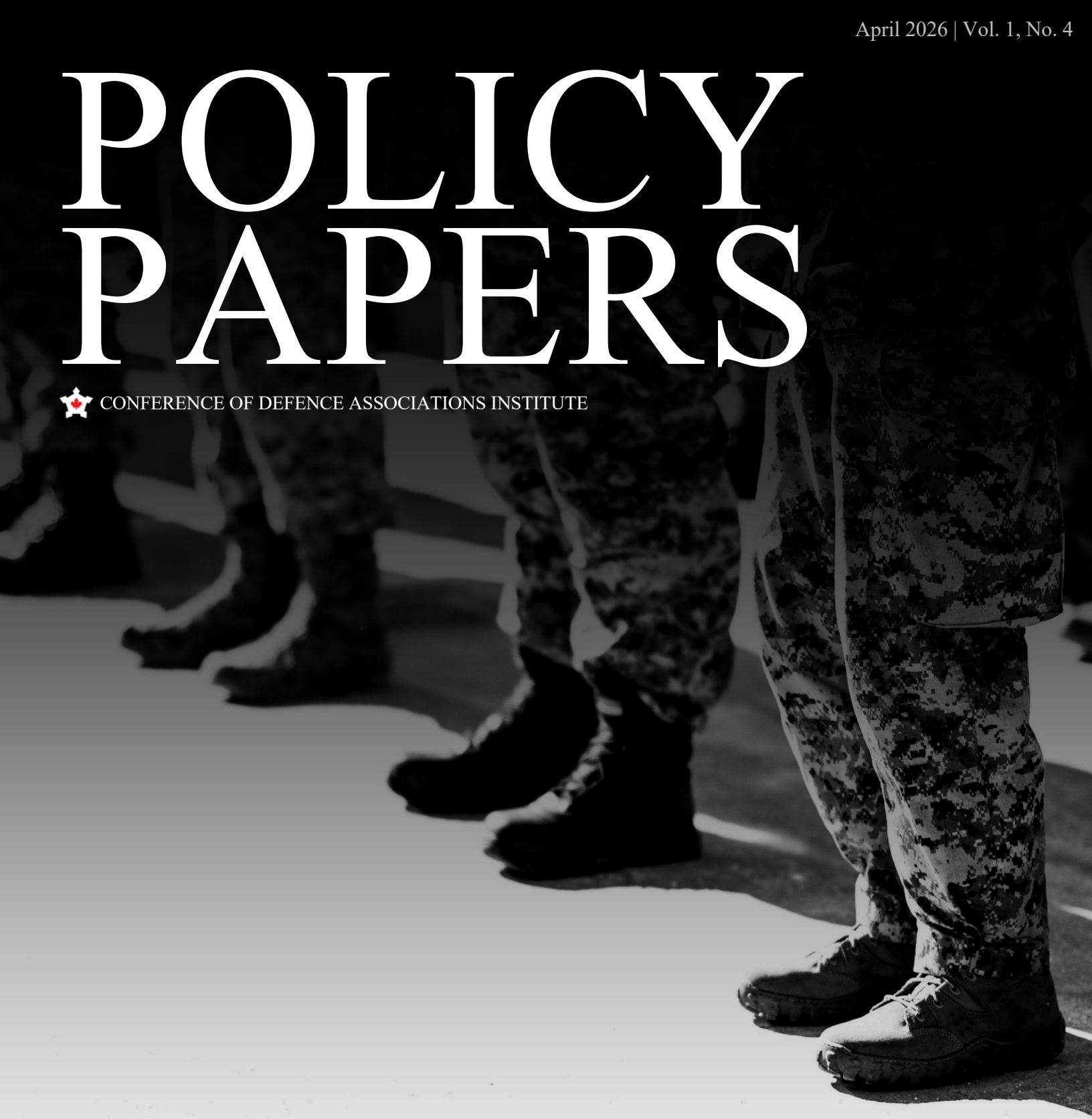
April 2026 | Vol. 1, No. 4

POLICY PAPERS

CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE



Building Whole-of-Society Resilience Against Foreign Information Manipulation and Interference in Canada

David Chobotov

POLICY PAPER

Building Whole-of-Society Resilience Against Foreign Information Manipulation and Interference in Canada

David Chobotov

April 2026

About the Author

David Chobotov is a 2025 MA graduate of the Centre for European and Eurasian Studies at the Munk School of Global Affairs and Public Policy. His master's research examined Ukrainian defence innovations, with a focus on how artificial intelligence is reshaping contemporary battlefields. He played a role in organizing the 2024 GLOBSEC Security Forum and has conducted extensive research on European security and defence policy, as well as strategies for countering foreign information manipulation and interference (FIMI).

On The Cover

Combat Camera / Flickr "Operation DISTINCTION"

Members of the Canadian Armed Forces Contingent conduct drill rehearsals in preparation for a ceremony honouring Veterans of the Persian Gulf War during Operation DISTINCTION, 35th Anniversary of the End of the Persian Gulf War, held in Halifax, from 25 February to 28 February 2026.

Photo Credit: Corporal Gregory Cole, Canadian Armed Forces Photo

Conference of Defence Associations Institute

The Conference of Defence Associations Institute is a charitable and non-partisan organisation whose mandate is to provide research support to the CDA and promote informed public debate on security and defence issues and the vital role played by the Canadian Armed Forces.

Conference of Defence Associations Institute 350 Sparks St. #701, Ottawa, ON K1R 7S8
613 236 9903 www.cdainstitute.ca

Views expressed here are those of the authors and do not necessarily reflect those of the CDA Institute.

All logos and trademarks used are the property of their respective holders. Use in this publication is under non-commercial and normative fair use provision of applicable Canadian law.

L'Institut de la Conférence des associations de défense est un organisme caritatif et non partisan dont le mandat est de fournir un soutien à la recherche à la CDA et de promouvoir un débat public éclairé sur les questions de sécurité et de défense et le rôle vital joué par les Forces armées canadiennes.

Conference of Defence Associations Institute
350, rue Sparks, #701 Ottawa (Ontario) K1R 7S8
613 236 9903 www.cdainstitute.ca

Les opinions exprimées ici sont celles des auteurs et ne reflètent pas nécessairement celles de l'Institut de la CDA.

Tous les logos et marques de commerce utilisés sont la propriété de leurs détenteurs respectifs. Leur utilisation dans cette publication est faite dans le cadre des dispositions d'utilisation équitable non commerciale de la loi canadienne applicable.

Executive Summary

Foreign Information Manipulation and Interference (FIMI) – the deliberate and coordinated efforts of state or non-state actors to manipulate information environments in pursuit of political, security, or other strategic goals – is a persistent and evolving national security threat to Canada and its national sovereignty. Canadians are largely unfamiliar with the threat of foreign information campaigns and have historically viewed Canada as an uncontested geopolitical space. The old-world order and assumptions of safety, however, are rapidly changing as Canada stands exposed within an increasingly politicized North American information environment. Relying on reactive and fragmented responses to information threats, Canada is vulnerable to the corrosive impact of false information on public trust and policy outcomes.

Canada, however, is not alone. A growing number of its allies, particularly in Europe, have developed measured, rights-respecting approaches to counter foreign information threats that balance free expression with democratic protection. Canada must learn from these lessons to hold foreign actors, very large online platforms (VLOPs), and very large online search engines (VLOSEs) – entities with more that 45 million users per month – accountable for disseminating harmful information campaigns within its borders.

This policy paper argues that Canada must elevate FIMI to a core national defence priority, and that it must adopt a portfolio of policy solutions to build durable, whole-of-society resilience against information threats. Importantly, it also proposes that measures taken to address FIMI can be considered part of national defence spending, helping Canada fulfill its North Atlantic Treaty Organization (NATO) commitment to allocate 2% of its GDP to defence.

Solutions proposed in this policy paper support four interdependent dimensions underpinning whole-of-society resilience against FIMI. The portfolio of policy solutions include recommendations (1) to safeguard democracy, diversity, and freedom of speech (the Social Dimension); (2) to adapt and respond to information threats and protect Canadian digital sovereignty (the Digital Sovereignty Dimension); (3) to protect Canadian sovereignty and national security (the Strategic Dimension); and (4) to enhance early detection, coordination, and response to information threats (the Public Safety Dimension).

1. Introduction: A Critical Moment for Canada's Information Ecosystem

Foreign information manipulation and interference (FIMI) is a national security threat to Canada, its partners, and allies (CSIS, 2025). FIMI, however, is difficult to fully define, measure, and understand; to safeguard democracy against it is to confront a vast and fragmented puzzle, one in which policymakers often fixate on individual pieces, such as social media or artificial intelligence (AI). Considering these puzzle pieces in a vacuum risks producing limited and fragmented outcomes. Accordingly, claims that any standalone policy constitutes a singular or urgent solution to FIMI warrants caution (Bateman and Jackson, 2024). This policy paper offers a nuanced understanding of foreign information manipulation. It argues that Canada must elevate FIMI to a core defence priority by adopting a portfolio of policy solutions aimed at building durable, whole-of-society resilience against information threats.

Recognized as a pressing challenge to democracy in the 2024 and 2025 World Economic Forum Global Risk Reports (WEF, 2024; WEF, 2025), Canada's efforts to address FIMI have not kept pace with its allies. It relies on reactive and fragmented responses to information threats and thus remains vulnerable to the corrosive impact of false information on public trust and policy outcomes. Importantly, Canada is not confronting the FIMI challenge alone. A growing number of its allies, particularly in Europe, have developed measured, rights-respecting approaches to counter foreign information threats that balance free expression with democratic protection. Canada therefore faces both a threat and an opportunity: to face the pitfalls of politicized inaction, and to draw strategically on allied best practices to reinforce democratic resilience before further erosion occurs.

The urgency for Canada to act is heightened by the current state of its information environment. Its closest ally and neighbour, the United States (U.S.), has increasingly becoming both a site and source of disinformation. Recent developments in U.S. policy discourse, particularly the politicization of efforts to counter FIMI (U.S. Department of State, 2025), risk normalizing the framing of counter-disinformation measures as threats to free expression rather than as safeguards for democratic integrity (The White House, 2025; Luscombe, 2025).[1] Such narratives not only undermine domestic resilience within the U.S. but also creates negative spillover effects for Canada.

Canadians are largely unacquainted with the threat of foreign information campaigns and have historically viewed Canada as an uncontested geopolitical space. Yet the old world order and assumptions of safety are rapidly changing: Canada's unequivocal support for Ukraine has made it a target of Russian disinformation operations aimed at eroding public consensus (GAC, 2024); the destabilizing rhetoric emanating from the U.S., particularly as the Trump

[1] In December 2025, the U.S. made moves to deny entry visas to fact-checkers and content moderators "responsible for, or complicit in, censorship or attempted censorship of protected expression in the US," by requiring consular officers to review resumes or LinkedIn profiles of H-1B applicants (Pamuk, 2025; U.S. Department of State, 2025).

administration sets its sight on Greenland and continues to push the narrative of Canada as a 51st state, underscores Canada's exposure within an increasingly politicized North American information environment (Djuric, 2025); and Canada's increasingly accessible Arctic frontier has heightened its strategic relevance not only to the U.S. and Russia, but to China, which views the Arctic as aligned with its own broader strategic objectives (Common, 2025; GAC, 2025). It is time for Canadians to recognize that foreign actors are both active and invested in shaping Canada's information environment to advance their strategic interests. Whole-of-society resilience against FIMI is, fundamentally, a national security issue that demands urgent attention. This policy paper advances a set of actionable recommendations aimed at addressing this challenge.

2. Background: Understanding Mis/Dis/Malinformation and Foreign Information Manipulation and Interference

To address FIMI, Canada must first contend with its framing of the issue. Precise terminology is key, as terms used to define information operations are not static but shift in response to the rapid evolution of broader information ecosystems.

In line with its NATO counterparts, the Government of Canada fully recognizes FIMI as a threat to democracy. However, it largely uses the framework of "misinformation, disinformation, and malinformation" to understand threats to its information ecosystem. Misinformation refers to false or misleading information shared without the intent to deceive (CCCS, 2024). Disinformation, by contrast, is falsified content deliberately spread with the intention to mislead and cause harm (CCCS, 2024). Malinformation is more nuanced, referring to information that stems from the truth but is exaggerated in ways that mislead or cause harm (CCCS, 2024). While mis/dis/malinformation are widely recognized as complex phenomena with deep roots in complex social, political, and economic structures (Bateman and Jackson, 2024), they have become too narrow to account for wide-ranging cross-border coordinated and intentional deception. Foreign information manipulation and interference, first coined by the European Union External Action Service (EEAS) (Debunk, 2024), has emerged as the newly accepted term to account for this discrepancy, emphasizing the deliberate and coordinated efforts of foreign state or non-state actors to manipulate the information landscapes of their adversaries for strategic gain (Cyber Risk GmbH, 2025).

At its core, FIMI threatens the safety, security, and well-being of Canadians and Canadian institutions. It is important to highlight, however, that youths, seniors, newcomers, diaspora populations, and other vulnerable groups are disproportionately affected by their impact.

According to Jon Bateman and Dean Jackson, disinformation disseminated through FIMI campaigns can be seen as jointly driven by forces of supply and demand. On the supply side, strong political

and commercial incentives motivate certain actors to produce, promote, or tolerate deceptive content, while on the demand side, psychological predispositions often make individuals receptive to false narratives (Bateman and Jackson, 2024). Emerging technologies add new layers of complexity to this dynamic, as FIMI actors have a growing range of tools at their disposal. AI-generated video and text can be used to create false content at scale, including "deepfakes" that falsely depict public figures saying or doing things they never did;[2] Large Language Models (LLMs) can be "groomed" or "seeded" with false or harmful information to influence AI outputs (Menn, 2025); "botnets" can automate social media accounts to amplify disinformation at scale (Blackbird.AI, 2025); and "doppelganger tactics" can be used to mimic trusted media brands (U.S. Cyber Command, 2024; Sessa and Miguel, 2024). All are commonplace within FIMI operations.

3. Framework: Resilience Against FIMI through a Whole-of-Society Approach

This policy paper defines resilience against FIMI as the ability of a society to prevent, resist, absorb, and recover from disruptive incidents, including hybrid threats, without compromising democratic norms, public trust, or institutional integrity (Wigell et al., 2021). Such resilience is sustained through four interdependent dimensions:

1. The Social Dimension: Safeguarding Democracy, Diversity, and Freedom of Speech.
2. The Digital Sovereignty Dimension: Adapting and Responding to Information Threats.
3. The Strategic Dimension: Protecting Canada's Sovereignty and National Security.
4. The Public Safety Dimension: Enhancing Early Detection, Coordination, and Response.

Policy solutions aimed at addressing FIMI must support these four dimensions, underscoring the need for a diversified portfolio of interventions for managing uncertainty.[3] True resilience against FIMI is only attainable with a whole-of-society approach, proactive and integrated by design, where government provides leadership, vision, and policy direction, while civil society, media, and individuals are equipped to identify and respond to foreign information threats.

4. The Canadian FIMI Threat Landscape

Historically, Canada has been targeted by FIMI operations from a variety of state actors, including China, Russia, Iran, India, and Pakistan (Hogue, 2025). These efforts

[2] For example, deepfake videos of Prime Minister Mark Carney announcing a ban on cars manufactured before the year 2000 (Saeed, 2025), or Ukrainian President Volodymyr Zelenskyy purportedly surrendering to Russia (Allyn, 2022).

[3] This four-part definition of whole-of-society resilience was adapted from the Disinformation Roundtable, a Chatham House Rule event hosted by Massey College in Spring 2025, which brought together experts from academia, the private sector, and the public sector.

can be traced to 2015, notably with Russian and Iranian "trolls" playing a central role in spreading disinformation during Canada's election period (Al-Rawi, 2021).[4] Since then, Canada has experienced widespread disinformation campaigns surrounding the 2016, 2020, and 2024 U.S. elections, the COVID-19 pandemic, the 2022 Freedom Convoy, the Russian invasion of Ukraine, and the Israel-Gaza War (Orr Bueno, 2023; CSIS, 2018; Boudreau, 2022).

More recently, Canada has faced an increasing flow of disinformation from the United States. President Donald Trump, who made 30,573 false or misleading claims over the course of his last presidency (The Washington Post, 2021), has taken major steps to dismantle both the international and domestic communities fighting FIMI. Importantly, funding cuts to the United States Agency for International Development (USAID) directly impacted NGOs and private organizations actively working to detect and counter FIMI inside and outside the country, leading many to closure (Barber et al., 2025). The Trump administration has also shuttered the State Department's last stronghold for monitoring FIMI campaigns: the Counter Foreign Information Manipulation and Interference (R/FIMI) hub, formerly known as the Global Engagement Center (U.S. Department of State, 2025). The closure of R/FIMI is highly significant, as it leaves the State Department without a dedicated resource to counter foreign information threats.[5] Canada finds itself in a position where it can no longer assume sustained U.S. leadership or benevolence on information threats, a national security issue that has traditionally been addressed through close bilateral cooperation.

Foreign information manipulation has become a strategic priority for many of Canada's adversaries, reflected in the scale and institutionalization of their financial investments. Iran's propaganda arm, for instance, had a budget of $1.26 billion USD in 2022 (U.S-China Economic and Security Review Commission, 2025). Russia allocates over $1.5 billion USD annually to foreign influence operations disseminated primarily through the GRU (Russia's military intelligence agency), the FSB (Russia's principal security agency and successor agency to the Soviet Union's KGB), and compatriot organizations outside the country (Michałowska-Kubś, 2022; Gedeon, 2025).[6] China, meanwhile, allocates over $7.9 billion USD annually on "diplomatic endeavors" – a category that includes international propaganda (PRC, 2023; U.S.-China Economic and Security Review Commission, 2025).

According to the EEAS, information is "only the bullet"; mitigating its damage requires

[4] The now defunct Russian Canadian Congress played a key role in pushing disinformation in the Canadian information ecosystem during the 2015 Canadian election.
[5] The U.S. Department of State website pages on Russian disinformation and FIMI have been taken down.
[6] Ukrainian Minister of Foreign Affairs, Andrii Sybiha, claims that Russia plans to increase funding for state propaganda by 54% in 2026 (Sybiha, 2025).

focus on the "weapon", or rather, the communication delivery method (Bolt, 2024). VLOPs and VLOSEs are central to information operations, particularly as 79.4% of Canadians are active social media users (Kemp, 2025). Financial cutbacks and policy shifts at VLOPs and VLOSEs have led to the downsizing of teams tasked with countering harmful information, weakening platform-level defences. This presents a structural vulnerability in Canada's information ecosystem, exacerbated further by the very design of social media platforms, which derive profits from advertisement revenue and specifically set out to maximize engagement, often at the expense of accuracy, and to prioritize content that elicits reactive emotions (Media Ecosystem Observatory, 2024). While the implementation of community notes, as seen on X (Twitter) and Meta-owned platforms like Facebook, attempt to address the problem, they are not a sustainable long-term solution, as they weaponize the lack of civilian experience in fact checking – work that requires both training and professional knowledge. In short, the Canadian public is ill-equipped to independently verify and debunk information, underscoring an urgent need for Canada to target the "weapon" rather than the "bullet".

5. Canada's Approach to Addressing FIMI: Strengths and Weaknesses

5.1 Strengths

5.1.1 Robust Institutions

The Royal Canadian Military Police (RCMP), the Canadian Security Intelligence Service (CSIS), Global Affairs Canada (GAC), the Rapid Response Mechanism (RRM Canada), the Communications Security Establishment (CSE), and the Security and Intelligence Threats to Elections Task Force (SITE TF) act as the primary government institutions leading Canada's efforts against FIMI:

- In 2024, the **RCMP** was allocated a budget of $49 million to "protect Canadians from harassment and intimidation", specifically from authoritarian regimes, such as Russia, China, and Iran, targeting diaspora communities in Canada (Public Safety Canada, 2024).
- **CSIS** is mandated to investigate and identify foreign disinformation campaigns within Canada, particularly those driven by foreign actors, that pose risks to national security, including attempts to influence Canada's democratic processes (CSIS, 2021; CCA, 2023).
- Through **GAC**, Canada has emerged as a key player in the G7 RRM, which coordinates efforts to identify and counter foreign threats to democracy (GAC, 2018). RRM Canada monitors the digital

information environment for foreign state-sponsored disinformation during electoral processes, particularly from Russia and China.

- GAC works in tandem with the **CSE**, which regularly publishes public and government facing reports. In its *Cyber Threats to Canada's Democratic Process: 2025 Update*, for instance, CSE documents how advanced AI tools have lowered the barrier to entry for foreign actors seeking to generate and disseminate disinformation, harass public officials, and enhance cyber-espionage campaigns in the country (CSE, 2025). In concert with the RCMP, CSIS, and GAC, CSE's Cyber Centre has developed real-time mitigation protocols to cyber threats (CSE, 2024).
- Created in 2019, the **SITE TF** is a whole-of-government working group comprised of experts from CSIS, CSE, GAC, and the RCMP, that coordinate the Government of Canada's collection and analysis efforts on federal elections (Government of Canada, 2025). Their mandate specifically includes researching foreign-origin disinformation campaigns targeting Canada.

Importantly, 2024 saw the introduction of Bill C-70: An Act Respecting Countering Foreign Interference. The bill enacted three important changes: (1) it amended the pre-internet Canadian Security Intelligence Service Act (CSIS Act), expanding CSIS' authority to disclose information and intelligence to partners outside the federal government relating to foreign influence; (2) it amended the Security of Information Act, enacting three new offences related to foreign interference (foreign-influenced or terrorist-influenced intimidation, threats or violence; commission of an indictable offence for a foreign entity; and conduct or omission for a foreign entity); and (3) it enacted the Foreign Influence Transparency and Accountability Act, which seeks to "counter efforts by foreign states or powers and their proxies to influence, in a non-transparent manner, political and governmental processes in Canada" (Government of Canada, 2024).

5.1.2 Strong Electoral Protection

The Canada Elections Act is central to safeguarding Canada's electoral process. It includes provisions to mitigate foreign election interference, particularly through campaign finance regulations that prevent foreign individuals and entities from influencing domestic elections (Government of Canada, 2000). Furthermore, the Critical Election Incident Public Protocol provides a framework for managing foreign disinformation threats during election periods (Government of Canada, 2019).

5.2 Weaknesses

5.2.1 Limited Public Awareness of Foreign Information Manipulation

Canadians remain largely unaccustomed to the threat of foreign information manipulation and continue to view Canada as an uncontested geopolitical space (CSIS, 2025).

The Government of Canada has heightened its policy awareness of foreign information manipulation in recent years, but it has yielded limited success in educating the public to its dangers. The Digital Citizen Initiative is a strong example. Through the DCI, the Government of Canada supports research initiatives and public awareness campaigns, including funding for civic, news, and digital media literacy programs (Government of Canada, 2023). While the DCI has functioned as a foundational starting point for public education on mis/dis/malinformation, the initiative has three key weaknesses:

- It lacks sustained long-term funding.
- Its structure is decentralized, with sponsored research initiatives largely operating in isolation.
- While the DCI acknowledges the importance of resilience-building, it is not supported by a coherent, centralized, national strategy for digital literacy beyond election cycles.

Furthermore, rapid fact-checking is broadly acknowledged as a short-term mitigation against harmful information (Bateman and Jackson, 2024). While the Government of Canada does publish fact-checking content through its official website, these resources – such as its page debunking disinformation of the Russo-Ukraine war – remain underpublicized and are not easily accessible to the public (Government of Canada, 2025). A nationally-coordinated response is urgent given the fact that individual Canadian citizens lack the tools to identify disinformation campaigns independently.

5.2.2 Weak Frameworks Governing VLOPs and VLOSEs

The Government of Canada currently has limited oversight and ability to ensure that the information Canadians provide to VLOPs and VLOSEs is protected, and limited ability to enforce online safety (Brassard, 2024). Canada's attempts to reign in VLOPs and VLOSEs operating within Canada have yielded limited success:

- **Bill C-27** sought to modernize Canada's privacy legislation by replacing the decades-old Personal Information Protection and Electronic Documents Act (PIPEDA) with the Consumer Privacy Protection Act (CPPA) (Government of Canada, 2022), calling on social media companies to provide clear data sharing consent, as well as data rights (including deletion). The bill also set out to introduce the Artificial Intelligence and Data Act (AIDA), which would have created a regulatory framework for AI systems used in commercial contexts (Government of Canada, 2022; Government of Canada, 2025). The bill died in January 2025 when Prime Minister Justin Trudeau prorogued Parliament.
- **Bill C-18**: The Online News Act set out to ensure fair compensation for Canadian news organizations, and inadvertently prompted social media companies (including Meta, X, and TikTok) to ban news industry from publishing

journalistic content on their platforms in Canada (Government of Canada, 2023). Canada saw a 43% drop in news media engagement in just one year, leaving other forms of inauthentic engagement to become commonplace (Media Ecosystem Observatory, 2024; Saba, 2025). Bill C-18, as a stand-alone provision, not only falls short in supporting the long-term sustainability of the Canadian news industry, it hinders public access to an open and free internet, compromising user safety and security, and ultimately strengthens the power of dominant platforms (Internet Society, 2024). In spite of Bill C-18, Canadians continue to consume news and information through social media, where a significant portion of content originates from low-credibility or unreliable news sources (Newman et al., 2024).

- **Bill C-63** aimed to enact the Online Harms Act, establishing a regulatory framework for online platforms to promote online safety and reduce harmful content (Government of Canada, 2024). This bill marked the federal government's second attempt at addressing online harms, following Bill C-36 (2021). The legislation proposed the creation of a Digital Safety Commission, an Ombudsperson, and a Digital Safety Office to regulate online platforms (Government of Canada, 2024). While these measures were a step toward increased oversight, they also sparked concerns over freedom of expression, as scholars and policy experts warned against overbroad regulatory approaches (Ahmad, 2024).
- The federal government ultimately rescinded the **Digital Services Tax** in 2025 to advance broader trade negotiations with the U.S.

5.2.3 Reactive Rather than Anticipatory Posture

While Canada has implemented a series of measures aimed at mitigating FIMI's risks through the RCMP, CSIS, GAC, RRM Canada, the CSE, and the SITE TF, its approach to addressing them has been disjointed and largely reactive – focused more on narrative tracking and monitoring rather than actively countering them or creating the information landscape hygiene conditions to minimize their impact. While these institutions each play a vital role in safeguarding Canada's information landscape by containing the impact of disinformation campaigns, containment is not enough. Canada must move away from a solely retroactive approach to managing FIMI by adopting a more proactive one. Harmful information cannot be fully eradicated, but there are proactive avenues, including: (1) the imposition of costs on FIMI actors through diplomatic, legal, and cyber countermeasures, (2) the investment in early warning systems, and (3) imposing costs on platforms that facilitate the spread of harmful information (Heer et al., 2021).

5.2.4 Cold War-Era Understanding of Psychological Operations

The Canadian Department of National Defence (DND) and the Canadian Armed Forces (CAF) play a limited role against disinformation. According to Brett Boudreau, the DND/CAF remains institutionally ill-equipped to effectively defend against mis/dis/malinformation (Bourdeau, 2023). While there is growing recognition within the organizations that Canada's information ecosystem is central to operational planning and execution, this perspective is not yet reflected in concrete strategic action by senior defence leadership. Despite possessing untapped capabilities to counter foreign information threats, the department's current posture remains constrained by legacy institutional attitudes rooted in Cold War-era conceptions of information warfare. These conceptions fail to appreciate the increase in scale and speed with which information warfare can be conducted in an increasingly fragmented information domain (Bourdeau, 2023).

6. Case Studies: How Canada's Partners and Allies Address FIMI

FIMI operations in the digital age are a nascent phenomenon. As such, it is difficult to fully determine what constitutes "best practice" for combatting them, mitigating their effect, or building societal resilience to their impact. In considering the policies employed by Canadian allies and partners, differences in legal systems and cultures may impact the appropriateness of application within the Canadian context. What works in one jurisdiction may not be legally feasible, culturally acceptable, or politically viable in another. While acknowledging that there is no universal blueprint for resilience building, and no panacea for combatting and building resilience to FIMI, this report does not seek to provide an exhaustive account of each ally's disinformation strategies. Instead, it aims to identify key lessons and policy development opportunities for Canada.

6.1 Finland Embeds Media Literacy into Education

Finland has developed one of the world's most effective counter-disinformation strategies, rooted in a strong education system and media literacy initiatives (Finland Toolbox, 2024). With a number one ranking in media literacy and resilience to the "post-truth" phenomenon (Media Literacy Index, Open Society Institute Sofia, European Policies Initiative, 2023), Finland emphasizes critical thinking as key to its national security. It integrates digital literacy into its education system, not as a stand-alone course but embedded across the curriculum, ensuring that students learn to identify misleading narratives and foreign propaganda from an early age (Mackintosh, 2019; Media Literacy Index, Open Society Institute Sofia, European Policies Initiative, 2023). Furthermore, the Finnish government actively encourages schools to partner with thinktanks and fact-checking agencies, such as Faktabaari (FactBar), which partnered with a local Helsinki school to develop a digital literacy "toolkit" for elementary to high school students learning about the European Union (E.U.) parliamentary

elections (Mackintosh, 2019). Finland's consistent high performance in media literacy indices underscores the role of education as the most sustainable long-term investment for building societal resilience against information threats.

6.2 The European Union Imposes Regulatory Constraints on VLOPs and VLOSEs

The European Union's (E.U.) Digital Services Act (DSA) is its most progressive instrument for imposing regulatory constraints on VLOPs and VLOSEs, outlining responsibilities for platforms to empower its users as well as an enforcement mechanism (European Commission, 2022). Key provisions of the DSA include (European Commission, 2025):

- Countering illegal content, goods, and services.
- Mandating control of personalized media consumption.
- Protecting minors.
- Requiring VLOPs and VLOSEs to report annually on content moderation procedures.

Fundamentally, the DSA sets out to enforce platform accountability and protect their users. X (Twitter), for instance, was fined €120 million in December 2025 for breaching its transparency obligation under the DSA (European Commission, 2025). Earlier in 2025, Apple was fined €500 million for limiting the ability of app developers to inform users about alternative purchasing options and promotions, and Meta was fined €200 million for its "pay or consent" model, requiring users to either pay for ad-free access to Facebook and Instagram or agree to receive targeted advertisements (Al Jazeera, 2025).

6.3 Ukraine Counters FIMI Through State and Civilian Led Institutions

Ukraine has emerged as a global leader in countering foreign information threats, developing a proactive and institutionalized response in the face of sustained Russian information operations since 2014 (Maksak and Chyzhova, 2024). Centralized bodies such as the International Center for Countering Disinformation (an independent entity) and the Center for Strategic Communications and Information Security (a state entity), working in close coordination with civil society, have enabled Ukraine to move beyond reactive fact-checking toward strategic narrative-building, public engagement, and innovative tools (including the use of humor) to impose reputational costs on FIMI actors (National Security and Defense Council of Ukraine, 2022; Zelensky, 2021). At the same time, Ukraine has partnered extensively with the private sector to address emerging AI-driven threats, investing in early-warning platforms and a sovereign large language model, offering Canada valuable lessons in whole-of-society coordination, technological adaptation, and institutional leadership despite differing threat contexts.

6.4 Estonia Counters FIMI Through Hybrid Threat Strategies and Public-Private Sector Collaboration

Estonia's approach to countering FIMI is shaped by its early digitalization drive and the 2007 Bronze Soldier Crisis, which marked the first major state-on-state cyberattack and catalyzed the development of a robust national cyber-defence and resilience framework that has since proved impervious to subsequent Russian attacks (Council on Foreign Relations, 2007; Juurvee and Mattiisen, 2020). Building on this experience, Estonia has become a leader in international cooperation through institutions such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDOE) and initiatives like the FREETAD project with France, pairing technical defence with strategic counter-disinformation efforts (Braghiroli, 2024). Complementing these state-level measures, Estonia emphasizes whole-of-society resilience through comprehensive media literacy education from early childhood in addition to a dynamic private sector that develops tools to counter cyber threats and disinformation (Magnuson et al., 2022). These inter-governmental partnerships as well as community level education initiatives create an environment ripe for innovation and for protection against foreign interference, including cyber-attacks and FIMI. This understanding extends throughout Estonian society into its private sector with the creation of companies such as Sentinel (deepfake detection) and the AccelerateEstonia project (a government innovation lab shaping public policy). Estonia's efforts highlight the importance of both technological defences and civic preparedness in countering FIMI.

7. Policy Options: A Portfolio Approach

The health of Canada's information ecosystem is essential for the functioning of its democratic society, security, and economic well-being. It must be protected against foreign exploitation. As no standalone policy exists to uphold the interdependent social, digital sovereignty, strategic, and public safety dimensions of resilience against FIMI described earlier, Canada must consider a portfolio of solutions to ensure a whole-of-society approach.

Notably, measures taken to address FIMI can be considered part of national defence spending, helping Canada fulfill its NATO commitment to allocate 2% of its GDP to defence. While NATO defines defence expenditures as payments made by a national government specifically to meet the needs of its armed forces, those of allies, or the Alliance, FIMI directly targets the information environment critical to military and societal resilience. Efforts to counter FIMI bolster the moral, conceptual, and physical components of fighting power, the three essential modes of military effectiveness recognized by the Canadian Military Doctrine (DND, 2009). Countering and mitigating the impact of FIMI strengthens Canada's ability to maintain public trust, cohesion, and resolve in times of crisis, factoring into NATO's broader understanding of collective defence. Therefore, investing in safeguarding

Canada's information ecosystem not only supports the CAF and DND's operational environment but also fulfills core national and allied defence obligations in the evolving security landscape.

While Canada recognizes information communication and technology (ICT) as one of its ten critical infrastructure (CI) sectors (PSC, 2025), a crucial first step for Canada is to place a renewed emphasis on its information landscape within this CI category. This would position the country to more effectively safeguard its information environment and justify greater investment in its protection, resilience, and governance. As such, a strategy that strengthens Canadian resilience to FIMI must consider the following recommendations, along with their risks and mitigations.

7.1 To Safeguard Democracy, Diversity, and Freedom of Speech, Canada Must Mandate Digital and Media Literacy Training in Schools

7.1.1 Rationale

Younger generations are disproportionately vulnerable to the damaging effects of false and harmful information (Kops et al., 2025). From a national security standpoint, the Finnish example illustrates that digital and media literacy education functions as a long-term investment in democratic resilience. Digital and media literacy is not a luxury, but a necessity for safeguarding civic engagement, public trust, and societal cohesion in the digital world (Bateman and Jackson, 2024).

Incorporating digital and media literacy as critical thinking training into school curricula will equip students with the ability to recognize harmful narratives, identify trustworthy sources, and understand how information can be manipulated by foreign actors. Finland's success in countering harmful information through education is a model Canada must replicate.

Psychological inoculation against FIMI requires embedding digital and media literacy across entire curricula; not limited to standalone units on mis/dis/malinformation but woven into every subject from statistics to civics, from grade one to graduation. Students must be continuously equipped with the tools to recognize and critically assess manipulative content that increasingly permeate digital spaces.

As education is a provincial responsibility, Canadian provinces must:

- First, define information threats within their respective provincial contexts.
- Second, support educators to recognize and respond to informational threats in their teaching environments.
- Third, play active roles in supporting school boards to collaborate proactively with media experts, educators, and NGOs in updating their curricula to help future generations navigate the complexities of digital information.

7.1.2 Risks

As Canadian school curricula continue to expand and adapt to shifting policy demands,

adding digital and media literacy requirements to the mix risks straining already overburdened education systems. Teachers face significant workload pressures and cannot reasonably be expected to deliver effective, up-to-date media and digital literacy instruction without access to standardized teaching resources, dedicated classroom time, sustained training, and ongoing professional development that keeps pace with rapidly evolving information threats and technologies.

7.1.3 Mitigation

First, Canadian provincial public services must actively recognize their information environment as critical infrastructure. A unified recognition of information integrity is essential to democratic resilience, which will be essential to secure long-term commitment and investment in media and digital literacy education.

Second, Canadian provincial education ministries must conduct research projects in their respective jurisdictions on:

1. How to best support teachers in integrating digital and media literacy into their classrooms. One potential starting point is the integration of digital and media literacy into existing civics classes. Digital and media literacy under a "civilian education" framing is a logical avenue for educating critical thinking, democratic participation, information consumption, and public discourse.
2. How to embed digital and media literacy into already packed curricula.

Third, Canadian provincial education ministries and school boards must proactively build partnerships with NGOs, research institutions, and media organizations to co-develop curricula on disinformation. Such partnerships can help translate cutting-edge FIMI research into practical, age-appropriate learning modules, co-designed with the educators who will deliver them.

7.2 To Adapt and Respond to Information Threats and Protect Canadian Digital Sovereignty, Canada Must Impose Regulatory Constraints on Very Large Online Platforms and Very Large Online Search Engines

7.2.1 Rationale

Canadian legislation must be modernized to address the challenges posed by digital media, AI, and the spread of harmful narratives through VLOPs and VLOSEs. Reforming legal structures, though difficult (Bateman and Jackson, 2024), is crucial to tackling information threats on social media while ensuring that regulations align with democratic values of free expression and transparency.

The E.U.'s DSA provides a strong example of how to impose regulatory constraints on online platforms without infringing on free speech. Canada must implement transparency requirements for social media algorithms, clearer regulations on political advertising online, and stricter penalties for foreign actors engaged in coordinated disinformation campaigns. These reforms must be designed in consultation with legal

experts, civil society, and the technology sector to balance security concerns with the protection of fundamental rights.

The Canadian Council of Academics notes in its *Vulnerable Connections* report that Canadian criminal law related to cyber-enabled crimes was originally designed for offline activities and remains ill-equipped to address the dynamics of the current digital environment (CCA, 2023). New technologies, especially those with broad information-sharing capabilities like social media algorithms, are deployed in Canada with minimal regulatory oversight, creating significant public safety and privacy risks. The rapid pace of ICT innovation means that law enforcement agencies, policymakers, and the public are forced to respond reactively to emerging forms of digital harm. As such, Canada must create a legal definition of FIMI from the perspective of the Canadian Criminal Code, recognizing the creation and dissemination of disinformation operations with the intent to deceive or cause harm as distinct offenses liable to prosecution and sanctions.

Canada must adopt a "Canadian DSA" by creating a "Code of Practice on FIMI" for VLOPs and VLOSEs to adhere to, imposing structured incentives and penalties. A VLOP and VLOSE governance regime must incentivize compliance, but curtail privileges, permissions, or access to contracts for platforms that refuse to adhere – similar to the temporary conditional public health restrictions implemented during the COVID-19 pandemic. This will preserve platform choice while ensuring that Canada's regulatory framework has real enforceability to protect Canada's information environment.

7.2.2 Risks

Adopting a Canadian VLOP and VLOSE governance regime inspired by the E.U.'s DSA carries three key risks:

- As discussed in *5.2.2 Weak Frameworks Governing VLOPs and VLOSEs,* Canada has had a poor track record of imposing regulation and accountability requirements on VLOPs and VLOSEs. Future attempts at meaningful regulation will invite retaliatory pressure from the U.S., as it has in the past.
- The U.S. is openly critical of the E.U. DSA, raising the likelihood that closer alignment with E.U.-style VLOP and VLOSE regulation could strain Canada-U.S. relations and complicate ongoing or future free trade negotiations.
- While the E.U.'s DSA represents a major step forward as a legal instrument to combat FIMI operations, its effectiveness remains difficult to fully assess given its recent implementation, with early indications of vast discrepancies in content moderation. A Cornell University study found that TikTok performs over 350 times more moderation decisions per user than X (Drolsbach and Pröllochs, 2023). The same study notes that content moderation largely targets text and video, with comparatively less focus on images and other content formats. Moreover, most moderation is automated rather than through manual intervention (though X

relies solely on non-automated methods). These variations imply a fragmented enforcement landscape, undermining the DSA's goal of harmonizing platform accountability. A further concern is the potential for overzealous enforcement and unjustified content removal. A 2024 study found that between 87.5% and 99.7% of comments deleted on Facebook and YouTube in France, Germany, and Sweden were legally permissible, indicating that platforms may be excessively censoring lawful speech to avoid regulatory penalties (The Future of Free Speech, 2024).

7.2.3 Mitigation

Canada must assemble an expert committee to conduct a legislative review of the makeup of the E.U.'s DSA to weigh what may work in the Canadian context. The political and economic risks associated with adopting a DSA-inspired framework can be mitigated through careful framing, coalition-building, and clear communication with both the public and regulated platforms:

- First, political sensitivity must be addressed by framing the proposal as multilateral alignment rather than unilateral divergence from the United States. Public messaging must emphasize that the objective is not the regulation of speech or individual expression, but holding large platforms accountable for profiting from harvesting, amplifying, and monetizing information. Anchoring this narrative in core Canadian values of fairness, accountability, and the rule of law can help defuse concerns about overreach. Importantly, this approach must be presented as allied learning rather than European imitation: the E.U. is a global agenda-setter in digital governance, and Canada can learn from its example. Framing the policy as convergence among democratic partners will reduce political friction and simultaneously draw Canada closer to the E.U. regulatory and security ecosystem.
- Second, adopting a national security framing strengthens the legitimacy of the policy. Positioning platform accountability as a response to FIMI, rather than as a cultural or free speech issue, aligns the initiative with Canada's existing national security priorities and helps justify regulatory intervention in a high-risk domain.
- Third, engagement with VLOPs and VLOSEs must stress that regulatory clarity and predictability benefit platforms over the long term by reducing legal uncertainty, harmonizing compliance expectations across jurisdictions, and creating a more stable operating environment. Finally, stronger platform transparency and accountability would also benefit DND by improving situational awareness of information threats, supporting threat attribution, and reinforcing Canada's broader defence and resilience posture in the information ecosystem.

7.3 To Protect its Sovereignty and National Security, Canada Must Establish an Independent, Non-Partisan Taskforce Dedicated to Leading Canada's Ongoing Response to FIMI

7.3.1 Rationale

Ukraine's Center for Strategic Communications and Information Security (a state entity), and the International Center for Combating Disinformation (a civil society initiative) have proven critical to the country's ability to detect and respond to FIMI operations. While Canada faces a different threat landscape to Ukraine, the establishment of a dedicated, independent, non-partisan taskforce with a clear mandate to lead Canada's approach to resilience building against FIMI and to monitor, analyze, and counter foreign information campaigns in Canada will fundamentally change its capacity to respond to information threats.[7,8] This body must not only include members of Canadian bodies currently engaged in combatting FIMI, such as RCMP, CSIS, GAC, RRM Canada, CSE, and SITE TF, but also be expanded to include academia, NGOs, media, the private sector, elected members of civil society, as well as senior officials from elected parties to ensure political and societal representation. It is important that the taskforce operate transparently, independently of government, and report directly to the Canadian Parliament, allowing it to maintain public trust and operate free from partisan bias. Furthermore, safeguards should be put in place to prevent its use as a tool for censorship.

7.3.2 Risks

Establishing an independent, non-partisan taskforce to counter and respond to FIMI threats in Canada carries four key risks.

- First, despite safeguards, such a body may be perceived by the public as a vehicle for censorship or government overreach.
- Second, the inclusion of government officials and political representatives could undermine perceptions of neutrality, creating concerns that the taskforce might be used to advance partisan interests or suppress dissenting views.
- Third, overlapping mandates with existing institutions (RCMP, GAC, CSIS, CSE, Elections Canada, and Public Safety Canada) risk duplication, bureaucratic friction, and unclear lines of responsibility.
- Fourth, operating outside formal government structures may complicate access to classified intelligence, limiting the taskforce's ability to fully assess and respond to sophisticated foreign information campaigns.

[7] As discussed earlier, a similar body was proposed in Bill C-63 in 2024, but this task force differs and does not carry the same controversies surrounding freedom of speech.
[8] NATO's StratCom division in Riga, Latvia, also provides a strong model for Canada.

7.3.3 Mitigation

The risks of establishing a non-partisan FIMI taskforce can be mitigated through clear mandate design, transparency, and institutional safeguards.

- First, the taskforce must not be set up in perpetuity. The taskforce must be created with an initial two-year term but have a renewal mechanism, leaving an open door for the Government of Canada to gradually transition the taskforce into to a permanent structure. The establishment of a permanent taskforce will not be feasible for two key reasons:

    1. Low awareness of the dangers to FIMI remains Canada's central obstacle to an effective defence. The establishment of a taskforce at this time in Canada's strategic development against FIMI may risk fostering civic complacency: believing that the burden of countering FIMI threats is wholly assumed by a central authority may undermine the whole-of-society vigilance that an effective response requires.

    2. Central offices risk being too static and cumbersome to effectively address the issues they were created for. With Canada's whole-of-society strategy against FIMI at its infancy, it is important for Canada to take incremental steps towards its development.

- Second, the taskforce must have a clear mandate to lead a proactive, integrated response to FIMI. Its mandate must encompass setting national strategic priorities, identifying and debunking viral falsehoods within hours, promoting collaboration across government, civil society, and the private sector, and ensure that counter-FIMI measures are integrated across Canada's institutions by design. This must include developing policy frameworks, improving digital and media literacy laterally, and creating rapid-response systems to address emerging threats. Public-facing outputs – such as regular threat assessments, methodology disclosures, and open engagement with civil society and media – will help build trust, normalize transparency, and anchor the taskforce's legitimacy in democratic accountability rather than executive authority.

- Third, governance structures must include fixed terms, cross-party representation, and independent oversight mechanisms (such as parliamentary reporting requirements or an external advisory board) to safeguard non-partisanship. Formal coordination agreements with existing federal agencies can clarify roles, prevent duplication, and enable structured information-sharing while preserving institutional boundaries.

7.4 To Enhance Early Detection, Coordination, and Response to Information Threats, Canada Must Commit Defence Spending to Public-Private Sector Collaboration

7.4.1 Rationale

Estonian inter-governmental partnerships and community level education initiatives have created an environment in Estonia that is ripe for innovation. Canada must strive to cultivate a similar dynamic, as investments in early warning systems capable of detecting and assessing information threats before they escalate will be key to its long-term resilience against FIMI. "FIMI favors viewing the world through the lens of threat and vulnerability and is currently locked in a reactive mode" (Bolt, 2024). Canada must break out of its reactive mode and tap into private sector talent for support. Canadian national defence outputs will be key to this end.

To drive Canada's private sector to engage in information threat and response, it must first identify which critical capabilities, information assets, and societal functions require protection from a national security perspective. Only by understanding these core vulnerabilities can early warning systems be properly designed to detect emerging threats and lay down appropriate defensive mechanisms. Without this clarity, monitoring efforts risk becoming directionless – unsure of where to look or what to look for. Furthermore, effective early warning depends on having clear mechanisms for reporting and escalating detected irregularities or attacks. Without an integrated system, Canada risks failing to distinguish between isolated incidents and coordinated, state-sponsored campaigns. This approach is consistent with the first recommendation of the Multinational Capability Development Campaign's *Countering Hybrid Warfare* report, which states that "at a minimum, national governments should conduct a self-assessment of critical functions and vulnerabilities across all sectors" (Cullen and Reichborn-Kjennerud, 2017).

7.4.2 Risks

Increasing funding to the private sector for harmful information detection and debunking efforts risks introducing a range of new challenges if such initiatives are not anchored within a coherent national resilience strategy:

- Without clear coordination, expanded private-sector involvement in Canadian information defence can lead to fragmented efforts, duplicated tools, and inconsistent standards for identifying, attributing, and responding to FIMI. Furthermore, without clear guidelines and targets, there is a danger that projects funded by government grants become unaccountable.
- Commercial incentives may skew priorities toward high-visibility or monetizable threats, rather than strategically significant but less immediately profitable, influence operations.

- Private sector engagement may lead to overreliance on private actors. This raises concerns about transparency, accountability, and data governance, particularly when proprietary methodologies limit public scrutiny or interoperability with government and civil society partners. Absent of a unifying framework, these investments risk producing isolated technical fixes rather than contributing to sustained, whole-of-society resilience against evolving information threats.

7.4.3 Mitigation

To stimulate private sector innovation against FIMI operations within Canada, increased private sector funding must be embedded within a clearly articulated national resilience framework that sets shared objectives, standards, and lines of accountability.

- First, the Canadian federal government must establish common definitions, reporting requirements, and interoperability standards to ensure that privately developed tools and analyses can be integrated across government, civil society, and allied partners.
- Second, funding mechanisms must prioritize long-term capacity-building and public-interest outcomes – including transparency, explainability, and open methodologies – rather than short-term or purely commercial metrics of success.
- Third, formal coordination platforms, including regular information-sharing forums and public–private working groups, can reduce duplication and align efforts with national security priorities.
- Fourth, oversight mechanisms and ethical safeguards must be built into funding agreements to protect civil liberties, ensure data protection, and prevent the perception that counter-FIMI efforts are being outsourced without democratic accountability.

8. Conclusion

FIMI operations are not a transient phenomenon, but a persistent and evolving threat to Canadian democracy, security, and societal resilience. Canada has made important strides in recognizing the challenges posed by FIMI, but its current frameworks remain largely reactive, fragmented, and insufficiently future-proofed. Building resilience to FIMI will require a proactive, layered, and whole-of-society approach, that considers 1) the Social Dimension (safeguarding democracy, diversity, and freedom of speech), 2) the Digital Sovereignty Dimension (adapting and responding to information threats), 3) the Strategic Dimension (protecting Canada's sovereignty and national security), and 4) the Public Safety Dimension (enhancing early detection, coordination, and response).

While this report focused on selected European allies, there remain partners and allies across Nordic and Asia-Pacific regions whose experiences offer valuable insights for Canada. Future research exploring these and other national strategies will further strengthen Canada's ability to design a

comprehensive, forward-looking resilience framework to combat FIMI.

In short, strengthening Canada's defences against FIMI will require coherent legislative action, sustained investment in media literacy and civic education, better coordination across all levels of government, regulation of media platforms, and stronger public-private partnerships. It will also require acknowledging that FIMI not only undermines electoral integrity, but erodes public trust, fractures social cohesion, and weakens democratic discourse at its core. A forward-looking national strategy – one that empowers civil society, holds foreign actors, VLOPs, and VLOSEs accountable, and promotes societal resilience – is essential for securing Canada's democratic future. Without decisive action today, Canada risks entering a prolonged era of vulnerability in an increasingly hostile and information-driven world.

References

AccelerateEstonia. 2024. *Combating Information Warfare*. AccelerateEstonia. https://accelerate.ee/projects/combating-information-warfare/

Al Jazeera. 2025. *EU slaps Meta, Apple with Nearly $800m Fines*. Al Jazeera. https://www.aljazeera.com/news/2025/4/23/eu-slaps-meta-and-apple-with-a-combined-700-million-euros-fine

Al-Rawi, Ahmed. 2021. How did Russian and Iranian Trolls' Disinformation Toward Canadian Issues Diverge and Converge? *Digital War* 2.1: 21-34. https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/COM0000016.pdf

Allyn, Bobby. 2022. *Deepfake Video of Zelenskyy Could be 'Tip of the Iceberg' in Info War, Experts Warn*. NPR. https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

Barber, Harriet; Ratcliffe, Rebecca; and Parent, Deepa. 2025. *Trump's aid cuts will lead to a surge in propaganda and misinformation, say press freedom groups*. The Guardian. https://www.theguardian.com/global-development/2025/feb/11/trump-usaid-cuts-freeze-press-freedom-ukraine-afghanistan-media-rsf

Bateman, Jon and Jackson, Dean 2024. *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en

Blackbird AI. 2025. *Social Botnets on the Rise: Countermeasures to Take*. Blackbird.AI, 2025. https://blackbird.ai/blog/social-botnets/

Bolt, Neville. 2024. Forward: Is this the Age of Disinformation or the Age of Strategic Communications? in *DEFENCE STRATEGIC COMMUNICATIONS*. NATO Strategic Communications Centre of Excellence, Volume 14, Pp. 5-25, Pp. 18. file:///Users/davidchobotov/Downloads/DSC_NATO_journal_V14_fin%20(3).pdf

Boudreau, Brett. 2022. *The Rise and Fall of Military Strategic Communications at National Defence 2015-2021: A Cautionary Tale for Canada and NATO, and a Roadmap for Reform*. Canadian Global Affairs Institute. https://www.cgai.ca/the_rise_and_fall_of_military_strategic_communications_at_national_defence_2015_2021

Bourdeau, Brett. 2023. *Understanding Department of National Defence/Canadian Armed Forces (DND/CAF) Research and Capability Needs to Deter and Limit the Impacts of (Adversary) [Dis]information.* Canadian Global Affairs Institute. https://www.cgai.ca/understanding_department_of_national_defence

Braghiroli, Stefano. 2024. *New Estonian-French Project on Disinformation Supported by NATO.* University of Tartu, Centre for Sustainable Development. https://kestlikuarengukeskus.ut.ee/en/content/new-estonian-french-project-disinformation-supported-nato

Canadian Centre for Cyber Security (CCCS). 2024. *How to identify misinformation, disinformation and malinformation*. Canadian Security Establishment Canada – CCCS. https://www.cyber.gc.ca/sites/default/files/misinformation-mesinformation-itsap.00.300-en.pdf

Canadian Security and Intelligence Service (CSIS). 2018. *Who Said What? The Security Challenges of Modern Disinformation.* Government of Canada – CSIS. https://www.canada.ca/en/security-intelligence-service/corporate/publications/who-said-what-the-security-challenges-of-modern-disinformation.html

Canadian Security and Intelligence Service Canada (CSIS). 2025. *Foreign Interference and You.* Government of Canada. https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-and-you/foreign-interference-and-you.html

Canadian Security Intelligence Service (CSIS). 2020. *Public Report 2020*. Government of Canada – CSIS. https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/CSIS-Public-Report-2020.pdf

Common, David. 2025. *As China explores the Arctic, Canada's military is preparing for confrontation.* CBC News. https://www.cbc.ca/news/canada/canada-arctic-military-exercise-sovereignty-1.7632848

Communication Security Establishment Canada (CSE). 2024. *Communications Security Establishment Annual Report 2023-2024*. Government of Canada – CSE. https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2023-2024

Communication Security Establishment Canada (CSE). 2025. *Communications Security Establishment Canada releases 2025 update to report on cyber threats to Canada's democratic process*. Government of Canada – CSE. https://www.canada.ca/en/communications-security/news/2025/03/communications-security-establishment-canada-releases-2025-update-to-report-on-cyber-threats-to-canadas-democratic-process.html

Council of Canadian Academies (CCA). 2023. *Vulnerable Connections – Expert Panel on Public Safety in the Digital Age*. CCA | CAC. https://cca-reports.ca/reports/public-safety-in-the-digital-age/

Council on Foreign Relations. 2007. *Estonian Denial of Service Incident*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/estonian-denial-service-incident

Cullen, Patrick J. and Reichborn-Kjennerud, Erik. 2017. *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.* Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Cyber Risk GmbH. 2025. *Foreign Information Manipulation and Interference (FIMI)*. Cyber Risk GmbH. https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html

Debunk. 2024. *Foreign Information Manipulation and Interference (FIMI)*. Debunk. https://www.debunk.org/fimi-foreign-information-manipulation-interference

Department of National Defence (DND). 2009. *CFJP 01 – Canadian Military Doctrine.* Government of Canada. https://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf

Djuric, Mickey. 2025. *Alberta Premier to Trump: Stay Out of Our Separatist Fight*. POLITICO. https://www.politico.com/news/2025/10/08/alberta-premier-to-trump-stay-out-of-albertas-separatist-fight-00598068

Drolsbach, Chiara and Pröllochs, Nicolas. 2023. *Content Moderation on Social Media in the EU: Insights From the DSA Transparency Database.* Cornell University, 2023. https://doi.org/10.48550/arXiv.2312.04431

European Commission. 2022. *The 2022 Code of Practice on Disinformation*. European Union, European Commission. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

European Commission. 2025. *The Impact of the Digital Services Act on Digital Platforms*. European Union, European Commission. https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

Finland Toolbox. 2024. *Media Literacy and Education in Finland.* Finland Toolbox, Ministry of Education and Culture, 2024. https://toolbox.finland.fi/life-society/media-literacy-and-education-in-finland/

Gedeon, Joseph. 2025. *Trump administration shutters US office countering foreign disinformation.* The Guardian. https://www.theguardian.com/us-news/2025/apr/16/trump-state-department-foreign-disinformation

Giovanna, Maria; and Raquel Miguel, Sessa. 2024. *The Doppelganger Case: Assessment of Platform Regulation on the EU Disinformation Environment*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/the-doppelganger-case-assessment-of-platform-regulation-on-the-eu-disinformation-environment/304

Global Affairs Canada (GAC). 2018. *Rapid Response Mechanism Canada: Global Affairs Canada*. GAC – Rapid Response Mechanism Canada. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng

Global Affairs Canada (GAC). 2024. *Global Affairs Canada Statement on Russian Disinformation.* Government of Canada. https://www.canada.ca/en/global-affairs/news/2024/10/global-affairs-canada-statement-on-russian-disinformation.html

Global Affairs Canada (GAC). *Canada targeted in a new Chinese transnational repression campaign linked to 'Spamouflage'*. GAC – Rapid Response Mechanism Canada. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2024-spamouflage.aspx?lang=eng

Government of Canada. 2000. *Canada Elections Act (S.C. 2000, c. 9).* Government of Canada. https://laws-lois.justice.gc.ca/eng/acts/e-2.01/

Government of Canada. 2019. *Critical Election Incident Public Protocol.* Government of Canada. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html

Government of Canada. 2022. *Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*. Government of Canada. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html

Government of Canada. 2023. *Digital Citizen Initiative – Online Disinformation and Other Online Harms and Threats*. Government of Canada. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html

Government of Canada. 2023. *The Online News Act*. Government of Canada. https://www.canada.ca/en/canadian-heritage/services/online-news.html

Government of Canada. 2024. *Charter Statement - Bill C-70 An Act respecting countering foreign interference*. Government of Canada. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c70.html

Government of Canada. 2025. *Countering disinformation with facts - Russian invasion of Ukraine.* Government of Canda. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng

Government of Canada. 2025. *Security and Intelligence Threats to Elections (SITE) Task Force*. Government of Canada. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html

Government of Canada. 2025. *The Artificial Intelligence and Data Act (AIDA) – Companion Document.* Government of Canada, 2025. https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

Heer, Tej; Heath, Charlee; Girling, Kimberly; and Bugg, Emma. 2021. *Misinformation in Canada: Research and Policy Options.* Evidence for Democracy. https://evidencefordemocracy.ca/wp-content/uploads/2023/06/misinformation-in-canada-evidence-for-democracy-report_.pdf

Hogue, Marie-Josée. 2025. *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions*. Government of Canada. https://foreigninterferencecommission.ca/fileadmin/report_volume_1.pdf

Internet Society. 2024. *Case Study: Canada's Online News Act Hurt Journalism, Competition, and the Internet*. Internet Society. https://www.internetsociety.org/resources/doc/2024/case-study-canadas-online-news-act-hurt-journalism-competition-and-the-internet/#:~:text=However%2C%20Canada's%202023%20passage%20of,the%20dominance%20of%20large%20platforms.

John Brassard. 2024. *Oversight of Social Media Platforms: Ensuring Privacy and Safety Online*. House of Commons Canada. https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP13390047/ethirp16/ethirp16-e.pdf

Juurvee Ivo; and Mattiisen, Mariita. 2020. *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict.* Estonia International Centre for Defence and Security.

https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf

Kemp, Simon. *Digital 2025: Canada*. Dataportal 2025. https://datareportal.com/reports/digital-2025-canada#:~:text=There%20were%2038.0%20million%20individuals,percent%20of%20the%20total%20population.

Kops, Maxime; Schittenhelm, Catherine; and Wachs, Sebastian. 2025. Young people and false information: A scoping review of responses, influential factors, consequences, and prevention programs. *Computers in Human Behavior*, Volume 169. https://www.sciencedirect.com/science/article/pii/S0747563225000974

Luscombe, Richard. 2025. *Trump Administration Moves to Deny Visas to Factcheckers and Content Moderators.* The Guardian. https://www.theguardian.com/us-news/2025/dec/05/trump-administration-us-visa-crackdown

Mackintosh, Eliza. 2019. *Finland is Winning the War on Fake News. What it's Learned May be Crucial to Western Democracy.* CNN, 2019. https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

Magnuson, Salamah; Keay, Morgan; and Metcalf, Kimberly. 2022. Countering Hybrid Warfare: Mapping Social Contracts to Reinforce Societal Resiliency in Estonia and Beyond. *Texas National Security Review*, Vol. 5, Iss. 2. http://dx.doi.org/10.26153/tsw/24028

Maksak, Hennadiy; and Chyzhova, Olga. 2024. *FIMI as Part of Russian War Machine: Ukraine's Fight*. Ukrainian PRISM Foreign Policy Council. https://prismua.org/en/english-fimi-as-part-of-russian-war-machine-ukraines-fight/

Media Ecosystem Observatory. 2024. *Old News, New Reality: A Year of Meta's News Ban in Canada.* Media Ecosystem Observatory. https://meo.ca/work/old-news-new-reality-a-year-of-metas-news-ban-in-canada

Media Literacy Index, Open Society Institute Sofia, European Policies Initiative. 2023. *The Media Literacy Index 2023: Measuring Vulnerability of Societies to Disinformation.* Media Literacy Index, Open Society Institute Sofia, European Policies Initiative, 2023. https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf

Menn, Joseph. 2025. *Russia seeds chatbots with lies. Any bad actor could game AI the same way.* The Washington Post. https://www.washingtonpost.com/technology/2025/04/17/llm-poisoning-grooming-chatbots-russia/

Michałowska-Kubś, Aleksandra. 2022. *Coining lies. Kremlin spends 1.5 Billion per year to spread disinformation and propaganda.* Debunk. https://www.debunk.org/coining-lies-state-budget-financing-of-russian-propaganda

National Security and Defense Council of Ukraine. 2021. *About Center for Countering Disinformartion*. National Security and Defense Council of Ukraine, Centre for Countering Disinformation. https://cpd.gov.ua/en/docs/about-center-for-countering-disinformartion/

NATO Allied Command Transformation. 2024. *Decoding the Information Environment: NATO's Strategic Communications Centre of Excellence*. NATO. https://www.act.nato.int/article/stratcom-coe-2024/#:~:text=The%20Centre%2C%20located%20in%20Riga,its%20Allies%2C%20and%20its%20Partners.

NATO Cooperative Cyber Defence Centre of Excellence (CCDOE). 2026. *About Us.* NATO CCDOE. https://ccdcoe.org/about-us/

Newman, Nic; Fletcher, Richard; Robertson, Craig T.; Ross Arguedas, Amy; and Kleis Nielsen, Rasmus. 2024. *Reuters Institute Digital News Report 2024.* Reuters Institute and University of Oxford. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024

Orr Bueno, Caroline. 2023. Russia's Role in the Far-Right Truck Convoy: An analysis of Russian State Media Activity Related to the 2022 Freedom Convoy. *The Journal of Intelligence, Conflict, and Warfare*, Vol. 5 No. 3. https://journals.lib.sfu.ca/index.php/jicw/article/view/5101

Pamuk, Humeyra. 2025. *Exclusive: Trump administration orders enhanced vetting for applicants of H-1B visa.* Reuters. https://www.reuters.com/world/us/trump-administration-orders-enhanced-vetting-applicants-h-1b-visa-2025-12-04/

People's Republic of China (PRC). 2023. *REPORT ON THE EXECUTION OF THE CENTRAL AND LOCAL BUDGETS FOR 2022 AND ON THE DRAFT CENTRAL AND LOCAL BUDGETS FOR 2023 – First Session of the 14th National People's Congress of the People's Republic of China*. PRC – Ministry of Finance. https://npcobserver.com/wp-content/uploads/2023/03/2023-MOF-Report.pdf

President Volodymyr Zelensky. 2021. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №106/2021 / *Presidential Decree No. 106/2021*. President of Ukraine | Volodymyr Zelensky, Official Website. https://www.president.gov.ua/documents/1062021-37421

Public Safety Canada (PSC). 2009. *Canada's Critical Infrastructure (CI).* Government of Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx

Public Safety Canada (PSC). 2024. *Parliamentary Committee Notes: Foreign Interference.* Governent of Canada – PSC. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240719/09-en.aspx

Saba, Rosa. 2025. *Local News Coverage in Canada in Steep Decline, Inviting Misinformation: Report*. CBC. https://www.cbc.ca/news/canada/newfoundland-labrador/local-news-coverage-report-1.7488636

Saeed, Henna. 2025. *PM Carney's Deepfake: How to Fact Check and Spot AI Manipulation*. CityNews Everywhere. https://kitchener.citynews.ca/2025/05/09/mark-carney-deepfake-how-to-spot-fake-videos/

Sybiha, Andrii. 2025. *Міністерство закордонних справ України / MFA of Ukraine's Post*. Facebook. https://www.facebook.com/UkraineMFA/posts/pfbid0fmRZeUe36FueMcFfHBrfJehFqkcuZ46Jd2tS5LkXgUqV7D4MxZDWxZ2UjzrcvQwl

The Future of Free Speech. 2024. *Preventing "Torrents of Hate" or Stifling Free Expression Online? An Assessment of Social Media Content Removal in France, Germany, and Sweden.* The Future of Free Speech. https://futurefreespeech.org/preventing-torrents-of-hate-or-stifling-free-expression-online/

The Washington Post. 2021. *In Four Years, President Trump Made 30,573 False or Misleading Claims*. The Washington Post. https://www.washingtonpost.com/graphics/politics/trump-claims-database/?tid=ptv_rellink

The White House. 2025. *National Security Strategy of the United States of America*. The White House. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

U.S-China Economic and Security Review Commission. 2025. *HEARING ON AN AXIS OF AUTOCRACY? CHINA'S RELATIONS WITH RUSSIA, IRAN, AND NORTH KOREA.* U.S-China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/2025-04/February_20_2025_Hearing_Transcript_0.pdf

U.S. Cyber Command. 2024. *United States Government. Russian Disinformation Campaign "DoppelGänger" Unmasked: A Web of Deception*. United States Government, U.S. Cyber Command. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/

U.S. Department of State. 2025. *Marco Rubio – Announcement of a Visa Restriction Policy Targeting Foreign Nationals Who Censor Americans.* U.S. Department of State – Press

Statement. https://www.state.gov/announcement-of-a-visa-restriction-policy-targeting-foreign-nationals-who-censor-americans

U.S. Department of State. 2025. *Marco Rubio – Protecting and Championing Free Speech at the State Department.* U.S. Department of State – Press Statement. https://www.state.gov/protecting-and-championing-free-speech-at-the-state-department

Wigell, Mikael; Mikkola, Harri; and Juntunen, Tapio. 2021. *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653632

World Economic Forum (WEF). 2024. *Global Risks 2024: Disinformation Tops Global Risks 2024 as Environmental Threats Intensify (2024).* WEF. https://www.weforum.org/press/2024/01/global-risks-report-2024-press-release/

World Economic Forum (WEF). 2025. *Global Risks Report 2025 – 20th Edition.* WEF. https://www.weforum.org/publications/global-risks-report-2025/