibiting election-related misinformation in specific circumstances (e.g. false information about the voting process, clear misrepresentations of candidates).[56]

[54] https://www.securitepublique.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/mdrnzng-tlkt-frgn-ntrfrnc-en.aspx [visited on 21 November 2024]

[55] https://www.canada.ca/en/democratic-institutions/news/2024/03/proposed-amendments-to-the-canada-elections-act.html [visited on 21 November 2024]

[56] https://elections.bc.ca/2024-provincial-election/election-integrity/threats-to-election-integrity/ [visited on 21 November 2024]

Support for journalism

Part of counting false and malicious content in the information ecosystem is ensuring a reliable and sufficient supply of high-quality, accurate information. Recognizing the critical role that accurate information plays in countering foreign interference and disinformation campaigns more broadly, the Canadian government has invested heavily in supporting journalism. Specific initiatives include the Canadian journalism labour tax credit, digital news subscription tax credit, and the *Online News Act,* which requires large digital news intermediaries to provide cash transfers to support Canadian journalism. By some estimates, half of private journalism in Canada is now publicly supported.[57] However, this effort has not been without setbacks, including a decision by Meta to block news across Instagram and Facebook in response to the *Online News Act,* which has been disastrous for the overall visibility of Canadian journalistic content, with local news organizations particularly hard hit.[58] This has also resulted in domestic voices criticizing these efforts as undermining a free press that is willing to criticize a government that provides direct financial support.[59]

Canada faces a diverse and evolving set of foreign interference threats from adversaries such as China, Russia, and India. These actors use a combination of cyberattacks, disinformation, and the manipulation of diaspora communities to achieve their goals. While Canada has made significant strides in addressing these threats through initiatives like the Critical Election Incident Public Protocol, the Canadian Digital Media Research Network, the Rapid Response Mechanism, and The Security and Intelligence Threats to Elections Task Force, gaps remain. In the years ahead, Canada's ability to protect its democratic institutions will depend on the robustness of its response to these foreign threats.

5 Policy Recommendations

A scaled Canadian response to the threat of FIMI should consist of four complementary pillars: coordination, research, policy and public education.

5.1 Coordination

Domestic Coordination: Establish a task force for the detection and combating of FIMI

The swift identification of FIMI and adequate response to counteract it are crucial. A task force dedicated to the detection and combat of FIMI can play a critical role. This task force should function as an interdisciplinary panel of experts, regularly producing reports on current FIMI, evaluating measures, and developing strategies for mitigation. To name just a few of the relevant roles:

[57] https://thehub.ca/2023/11/30/half-of-private-canadian-journalism-could-now-be-government-supported/ [visited on 21 November 2024]
[58] https://meo.ca/work/old-news-new-reality-a-year-of-metas-news-ban-in-canada [visited on 21 November 2024]
[59] https://www.michaelgeist.ca/2023/11/on-media-bailouts-and-bias-why-government-media-policy-is-undermining-public-trust/ [visited on 21 November 2024]

- Media and communication scholars analyze the dissemination patterns of misinformation and devise strategies for effective communication and public education.
- Legal experts ensure that all measures comply with legal standards and assist in the prosecution of those responsible for disinformation.
- Psychologists and sociologists examine the psychological and social impacts of disinformation and develop approaches to enhance societal resilience.
- Technology and security experts work on the development and implementation of security measures to prevent the spread of false information.
- Education specialists design and conduct campaigns to inform the public about the dangers of disinformation and promote media literacy.

The task force could collaborate with platforms such as Facebook, X/Twitter, TikTok, and YouTube to improve mechanisms for detecting and curbing FIMI.

Germany has established such an inter ministerial task force to address the challenge of disinformation. This task force is led by the Federal Ministry of the Interior (BMI) and focuses on combating disinformation, particularly in the context of Russia's war against Ukraine. In addition, a Central Office for the Detection of Foreign Information Manipulation (ZEAM) was established within the BMI. The goal of ZEAM is to ensure the German government's ability to act against manipulation and influence campaigns directed from abroad in the information space to better protect free democratic discourse. The cooperation with the platforms has so far been sporadic in both institutions and has room for improvement.

France has also set up an agency (VIGINUM) to combat disinformation and fake news aimed at destabilizing the state. This agency is operated by the Secretariat for National Defence and Security (SGDSN) and employs approximately 60 individuals who monitor online content. The agency identifies attacks from foreign actors or organizations and works closely with politicians, diplomats, the judiciary, and the media.

International Coordination: Counter Disinformation Initiative (CDI)

Combating disinformation requires international coordination and a global platform for exchange. Through a global partnership, collective resilience against disinformation can be strengthened and the disinformation ecosystem disrupted. Additionally, information, best practices and methodologies can be shared, and policy approaches to combat these threats can be developed. Various working groups actively involve members in current policy processes, and the members can cooperate in fact-checking.

Furthermore, there is an opportunity to include the private sector alongside the governmental and public sectors to effectively combat disinformation, identify actors, and hold perpetrators accountable.

Such an initiative should not stem from an existing coalition to ensure equal opportunities for all states and sectors from the outset and to avoid existing reservations of other forums. The EU's successful establishment of platforms like EUvsDisinfo, which actively counters Russian disinformation campaigns through coordinated efforts, provides a good model for such an initiative. Another is the EU's Early Warning System which showcases effective coordination among member states in sharing information and best practices to counter FIMI threats. By fostering such international collaborations, Canada can strengthen its defences against foreign interference.

5.2 Research

A scaled national independent information ecosystem observatory

Building on the work of the information ecosystem observatories worldwide, including the Canadian Media Ecosystem Observatory, an expanded national digital media observatory should be set up immediately. Such an observatory should include large-scale online data collection and survey work, building and resourcing a network of research and civil society groups and communicating lessons learned to a broad Canadian public as well as to policymakers. The Canadian capacity for doing this work, unlike in other countries such as the US, is underfunded and has limited capacity. The result is that both public awareness of the problems of FIMI, as well as government responses to them, are too often based on research from other contexts. Canada needs an enriched domestic capacity.

As this organization becomes fully operational, it is critical that it be provided with meaningful access to data from the platforms. At the moment, there is a profound imbalance of power between the platforms that have access to data about how their products are used and the impact they are having on society and the researchers who are trying to understand these same problems with very limited data. This asymmetry needs to be addressed by mandating data sharing from the platforms to researchers in the online safety legislation. The regulatory gatekeeper would enforce mandatory platform data access and sharing requirements outlined in legislation for accredited researchers. This approach of mandated data access for researchers overseen by an independent regulatory body is modelled from the EU Digital Services Act and the European Digital Media Observatory.

The mandate of this organization should be to house the data provided by the platforms in a manner that preserves data privacy and to oversee and resource the use of these data by researchers across the country. It should encourage interdisciplinary research conducted by scholars and civil society into all aspects of the information ecosystem and communicate their findings to a very wide Canadian audience. The opportunity is significant since, unlike the EU or the US, the Canadian information ecosystem is small enough that it can be studied as a whole, and the work on Canada can be used to inform global understanding of and response to mis and disinformation.

Such a Canadian observatory could also draw inspiration from the European Framework for Countering Foreign State Influence (EFCSN) emphasis on data-sharing and transparency among member states. By establishing protocols that facilitate access to data on foreign influence operations, Canada can better equip researchers and policymakers with the necessary tools to analyze and respond to FIMI threats effectively.

A scaled Canadian incident response protocol

Information ecosystem incidents are disruptions that significantly impact the normal flow and/or integrity of information leading to potential or actual harm. The Media Ecosystem Observatory and the Canadian Digital Media Research Network's Information Incident Response Protocol could be scaled significantly, to not only better safeguard information ecosystems in like-minded democracies but to enable strategic national collaborations to address, mitigate, and respond to foreign interference and other information ecosystem threats. The incident response protocol provides rapid, research-based insights into what happened, how the incident impacted the information ecosystem, as well as attitudes and behaviours of politically influential voices and citizens-at-large. There are a variety of adjacent response protocols in the EU (e.g. the EU Crisis Protocol[60] or for cybersecurity incidents or other hybrid threats[61]) and learnings and best practices can be shared and capitalized upon.

5.3 Policy

Move swiftly on online harms policy

One of the most important things that the government can do is build a governance architecture to address the structural elements of the online harm problem. This involves adapting the risk-based regulatory models used in the EU and UK to fit the specific context and needs of Canada. This means passing *The Online Harms Act*. In short: platforms would have a duty to act responsibly. This duty would require them to conduct risk assessments on the products they offer to Canadian citizens and to follow or develop codes of practice to address risks that are identified through the risk assessment. This process would be held accountable through an independent regulator with audit powers over the platforms and the ability to penalize for non-compliance, as well as a new regime of mandated data transparency.

While the development of online harms regulations might seem adjacent to policies that more directly target FIMI, they are a pre-condition for addressing the core structural vulnerabilities in the information ecosystem that malicious actors capitalize on. While there are instances where intelligence and national security agencies will be the most appropriate vehicle for identifying and neutralizing foreign interference campaigns, the vast majority of such efforts are better addressed by making the digital ecosystem healthier, but mandating platforms to design their products to be safer and less prone to manipulation and abuse, and by ensuring a high degree of transparency over the

[60] https://home-affairs.ec.europa.eu/system/files/2023-05/EUIF_Factsheet_May_2023.pdf [visited on 21 November 2024]
[61] https://www.enisa.europa.eu/topics/incident-response [visited on 21 November 2024]

entire system so that researchers, the public and policymakers can better understand and respond to actors seeking to manipulate their behaviour.

In further developing its approach to online harms, Canada could consider integrating principles from the EFCSN, which advocates for a risk-based regulatory model tailored to counter foreign influence. This would involve establishing clear responsibilities for platforms regarding their role in mitigating foreign interference, thereby ensuring accountability for their impact on democratic processes.

Adopt the EU Code of Practice

Beyond changing the structural incentives that lead in part to the propagation of disinformation and enhance democratic vulnerability to it, Canada could embed the EU Code of Practice on Disinformation in their online harms legislation as a potential code of practice for platforms to undergo in response to risk assessments that identify the risk of disinformation. This would roughly mirror the inclusion of the code of practice in the DSA. The new strengthened code outlines 44 commitments for signatories, including demonetizing the spread of disinformation, ensuring transparency in political advertising, enhancing collaboration with fact-checkers, and improving researchers' access to data. These measures promote the integrity of the information ecosystem and serve as a blueprint for future efforts.

As the Commission on Democratic Expression concluded, "The Code would represent an efficient means of collaboration between public institutions and tech companies, especially considering that fighting disinformation must be a shared responsibility and goal. Soft law measures such as the Code of Practice on Disinformation are characterized by their flexibility and low pre-agreement transaction costs. Soft law mechanisms also facilitate systemic revisions to ensure that the provisions are constantly targeting contemporary societal issues."

Harnessing technological solutions

Technological advancements play a pivotal role in combating FIMI. Among the most significant solutions are automated detection systems that utilize algorithms and AI to identify and flag disinformation in real time. These systems analyze texts, images, and videos for signs of manipulation. Verification tools such as InVID and Factmata assist users in verifying the authenticity of images and videos, proving especially valuable in identifying deepfakes and other manipulated media.[62] Some social networks are implementing mechanisms to slow the spread of disinformation, including warning labels and reducing the visibility of suspicious content. Canada should continuously evaluate its technological approach to combating FIMI and ensure regular communication with global leaders to ensure appropriate usage.

Disinformation profiles of the actors for the regions

[62] Refer to the InVID Verification Plugin, available at: https://www.invid-project.eu/tools-and-services/invid-verification-plugin/ [visited on 21 November 2024]

To effectively counter FIMI, it is crucial to understand the unique profiles of disinformation actors in different regions. Each country faces distinct challenges and vulnerabilities that are exploited by malicious actors, primarily Russia, to spread false narratives and influence public opinion.

The proliferation of disinformation, particularly from Russian sources, poses a significant threat to democratic processes and social cohesion in European countries. Based on an analysis of disinformation campaigns in Poland, Germany, Austria, and France[63], this report proposes the development of comprehensive disinformation profiles for key actors in the region. These profiles should include:

- Primary Narratives. Identify and catalogue the main themes and messages used in disinformation campaigns. For instance, in Poland, narratives often focus on undermining Polish-Ukrainian relations and portraying Ukraine as a burden on the Polish economy. In Germany, narratives frequently question the legitimacy of supporting Ukraine and attempt to erode trust in democratic institutions.

- Dissemination Channels. Map out the primary platforms and media outlets used to spread disinformation. This includes social media platforms, state-sponsored media, and co-opted local news sources. For example, in Austria, far-right political parties and their associated media outlets have been identified as significant vectors for pro-Russian narratives.

- Target Audiences. Analyze the specific demographic groups and societal segments that are most vulnerable to or receptive to disinformation narratives. This could include groups with pre-existing anti-EU sentiments, economic concerns, or historical ties to Russia.

- Tactical Approaches: Document the specific techniques used to spread disinformation, such as the use of fake social media accounts, coordinated inauthentic behaviour, or the exploitation of legitimate concerns to introduce false narratives.

- Impact Assessment. Develop metrics to measure the reach and effectiveness of disinformation campaigns, including engagement rates on social media, shifts in public opinion, and influence on policy decisions.

5.4 Public Education

A poorly supported element of the required response to FIMI is the ways in which the public can be meaningfully brought in. Multiple Canadian government efforts to date have provided funds to civil society organizations, which is critically important but insufficient. Citizens need to also be brought into the governance decision-making and oversight system in a meaningful way. This is critical to

[63] E. Malitskaya, “Fighting Russian Disinformation in Europe,” ISE Group, 14 March 2024.

ensure that this system, which touches on core aspects of democratic rights, is embodied with the values of Canadian citizens and is a process in which they feel legitimately represented and included. This can be done in at least three ways.

Citizen Deliberation: First, regular and mandated citizen assemblies could review the terms and efficacy of digital governance. While Canadians may appear deeply divided on issues of digital governance, and particularly the regulation of speech, the two citizens assemblies as part of the Canadian Commission on Democratic Expression have demonstrated that gathering a broad cross-section of Canadians together to identify the problem and propose solutions to it generates a remarkable level of agreement. This experience is consistent with numerous successful initiatives in several EU countries, for example, the ten citizen assemblies on a range of issues, including democracy and Artificial intelligence.[64] These assemblies have demonstrated their effectiveness in fostering consensus on complex issues related to digital governance, ensuring that citizens' voices are represented in policy-making processes.

Ombudsperson: Second, there is a need for a body that can take on the concerns of citizens about what they are experiencing online and give them context and voice. The Online Harms Act suggests an Ombudsperson model for this. Such an office would compile and investigate complaints made by citizens and, when appropriate, issue public reports. The objective would be to hold both platforms and governments accountable to the citizens they serve.

Media and information literacy: Third, a serious and very well-resourced national media and information literacy program is necessary. Education is critical to bolstering resilience against disinformation, with one of the most crucial measures being the promotion of media literacy in schools and educational institutions. These programs are designed to teach critical evaluation of sources and provide practical and analytical tools for the identification of misinformation.[65]

However, it is not only the handling of media and its content that is decisive and critical but also an increased focus on geopolitical awareness. The actors, along with their strategies and objectives, should also be scrutinized and well-understood. A significant challenge lies in the training and education of teachers, ensuring they possess the necessary knowledge to impart in educational settings. Concurrently, influencers could play a pivotal role in raising awareness and acting as multipliers. The government could establish a “Social Impact Initiative” to enhance the appeal of engagement in educational efforts. Particularly active influencers could be annually honoured with a Social Impact Award.

Moreover, the older generation is often not reached through educational institutions or social media. Age-appropriate information dissemination at marketplaces, in front of supermarkets, in church

[64] Refer to: https://www.buergerrat.de/en/citizens-assemblies/eu-citizens-assemblies/ [accessed on 21 November 2024]
[65] See, for example, Strengthening Media Literacy: “Stop Fake News!”, available at: https://www.schulministerium.nrw/medienkompetenzen-staerken-stop-fake-news [visited on 21 November 2024]

communities, or at village fairs could better target this demographic. There is considerable room for improvement in this regard.

Additionally, traditional media outlets such as TV and radio advertising can contribute to raising awareness and reaching different societal groups. Governments and NGOs could launch public campaigns to educate the population about the dangers of disinformation and equip them with tools to raise awareness around the issue and better identify it.

There are already numerous information, training, and continuing education offerings in the EU and its member states. It will be more important to consolidate the various initiatives that have been developed and advanced by civil society organizations over the years and to broaden their reach. The European Digital Media Observatory (EDMO) already connects various organizations and stakeholders and provides valuable resources for enhancing media literacy among citizens through collaborative efforts among educators, policymakers, and civil society organizations. There is still a lack of creative solutions for targeted communication and outreach, like the approach of the German-American Initiative on Influencers, Disinformation, and Democracy in the Digital Age.

5.5 Prioritisation

The matrix below categorizes the policy recommendations based on their potential impact and the time needed for implementation. This impact scale is used to assess the potential effectiveness of a given recommendation in achieving its intended outcomes. Regarding the time for implementation, those marked as suitable for short-term implementation could be set up relatively quickly, within a few months, while short- to long-term recommendations could be implemented quickly but will require sustained effort over time to achieve their full impact. Those marked as being for 'long-term implementation' may take more than a year to put in place.

Figure 2 Matrix of policy recommendations

	Short-term implementation	**Short to long-term implementation**	**Long-term implementation**
High impact	Task force for the detection and combat of FIMI Scaled National Observatory	Scaled Canadian incident response protocol	Digital Literacy
Moderate impact	Online Harms Act	Counter Disinformation Initiative (CDI) Adopt the EU Code of Practice Citizen Deliberation Ombudsperson	
Low impact		Harnessing Technological Solutions	

	Disinformation Profiles of the actors for the regions

Source: Authors’ own elaboration

6 Conclusion

Like all democratic societies, Canada is faced with balancing tension between the tremendous benefits of the digital information ecosystem and the serious democratic harms that are, in part, a consequence of vulnerabilities in this same infrastructure. The problem of foreign information FIMI is not new, but the vectors, its effects, and the policies required to counter it are. A whole-of-society response requires that a broad range of actors better understand the nature of the threat, act in a concerted fashion, and coordinate and, at times collaborate on their responses:

- *Canadian policymakers* will need to depoliticize this issue, coordinate across government departments and communicate internationally;
- *Big Tech* will need to take this threat seriously and adopt rather than fight sensible public policy;
- *The media* will need to report more responsibly on the threat of foreign interference and to contextualize this threat in the changing nature of the information ecosystem;
- *Think tanks and researchers* will need to collaborate across institutional and disciplinary bounds and communicate their work to policymakers and the public in a far more responsible and concerted manner;
- *Civil society* will need to take policy on disinformation seriously and to bridge what are often fragmented efforts and
- The *broader Canadian public* will need to accept its own responsibility, to engage in the policy process, and work to become more responsible consumers and producers of information.

Canada has much to learn from the experience and initiatives of the EU. No country is alone in their fight against FIMI and learnings, lessons, and learnings should be widely shared and attended.

About the Authors

Aengus Brigdman, Director of the Media Ecosystem Observatory

Aengus Bridgman is the Director of the Media Ecosystem Observatory and an Assistant Professor at McGill University's Max Bell School of Public Policy. A leading expert on misinformation, digital activism, and digital media politics, his research has been published in top journals like The Journal of Politics and Party Politics, and featured in outlets such as The New York Times, CBC, and Vox.

Ferdinand Gehringer. Policy Advisor Cybersecurity, Konrad-Adenauer-Stiftung, Germany

Ferdinand Gehringer has worked at the Konrad-Adenauer-Stiftung since March 2021, initially as a Policy Advisor on International Law and Rule of Law, and later as a Policy Advisor on Cybersecurity. A licensed attorney and certified mediator, he studied law at Johannes Gutenberg University and Universidad de Valencia. His professional experience includes roles at Hengeler Mueller law firm, the European Parliament, Rödl & Partner in Barcelona, and the Federal Supervisory Authority for Air Navigation. He also worked for the German Embassy in Armenia and the KAS Rule of Law program in Colombia before completing his legal clerkship and state exams.

Taylor Owen, Founding Director, Center for Media, Technology and Democracy

Taylor Owen is the Beaverbrook Chair in Media, Ethics, and Communications at McGill University. He is the founding director of the Center for Media, Technology and Democracy and is an Associate Professor at the Max Bell School of Public Policy. He hosts the Big Tech podcast, is a Senior Fellow at the Center for International Governance Innovation, and serves on the SSHRC Governing Council. Previously, he was an Assistant Professor at the University of British Columbia and Research Director at Columbia's Tow Center for Digital Journalism. Owen holds a PhD from the University of Oxford and has received multiple fellowships and awards.

Alexander Romanishyn, Strategy Director, Razom We Stand

Alexander Romanishyn is an economist and policymaker, formerly Deputy Minister of Economy of Ukraine. With expertise in public policy, corporate finance, digital transformation, and resilience, he has shaped Ukraine's economic and digital strategies and contributed to its recovery. In the private sector, he led successful M&A transactions in Central and Eastern Europe with EY, Midland Group UK, and Volwest Group. Alexander holds a Master's in Finance and a Bachelor's in Economics and Business from the National University of Kyiv-Mohyla Academy and is an active mentor in the European innovation ecosystem.