Centre for International
Governance Innovation

CIGI Papers No. 354 — May 2026

A Beast of a Different Kind: Malign Foreign Information Operations

Jordan Miller

Centre for International
Governance Innovation

CIGI Papers No. 354 — May 2026

A Beast of a Different Kind: Malign Foreign Information Operations

Jordan Miller

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Research Director, Digitalization, Security & Democracy Aaron Shull
Director, Programs Dianna English
Senior Program Manager Jenny Thiel
Publications Editor Lynn Schellenberg
Publications Editor Susan Bubak
Graphic Designer Sepideh Shomali

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
cigionline.org

Table of Contents

About the Author

Jordan Miller is a Ph.D. candidate at the Royal Military College of Canada and works in the defence and space industry. He is the vice-chair of the Public Policy and Advocacy Committee for Space Canada and a fellow with the Canadian Global Affairs Institute.

Acronyms and Abbreviations

AI	artificial intelligence
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
EEAS	European External Action Service
FIMI	foreign information manipulation and interference
NATO	North Atlantic Treaty Organization
NSICOP	National Security and Intelligence Committee of Parliamentarians
PDA	Psychological Defence Agency
TTPs	techniques, tactics and procedures
VIGINUM	Service de vigilance et de protection contre les ingérences numériques étrangères (service for vigilance and protection against foreign digital interference)

Executive Summary

Canada and its allies are facing an array of threats, ranging from conventional military threats of all kinds to non-kinetic threats such as cyberattacks, financial crimes, intelligence collection and information operations. Among this list, information operations are frequently lumped together with cyberattacks, because besides their potential use in cyberattacks, computers and mobile devices are also often used to connect information with audiences. However, information operations have their own characteristics, advantages and disadvantages and should be considered distinct from these other types of attacks: they are a beast of a different kind.

In the Canadian context, information operations gained public attention in 2024 with the release of two reports: the special report on election interference from the National Security and Intelligence Committee of Parliamentarians (NSICOP), and the final report of the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (informally, the Hogue report). These reports focused on discrete information campaigns targeting elections — not on information operations in a broader sense, or on better understanding how and why adversaries use them.

Some of Canada's allies have taken a different tack to analyzing information campaigns that includes identifying their messages and themes, the pathways to amplification, and other aspects of the operators' techniques, tactics and procedures (TTPs). These governments are generally seeking to understand more aspects of the attackers' approaches — the digital and psychological pathways — and taking measures.

Canada should be embracing a more comprehensive approach to understanding how information attacks work. Protecting the integrity of our elections is vital; however, the threat these operations present goes beyond such specific events. Canada's adversaries are likely to keep targeting us with information operations. To better defend against them, Canada should be learning from our allies' experience with information operations and building the necessary structures and measures to counter this distinct threat.

Introduction

Canada is facing many and varied threats in the modern world, including armed conflict and non-kinetic threats. Canada's 2024 defence policy, *Our North, Strong and Free*, emphasizes the importance of conventional military power for security and deterrence operations to protect Canadian sovereignty, including in the Arctic, and of contributions to collective security through commitments to its fellow North Atlantic Treaty Organization (NATO) members, and to Ukraine, the Baltics and partners in the Indo-Pacific (Minister of National Defence 2024). The policy also acknowledges the changing character of conflict, with "hybrid warfare" and non-kinetic activities enabled by cyber, space, artificial intelligence (AI) and quantum technologies (ibid.). Canada's earlier defence policy, *Strong, Secure, Engaged*, warned of "grey zone" and "hybrid" warfare challenges, where adversaries rely on a combination of diplomatic, informational, cyber, military and economic instruments to exert influence in pursuit of their strategic objectives while minimizing the costs and risks of conventional military confrontation (Minister of National Defence 2017).

Combining non-kinetic measures with credible military power is central to how adversaries view global competition and is likely to endure for the foreseeable future. However, not all threats to Canada are focused on military power, or even on the use of technology at all.

Foreign powers and non-state actors are actively seeking to manipulate perceptions and attitudes and to otherwise exert influence over Canadians, our politics and our institutions, through deliberate and often coordinated information operations, influence activities and propaganda campaigns. These threats know no national boundaries, and even if they often rely on technology vectors — social media, print media, television — their objective is ultimately to manipulate perceptions without the target audience being fully aware of what is happening.

Information operations, influence activities, propaganda and attempts to interfere in our politics cannot be treated as an annex or subset of other threats, such as cyberattacks, or as a companion to military operations in the "hybrid warfare" concept. While computational vectors are used to deliver information operations, computer networks are not the target: people's psyches are. Information can be used during armed conflict but is also a potent tool to shape perceptions prior to crisis or conflict. The threat from information operations is truly a "beast of a different kind" compared to the threats from military attack, terrorist attack or cyberattack. Accordingly, these operations should be treated as a distinct category of attack — even if sometimes used in combination with other attacks. Information is one type of attack in a suite of tools that adversaries use as part of war, statecraft and competition below the threshold of armed conflict.

This paper will present the case for why the challenge presented by information operations matters for Canada. It includes:

- an overview of information operations and what they intend to achieve;
- the similarities and differences between information operations and other attacks, to highlight why information operations should be treated as a distinct category from others;
- how Canada has addressed hostile information operations;
- how our allies and partners have addressed these threats; and
- the implications for Canada.

In a time when Canada is facing unprecedented threats to its sovereignty and security, preparing to defend against information operations is essential. Though billions of dollars in additional defence spending is planned, there is no single technology solution that will better defend Canada and its interests. The first step in addressing the information threat is defining it as a distinct threat and then prioritizing measures to more effectively counter the threat. Given the low costs and low barriers to entry in conducting information operations, adversaries are likely to keep using them. Canada should improve its ability to meet this threat.

The Challenge and Why This Matters

Information operations targeting Western democracies are fundamentally about eroding social cohesion, weakening public trust in institutions and undermining the notion of truth itself by blurring the lines between facts and opinion through a massive volume of information (Patterson, Gleiman and Troutman 2024). Information operations are organized and deliberate, and seek to harm democracies by sowing division and anxiety, and by exacerbating and entrenching social divisions to undermine social unity and trust (Young 2023). The fundamental challenge for Canada and its allies is twofold. First, Canada's adversaries understand the information space and how to use it to their advantage and are organized to conduct information operations at scale. Second, democracies generally do not understand the information domain as well as those that use it to target democracies, and are therefore not as well organized to counter the threat.

Why does the way we think about information operations matter? Simply, because those targeting Canada with information operations in an attempt to interfere in our politics and undermine trust in our government and institutions are likely to keep using these operations — in large part because many Western governments are not as well prepared or organized to compete in the information domain. Authoritarian governments have an inherent advantage in the information domain because they are willing to do things democracies are not, making it harder for democracies to fight back in comparable ways. Accepting the distinct nature of information operations is essential to understanding how democracies can be targeted, and to thinking about how democracies can fight back.

In addition, states being targeted with information operations have little international legal or governance-based arguments to make against those targeting them. The legal and governance frameworks that do exist — the original *Tallinn Manual*, published in 2013, and its 2017 update — focus on the laws of international conflict, use of force and state responsibility surrounding the use of cyber operations, with most countries relying

on their own state-level policies and frameworks to manage defence against information operations and cyberattacks (Munk 2024, 166–67). Originally drafted by academics in partnership with NATO, the *Tallinn Manual* was intended to provide guidelines for NATO members on how to respond to cyberattacks themselves — treating the worst as equivalent to the use of armed force — and how to exercise the right to self-defence during both peace and wartime.[1] As an academic study, the *Tallinn Manual* is non-binding. It clearly does not carry the same formal authority as an agreement or treaty among signatories. Without stronger governance or agreement from states on terms and parameters, the existing structures are unlikely to present an impediment to using information operations in international politics.

Concepts in Information Operations

Classical theory of propaganda and information operations focuses on persuasion and on convincing groups of people to embrace ideas and attitudes.

Information operations are described differently across cultures. These definitions help us understand, in part, why adversaries are often more adept at using them to target democracies: they have a better understanding of information operations' activities, value and purpose. Information operations, influence activities and propaganda are about consistent and repeated efforts to shape opinions about a group, enterprise or idea (Bernays [1928] 2005). Information operations are fundamentally about persuasion and attempting to build a consensus, often by making emotional and identity-based appeals to an audience rather than relying on facts and logic alone (Wagner and Petty 2022). A common approach in making emotionally based arguments is to appeal to the audience's identity, by invoking defining attributes and symbols of the "in group" — ethnicity, nationality, gender, political beliefs, socio-economic markers and so forth (Berger 2018). In large societies, there is rarely a *single* identity but rather many overlapping identities and sub-identities — such as being a sports fan of a particular team, calling a specific town or borough home — and each comes with a series of symbols, colloquialisms and idioms (Young 2023). Because humans in large societies have so many potential group identifiers — of varying importance — information operations can appeal to a wide range of potential emotions, even within the same sub-populations. Humans have complex and layered identities, giving many options to those targeting a group.

The vectors of information delivery are also complex. Social media campaigns have been used by foreign actors trying to influence the politics of Western countries, most notably, the efforts to influence the 2016 US presidential election. Social media is important; however, it is only one vector. The vectors for delivery include television, radio, print media, word-of-mouth and digital media, and those sources all work together to create discussion, information exchange and discourse among humans (Wanless 2025). The discourse between humans is an essential component of the information environment. It is humans' embrace of certain issues or perspectives that creates public discourse.

Sometimes foreign powers seeking to influence the public discourse of another country are not seeking to drive action or a specific outcome beyond creating a consensus position on an issue that is beneficial to that power (Jebb and Darnley-Stuart 2023). The objective does not need to be violence, or even organized action. In international politics and competition, the scope includes persuading government leaders, civil society groups or different blocs of voters (or some combination of these) to embrace beliefs and attitudes in a way that is favourable to the persuader and their objectives (Nye 2011). However, this description appears quite anodyne when compared to some authoritarian states' view that connects information concepts directly to their domestic security, or that information is simply one more tool in a never-ending competition.

Russian doctrine, for example, points to the need for information security against foreign and domestic threats, and emphasizes the importance of targeting the cognition and perceptions of the adversary, while understanding the value of information to either achieve political strategic objectives on its own, or in combination with other tools (Jonsson 2019). The Russian doctrine clearly

1 See https://ccdcoe.org/research/tallinn-manual/.

differentiates between technical means of delivery (i.e., the technology used to deliver information operations) and the psychological nature of the target: the psyche of the audience. This represents a clear understanding of the difference between the *tools* and the *objective*. The Chinese People's Liberation Army takes an even broader approach, viewing information operations and "lawfare" as means of competition through which discourse is shaped to favour the user in any context (Qiao and Wang [1999] 2015). This concept sees information operations as a distinct policy instrument and a weapons system that supports political objectives without firing a shot (Edwards and Giunta 2025).

Western perspectives generally do not separate the tools of information operations from the human target. Previous Western concepts of information operations sometimes group information technologies (cyberwarfare, electronic warfare, command-and-control resilience) in the same category as information operations (US Department of Defense 2016), combining the effector and the target. Not surprisingly, many democracies face challenges with assigning clear department and agency roles and responsibilities for the information domain (including between civilian and military organizations), with little coordination across government to counter information threats (Jones and Sinnott 2021). Part of this is inherent to democracies, marked by clear divisions of responsibility between civilian, law enforcement and intelligence, and military organizations. Authoritarians do not generally observe those types of jurisdictional divisions and prefer a "tools for the job" approach (Qiao and Wang [1999] 2015) bringing together the right capabilities — civil or military — to achieve the effect they seek, whether to protect the government domestically or to pursue its interests internationally. This structural challenge inherently disadvantages democracies at the level of execution, because there are tactics authoritarians use in the information domain that run counter to the moral and legal limitations that democracies tend to observe in armed conflict and competition (Milburn and Sinnott 2021).

Despite not typically treating information operations as a distinct threat, Western thinkers tend to have a good understanding of the specifics of how information is weaponized against democracies.

There is clear conceptual differentiation between misinformation and disinformation. Both misinformation and disinformation involve the spread of false or misleading information, and the difference lies in the intent: disinformation is the deliberate and organized spread of false information as part of a campaign to shape perception and opinions (Roozenbeek and van der Linden 2024, 9–13). A spreader of disinformation (intentionally misleading content) may be engaged in misinformation if they believe the information to be true. The difference is fundamentally about *knowingly* spreading false information *for a purpose*, versus people unknowingly spreading information that they believe is accurate.

People on the internet regularly engage in sharing false information online, whether about celebrity gossip, unverified newspaper headlines or rumours or other information. This may not be done knowingly, or with any broader political intent. We can see the outputs, but this does not mean that they have broader meaning or connection within the information environment (Wanless 2025). In a democracy, people are free to hold opinions or perspectives that others disagree with or even describe as "wrong" or based on incomplete or false information. In democracies, citizens expect a level of debate and difference in opinion, so detecting propaganda becomes a choice of finding out which open and freely available information is seeking to mislead us (Stanley 2015). The Nazi propaganda minister, Joseph Goebbels, once said that democracy's openness and freedom of speech "gave its deadly enemies the means by which it was destroyed" (quoted in Malkopoulou and Kirshner 2019). The challenge for democracies is that disinformation and misinformation present themselves in the same media ecosystem, often with no clear indication of the information being intentionally misleading or not. Moreover, the freedom of speech and freedom to consume media provides easier pathways to audiences in democracies than in authoritarian states where information is much more tightly controlled. Openness is a clear feature for citizens in democracies. By contrast, openness is viewed as a bug by authoritarians seeking to influence and interfere.

Muddying the waters somewhat, the term "fake news" is somewhat more problematic, because it can be used to refer to deliberately misleading information, mistakes made by journalists — either by publishing insufficiently investigated stories as truth, being misled by sources, or by sloppy

use of terminology with implied meaning that confuses an issue (Kapatani et al. 2021, 1305–6). The term "fake news" is therefore less useful than misinformation or disinformation because it does not clearly identify agency and intent.

Agency and intent are vital baselines to identifying what is low-quality or false information, and what is part of a deliberate operation. The European External Action Service (EEAS) uses a broader definition than simply disinformation, preferring the term "foreign information manipulation and interference" (FIMI). FIMI is defined as the "mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes" (EEAS 2025, 4). This definition clearly adds a sender: that is, the intent *belongs to someone*. This definition emphasizes that much of the FIMI approach is *not* illegal; emphasizes a pattern of behaviour connected to TTPs being used as part of FIMI efforts; and emphasizes the threat to political values, procedures and processes that the behaviour presents, and its intentional and coordinated nature (ibid.). This is a significant departure from a definition of disinformation on its own, because it combines a sender with malicious intent with the use of clear tactics to achieving the aim. This definition goes beyond simply identifying deliberate lies, and connects the information being shared to the negative effects FIMI is trying to achieve. Moreover, it emphasizes that FIMI works within the bounds of existing laws, putting limits on how criminal justice can be used as a tool to combat FIMI.

Technology has made the automation and acceleration of disinformation campaigns much easier. "Bots" are automated social media accounts masquerading as actual human users that are used to amplify specific disinformation narratives to increase the reach and number of real people who see the content, to automate escalatory or provocative responses on a divisive topic, or to harass journalists and others who are seeking to debunk disinformation campaigns (Woolley 2020, 93). Bots fulfill an important role for bad actors, because they are lower-cost than human operators, and can be used to artificially amplify content into peoples' social media feeds — making inauthentic information campaigns appear legitimate. Crucially, they are also deployed to harass and threaten people who seek to counter disinformation online, which drives self-censorship out of fear for safety. Bots enable amplification of disinformation and discourage debunking of disinformation, reducing the differential between disinformation and competing voices.

AI is also creating new possibilities for actors engaged in information operations. First, AI enables the creation of false or misleading content ("deepfakes") and enables sharing to a broader global audience by automating elements of audience targeting, automating bot networks and translation into different languages in ways that feel more sophisticated and natural than non-AI translation (Ünver 2023; Bontridder and Poullet 2021). AI image and video generators are often used for satire; however, they can be just as easily used to produce alleged content of events that never happened. Information operators can also automate bot networks using AI to amplify content so it spreads faster; use demographic data to artificially route content to more audiences than would see it otherwise; and enable more sophisticated translation so that content reaches a more global audience without needing native-speaking language profiles. AI tools do not fundamentally change why an audience likes or embraces content, but using them allows information operators to reach exponentially larger potential audiences. By sharing more content in different languages with emphases tailored to different audience subsegments' preferences, the AI-enabled campaigns may look more genuine than content that is translated literally or repeated verbatim across multiple channels.

Another risk is that AI will accelerate the spread of information or misinformation through AI searches and queries unrelated to information operations. AI tools may start providing false information to users because the large language models integrate false information into their outputs. This means that AI-enabled disinformation and misinformation could be artificially laundered into unrelated AI searches and potentially gain more credibility with audiences not participating in online discourse.

There is some hope for AI-enabled defences, however. Bot networks are more likely to be spotted by AI-enabled detection software screening for content that is either prohibited or clearly misinformation, and through detection of the bot accounts themselves because of known characteristics (Kertysova 2018). However, any AI-enabled defensive solution will require human guidance to prevent identifying false positives

for flagging and presumably for removal, and to keep pace with evolving language, slogans and images associated with information operations.

The measurement of these campaigns' performance remains a challenge. For example, data regarding the impact of the Russian 2016 US election campaign is inconclusive. There is clearly an ability to measure the outputs of information operations — that is, what content was shared, from what accounts, and the number of times it was reshared (Benkler, Faris and Roberts 2018). However, a study on the correlation between exposure to Russian information operations and voting behaviour found "no evidence of a meaningful relationship between exposure to the Russian foreign influence campaign and changes in attitudes, polarization, or voting behavior" (Eady et al. 2023, 1). It is difficult to isolate one information source from a massive ecosystem of information. Target audiences are exposed to many kinds of information — not simply that which is deliberately intended to change perceptions (Milburn and Sinnott 2021). Even if it were possible to isolate an information operation from other factors, there is no way to specifically quantify information operations. To use a military analogy: analysts can measure the impact on a target from air-dropped bombs, but they cannot measure the impact of a single social media post (Jones and Sinnott 2021).

The discussion above has clear implications for understanding information operations. The overarching purpose of information operations and propaganda remains today as outlined in classical theory: to persuade a target audience to embrace attitudes or feelings about something. Disinformation seeks to appeal to the feelings of an identity group to persuade them that false, incomplete, or misleading information is fact. Foreign actors understand that they can exacerbate existing social tensions, and therefore undermine the social cohesion and trust in institutions in target countries. Though technology is enabling content creation, translation and dissemination of content, the core purpose remains persuasion of target audiences — including by deceiving or misleading them toward attitudes that benefit the sender. The broad principles of persuasion have not been changed by technology, but the pace of information has accelerated.

Cyber Operations and Information Operations: Differentiating the Means from the Target

Similarities

Information operations have many similarities with cyberattacks or cyber operations. Both are tools of statecraft, competition and conflict; both are often intended to be unattributable to the attacker, to reduce the risk of detection and retaliation; both have global reach; both seek to exploit vulnerabilities; and both have an attack surface almost too big to fathom.

Information operations and cyberattacks are understood to be non-kinetic tools of national power: neither physically harms people nor destroys buildings and infrastructure on their own. Non-kinetic operations are generally viewed as both "cheaper" and "safer" than physical attacks. They are cheaper because although some countries make provisions for responding to cyberattacks with proportional measures,[2] there is little agreement on what constitutes proportionality. They are safer because the response to cyberattacks is not likely to take the form of missile strikes. Retaliatory cyber operations, or some other measure, are much more likely responses to a cyberattack than kinetic retaliation.

Both cyberattacks and information operations are often intended to be non-attributable. In the lead-up to the 2016 US presidential election, the Russian Federation used the "Internet Research Agency" as a proxy to target American voters with social media content using accounts meant to look like legitimate political parties and grassroots organizations while seeking to avoid accountability for them.[3] These operations were designed to look genuine (and thus unattributable to Russia) and

2 US, Bill HR 5515, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, 115th Cong, 2018 (enacted).

3 US, Senate Select Committee on Intelligence, 116th Cong, 1st Sess, *(Unclassified) Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views* (S Rep No 116-XX) (2016), online: <www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf>.

were so effective that they prompted some US citizens to demonstrate publicly after seeing the content online.[4] By pursuing non-attributable or deniable means, states and groups seek to reduce the risk of being caught and therefore reduce the risk of having costs imposed on them by a victim of attack that correctly identifies its attacker.

To minimize the likelihood of being identified and caught, both cyber operations and information operations tend to take time to conceive, plan and execute. Attackers generally balance the time required to plan and execute an operation with the magnitude of effect they can generate with it, all while remaining deniable to minimize the risk of detection and interdiction (Maschmeyer 2024). For example, the 2016 US election information campaign began putting together the operation more than a year prior to its going live, making detailed studies of target populations and key hot-button issues that would exacerbate social division.[5] Time and patience are essential for operations to remain undetected.

Cyberattacks and information operations both exploit vulnerabilities to achieve their desired ends, but in very different ways. Cyberattacks exploit gaps in network security protocols and approaches, exploit as-yet-unpatched gaps in software, or use social engineering approaches to prompt humans into violating security protocols. Information operations also exploit vulnerabilities by calling attention to social fissures or cleavages in the target society. The Soviet Union, for example, stoked anti-Semitism in West Germany in the 1950s in an attempt to re-ignite Nazi-era social divisions (Rid 2020). The Russian 2016 campaign sought to connect identity to party affiliation to deepen political divisions (Benkler, Faris and Roberts 2018). Vulnerabilities are important because they represent targeted areas against which an operation has a higher likelihood of success than either well-defended computer networks (in the case of cyberattacks) or issues where there is strong social consensus (in the case of information operations).

Lastly, both cyberattacks and information operations exist in immense ecosystems. For cybersecurity, the "attack surface" is a reference to the number of potential access points that could be exploited for offensive cyber operations. Data centres, servers, desktop computers, mobile devices of all kinds and Internet of Things connected devices are all part of that attack surface. With billions of mobile devices alone, the global aggregate attack surface already defies comprehension, and the challenge is getting bigger. As the use of AI expands, there is serious concern that the global attack surface is rapidly growing, with 99 percent of respondents in one survey reporting cyberattacks targeting their AI infrastructure (Palo Alto Networks 2025).

Information operations, similarly, have a massive attack surface. With smartphones in most pockets, information reaches people through news websites; as video content from television channels; and in media feeds — including both official media outlets and "influencers" creating content. Traditional radio, print and television provide direct content to users; add to that, word-of-mouth through social and professional networks. These vectors of information are not separate but, rather, mutually reinforcing, with traditional media content made available on provider websites, shared and reshared online, and then talked about in social circles. The information ecosystem is vast and interconnected (Wanless 2025) and provides an information attacker with many vectors into the overall ecosystem. Such large attack surfaces mean that creative attackers have many potential pathways, either to target computers and networks or to attempt to influence perceptions and attitudes.

Differences

The differences between cyber and information operations are essential to understanding why information operations truly are a beast of a different kind.

The biggest difference is that the target for cyberattacks is human cognition, not a computer network. Because the target is human and has feelings and a sense of identity, there can be demand for information operations, where there is no possible demand from the target of a cyberattack. Information operations are also an important part of the pathway to

4 *Ibid*.

5 US, Senate Select Committee on Intelligence, 116th Cong, 1st Sess, *(Unclassified) Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 5: Counterintelligence Threats and Vulnerabilities* (S Rep No 116-XX) (2016), online: <www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume5.pdf>.

radicalization, including toward terrorism. Cyberattacks cannot radicalize their targets.

Two additional differences are about time and effect. Although both cyberattacks and information operations require planning, cyberattacks tend to generate an immediate effect once they are enacted, whereas the effects of information operations are only felt over time as the target audiences' attitudes and perceptions are influenced. Similarly, once cyberattacks are detected as an attack, vulnerabilities can be quickly patched. With information operations, social fissures cannot be so easily addressed, even when an information campaign is detected.

These differences explain the core of why information operations should be treated as a distinct threat from others. Treating information operations as distinct is also essential to crafting the appropriate governance structures and policy instruments to effectively counter them.

The Human Target, Not the Computer Target

Cyber operations are typically about attacking servers, networks and digital infrastructure to achieve a specific outcome. In the context of war and competition, cyberattacks can be key enablers to a bigger operational or strategic picture. Mere hours before Russia invaded Ukraine in 2022, a cyberattack was launched against US satellite communications provider Viasat. Analysts concluded that this attack targeted ground infrastructure to disable the network of communications satellites, so as to limit Ukraine's ability to communicate on the battlefield (O'Neill 2022) and undermine their command-and-control capabilities during the vital early stages of defending against the Russian invasion. The attack impacted more than 30,000 satellite ground terminals and knocked 5,800 German power-generating wind turbines offline, temporarily removing 11 gigawatts of power-generating capability (Satter 2022). These attacks were clearly targeting physical infrastructure with the purpose of impacting Ukraine's ability to organize its defence. Whether the windmill outage was intentional or a knock-on effect is not known, but the point remains the same: computer systems were targeted to achieve a clear operational effect.

Cyber means are used to support informational objectives; however, the cyber component is the means of attack, not the target. For example, phishing attacks target individuals to compromise their personal information. This information can then be leveraged to achieve political effect. The 2016 "hack-and-leak" operation that was allegedly conducted by Russian military intelligence compromised the email account of Hillary Clinton's campaign chair for the purposes of then leaking the content specifically to sow political division.[6] The attack's objective was to influence perceptions of the Democratic candidate, and the hacking of an email account was the means of doing so.

Demand for Information Operations

Another factor that presents significant challenges for elevating the issue for policy makers and the public is that although information operations have a supply, they also have a demand. There is no demand for cyberattacks from their targets and victims, but there is a demand — unwitting, in many cases — for information operations. Information operations are crafted to resonate with existing world views, attitudes and perceptions of self-identity within a group. In that context, there can be demand for disinformation when it resonates with self-perceptions about identity (Young 2023). Identity-reinforcing content consumption and sharing is especially challenging in online spaces where algorithms prioritize showing us more of the content we like for our own consumption (Singer and Brooking 2019). Algorithmically driven content curation creates a risk of so-called "filter-bubbles" and "echo chambers," which show us only the content that aligns with our existing world views (Roozenbeek and van der Linden 2024). Disinformation may be factually untrue or misleading, but if it appeals strongly enough to emotions and identity, it may deliver a stronger sense of *meaning* than competing messages (Maan 2018).

The existence of a demand — especially if the audience is not consciously aware of it — means that malign information operations can insinuate themselves into our public discourse with the approval of the target audience. This creates opportunities for adversary information operations to exploit identity-based and emotional preferences of a target audience. In a democratic society, where people have reasonable expectation to consume the content they like, countering information for which there is a demand presents very different

6 *Ibid.*

challenges from defending against cyberattacks for which there is no demand from the target.

Vector for Radicalization and Terrorism

Information operations and propaganda play a significant role in recruitment and showing off operational successes of terrorist groups, including videos of successful attacks to connect rhetoric about attacking with actual attacks. Literature on radicalization indicates that a lack of personal significance and esteem are major contributing risk factors to making individuals vulnerable to radicalization (Kruglanski, Bélanger and Gunaratna 2019). A socially driven, slow-and-steady flow of radicalizing content is a common influence in transforming vulnerability into extremist views, with the potential for these views to cross into violent action (Braddock 2020). The pathway from vulnerability to radicalization requires an external force: either personal contact with people seeking to radicalize potential recruits, or communities of like-minded people finding each other online. The internet has allowed many kinds of social groups to find each other online and then translate those virtual social relationships into in-real-life meeting and action. This has been called the pathway from "the wires to the weeds" (Donovan, Dreyfuss and Friedberg 2022).

Groups such as the Islamic State have spent considerable time, effort and resources developing varied content, all under the umbrella of a broad narrative, that is then dispersed across print and digital channels and in different languages to reach the widest possible audience and present pathways to radicalization (Hughes 2019). There is strong evidence in the Canadian context that "self-directed" radicalization through online content is a risk. The person who shot a Canadian Army soldier performing ceremonial duties at the National War Memorial and the person who ran over Canadian Armed Forces members in St-Jean-sur-Richelieu, Quebec, were both "self-radicalized" (Gollom 2014). The person who killed 10 people in Toronto using a van said that his pathway to the "involuntary celibate" movement was largely through 4chan — an online platform known for allowing extremist content (Australian Broadcasting Corporation 2019) — not through in-person contact. The Quebec man who killed six people at a mosque was also radicalized through online content without ever making contact with like-minded people or seeking to join a group (Moore 2018). All of these individuals were apparently radicalized without being targeted by recruiters or through direct contact with people inside a group.

Individuals acting alone are examples of "stochastic terrorism." Stochastic terrorism refers to the use of mass communications pathways — including leadership statements, broadcast media, social media and so forth — to incite "random loners to commit violent or terrorist acts that are statistically predictable but individually unpredictable" (Nederveen et al. 2024, 2). The individually unpredictable and statistically predictable nature of stochastic terrorism means that groups with sufficient resources can broadcast messaging and content with some confidence that it will lead to self-directed attacks. By taking this approach, leaders and propagandists minimize the risk of arrest or of losing recruiters and facilitators to criminal conviction. A successful terrorist attack committed by a random person inspired by content and messaging also delivers the group the outcomes of fear, anxiety and possible policy overreaction that they seek to generate through violence. Without information operations, stochastic terrorism is not possible, because the concept relies on sending messages with no specific plan or person in mind. No other threat to Canada's national security can deliver the same kind of unplanned or unaccountable benefit.

Repetition and Planning

Cyber operations may also have long horizons in planning, like information operations. The Stuxnet computer worm is a cyber weapon that targeted Iran's nuclear enrichment capability and allegedly destroyed enrichment centrifuges in 2009 and 2010. However, the earliest versions of the worm are believed to have been developed in 2005 (Finkle 2013). Similar to information operations, cyber operations can take years of planning; however, the impact of cyber operations is immediate once the operation is initiated.

Information operations require repeated exposure to have effect on their target audience. Advertisers understand very well that building affinity for a product is not about showing a person one advertisement, one time. It is about the steady repetition of messages that coalesce around some central themes and constitute an overall narrative. The savviest information operators know that a general audience is made up of many subsegments, each with its own preferences and perspectives. Showing a range of similar

messages delivers an overall story or narrative to communicate something about identity and group values and preferences (Windisch 2020). Cyberattacks and computational attacks simply do not operate that way. The Viasat hack was scheduled to begin one hour before the Russian invasion of Ukraine in February 2022, calculated to generate the specific effect *immediately*. Information operations rely on much longer horizons *because* they require repetition.

States seeking to shape discourse or consensus in a target society typically expect information operations to be long-horizon tasks. Some states have sought to shape elite consensus through avenues such as think tanks, political seminars and research to influence the perspectives of decision makers (Jebb and Darnley-Stuart 2023). Social media relies on repetition and consumer scrolling to get eyes on its content. The planning for Russia's 2016 US election interference operation allegedly began in 2014, including defining clear objectives; targeting subaudiences, including different ethnic groups; devising key slogans; planning fake civil-society social media pages; and even making reconnaissance trips to the United States (Mueller 2019). This operation was clearly optimized to provide a depth and variety of content, so as to give the target audience as many data points coalescing around the same basic argument as possible.

Immediate Crisis Versus Prolonged Threat

The immediate nature of the effects of cyberattacks — often severe — means governments are forced to respond quickly. The Viasat cyberattack not only denied Ukrainians access to satellite communications, but also had immediate, tangible effects on Germany's hydro production capability. A cyberattack on hospitals in Southern Ontario put computer systems offline, delaying appointments and medical procedures — including surgeries (*CBC News* 2024). The impacts of information operations are harder to pinpoint in time and effect on perception and discourse. How seriously are the impressions of voters changed by one day of information operations? By five days? By 100 days? The slower nature of effect generation from information operations means they typically do not cause the same degree of public pressure as a discrete event with immediate effects.

In the wake of the release of the special report by NSICOP in June 2024, Canadians were seized with the issue of foreign interference targeting parliamentarians. In a subsequent survey by the Angus Reid Institute (2024), two-thirds of the Canadians polled, regardless of their political stripe, said all political party leaders should read the report, and expressed greater confidence in law enforcement (the Royal Canadian Mounted Police) and national security organizations (the Canadian Security Intelligence Service [CSIS]) than in Parliament or political parties to stop foreign interference.

In the months since, it is highly unlikely that foreign powers hostile to Canada have simply stopped all information operations targeting Canadians, yet without a great deal of public discussion, or renewed crisis over foreign interference, there has not been sustained interest from the public on the issue. Longer-term, slower-moving information operations may remain undetected or unnoticed, even while they influence the perceptions and attitudes of their target audiences. If information operations remain undetected as a deliberate foreign influence activity, they can continue to reach their target audiences without ever becoming a crisis or an incident that galvanizes public attention and elicits government response.

The Canadian Experience of Countering Foreign Information Operations

The concern over FIMI targeting Canada is known and described in unclassified, public reports from CSIS, the Communications Security Establishment Canada (CSEC), NSICOP and the subsequent Hogue inquiry into electoral interference.

In 2021, CSIS presented a report on the foreign interference threats to Canada's democratic processes, observing that clandestine and deniable campaigns of organized disinformation attempt to influence the perceptions of target voter audiences — and therefore to influence the outcome of Canadian elections (CSIS 2021). The report found that the purpose of these campaigns was to shape narratives and perception

to encourage targeted voters to vote in ways preferential to the attacker, or to suppress voter turnout for the same purpose. More active measures include cultivating relationships with elected and public officials to attempt to influence them (ibid.). This approach marked a significant departure from purely "send only" information operations in the media space, because it involved cultivating relationships through dialogue.
The 2024 CSIS annual report expanded on its description of foreign interference, including disinformation operations, as it did in 2021, and adding "transnational repression" carried out by targeting members of diaspora populations in Canada with intimidation, threats of violence and the use of proxy criminal networks to murder targets living in Canada (CSIS 2025). The report also points to the use of propaganda as part of the radicalization process for terrorist groups of all kinds, including those involved in religiously motivated violent extremism, ideologically motivated violent extremism and politically motivated violent extremism.

The nature of this threat was repeated and confirmed by NSICOP's special report on foreign interference, which stated that at least seven states are seeking to interfere in Canada's democratic processes and political institutions (NSICOP 2024). Their approaches blend traditional and social media communications with direct social contact, using civil society groups as a front, to target diaspora populations living in Canada, and by cultivating relationships under false pretenses with parliamentarians — all done through clandestine networks including the use of proxies (ibid.).

What is notable in the CSIS report is the confirmation that many states combine tools and methods to achieve their desired outcomes. Disinformation and propaganda are being used to shape perceptions and activities alongside more traditional source recruitment, and are even used to target violence against people in Canada. It also notes the centrality of propaganda to all extremist radicalization — no matter the grievance or perspective of the extremist group. Information is central to the tool kit of state and non-state malign actors and is combined with real-world actions such as transnational repression and cultivation of relationships.

CSEC describes the threats of disinformation coming from state actors in its 2024–2025 annual report. CSEC's mandate, as the signals intelligence agency for Canada, is focused on foreign threats and not domestic security; the latter falls under CSIS's mandate. CSEC describes conducting numerous foreign cyber operations in 2024–2025 to disrupt disinformation campaigns and to protect Canadians from violent extremism by targeting their digital infrastructure (CSEC 2025). CSEC's operations were presumably successful, and show that Canada is taking offensive measures more seriously. There were also second-order effects from CSEC's operations that were non-technical in nature, such as reduced credibility and influence of key campaign leaders and undermined trust and cohesion between these leaders and their followers, ultimately undermining their unity and strength (ibid).

The final report from the Hogue commission in 2025 identified that — at the time of reporting — Canada was not taking meaningful measures to improve defences, that passage of information about threats was too slow, that decision-making processes were unclear, and that communications and transparency in addressing foreign interference were lacking (Hogue 2025). Presumably, CSEC is now conducting active operations to counter the threat, given that the Hogue report's initial findings came out in 2024 — well before the release of the CSEC 2024–2025 annual report.

The content of the CSEC annual report is significant for three reasons. First, it shows that Canada is willing to engage in offensive cyber operations to counter malign foreign influence. Second, it shows that technical measures can be used to deny an attacker's use of the target country's digital infrastructure — at least for a time. Third, it also shows that countering malign influence through technical means can have a non-technical effect on an attacker. Canada is capable of characterizing and identifying a threat, communicating with the public about its severity and taking actions to counter it. The concern is that these Canadian actions are narrowly focused on major threats such as interference in elections and transnational repression. These are significant threats and must be countered. The protection of their institutions is central to Canadians' perceptions that their elections remain free and fair, that their votes will be counted, and that the peaceful transition of power is legitimate and lawful. Acting to counter threats against these institutions is necessary.

However, the findings contained in these reports do not address the role of foreign information

operations that target people who are not from a diaspora or not an elected public official (or their families), or not part of government apparatus. Broader inauthentic information amplification campaigns that seek to undermine social cohesion and stoke animosity are not addressed in these findings as thoroughly as clear attempts to target people and diasporas. This is an important point, because it implies that Canada is taking action only on *the worst* of the threats to our sovereignty and social integrity. The less acute threats — such as influencing our discourse and our political consensus — are not addressed in as much detail. It is possible that actions are being taken and not being reported in the unclassified reports; however, that remains unknown.

The following section provides a summary of how some of Canada's allies and partners have approached the information operations threat. Our allies are generally taking a more focused approach on understanding any information operation conducted by a hostile power as a threat — no matter the content or target population.

How Other Democracies Are Approaching the Problem

Other democracies have taken different approaches to countering foreign influence, with focuses that range from fostering societal resilience so as to undermine the demand for malign information, to mapping the architecture and tactics of those using malign information campaigns.

The European Union

The EEAS has taken a broad approach to identifying information operations using the FIMI model. The FIMI characterization is important, definitionally, because it connects the information specifically to attempts to manipulate and interfere in European politics — not simply to states' expression of policy positions. States engage with each other regularly, and make official statements of policy. FIMI is not that. FIMI is focused on actions that are intended to distort, confuse and manipulate perception while distracting from the true intention.

The EEAS takes a holistic approach to understanding how narratives are delivered using all available channels in the information ecosystem. These include the official state news outlets, state-linked channels and state-aligned channels that are intended to remain unattributed (EEAS 2025). This approach is significant because it acknowledges that FIMI campaigns do not rely solely on coordinated information distribution from online bot and troll networks. It is also important because it acknowledges that mass media campaigns — unaccompanied by coercive threats or transnational repression — are still malign and constitute threats to democratic societies. FIMI campaigns seek to use all elements of national informational power — from official state channels to non-attributable channels. The EEAS's approach acknowledges that foreign powers may seek to leverage all their tools in the information ecosystem to reach the biggest cross-section possible of their target population.

Another layer of analysis that FIMI provides is aiming to understand both the technical and the behavioural aspects of a FIMI campaign. This analysis seeks to identify common narratives, messages and themes that are being used in a coordinated fashion by both official and unattributable channels. It combines a mapping of the entities that are distributing the FIMI information and how they are distributing information, with an analysis of the actual content to understand the probable intentions of the state conducting FIMI in the information ecosystem (ibid.). The results of the analysis are then used to develop visual representation of how FIMI content appears in the information ecosystem and who is amplifying content and how, and gives a detailed overview of how a FIMI operation is being executed — including overt and covert sources of information. This approach provides a full understanding of the architecture of the FIMI operation. By understanding the key messages, themes and narratives being shared, we can understand *what the sender is likely trying to achieve.* Knowing the objective is vital, because it indicates the likely TTPs that entities operating FIMI campaigns are likely to use, enabling FIMI campaigns to be identified and interdicted based on those TTPs' use. This is about being able to quickly spot likely FIMI campaigns to limit their influence on the target audience — irrespective

of who that audience is. The EEAS's approach assumes that all foreign operations seeking to influence domestic perceptions, whether that intent is disguised or not, are a threat to democratic states and therefore must be mapped, unpacked and understood. This differentiator is important to understanding what adversaries are trying to achieve with their FIMI operations.

Sweden

Sweden has established a Psychological Defence Agency (PDA) focused on protecting Sweden and its interests from foreign information operations. The PDA works with military, security and intelligence, law enforcement and civil contingencies organizations to build psychological defences for government, companies and civil society against foreign information campaigns.[7] The PDA provides information for individuals, a rich data repository that shares research on previous case studies of malign information campaigns, summary reports on tactics used in malign information campaigns, and practical how-to manuals to improve resilience against malign information. The PDA's approach focuses on giving citizens and organizations the information and the tools they need to understand how malign information campaigns work, a rich compendium of how campaigns have been executed in the past, and practical guidance. The PDA does not replace activities by military, security and intelligence, or law enforcement: rather, it provides accessible information to educate the public and organizations on the nature of the threat and how it manifests — and, importantly, provides actionable advice on what to do.

The Swedish approach combines some of the components used by the EEAS (understanding how information campaigns work), with the added layer of information for the public. This approach, like the EEAS's, combines the supply and demand sides of information campaigns to deliver a holistic approach. The Swedish approach is also heavily focused on the *demand* part of information operations, by providing citizens with detailed studies on how operations have worked in the past, with practical how-to information. This approach appears designed to allow citizens to better spot the *supply* of information to undermine its *demand* at a population level.

France

France has established a dedicated agency called VIGINUM (in full, Service de vigilance et de protection contre les ingérences numériques étrangères, or service for vigilance and protection against foreign digital interference) to identify coordinated information operations targeting the country, and to then share that information with the public. The criteria VIGINUM uses to identify coordinated information operations are:

- the content of the messages in information operations;
- coordinated inauthentic behaviour (i.e., troll and bot networks);
- the foreign source — either a state, or through foreign proxies or agents; and
- information targeting national interests (institutions, health, the economy and so forth). (Gilah 2025)

This approach relies only on open-source, unclassified information and takes a "name and shame" approach that appears intended to target both the supply of information and the demand for the information by identifying it as foreign-directed. Similar to the EEAS approach, VIGINUM seeks to show the public how information campaigns are coordinated, including links to the unattributed channels being used. Coordinated foreign information campaigns generally strive to remain unattributed to make the content appear homegrown. Identifying and exposing the actual author of the campaign undermines that actor's effectiveness.

Like the EEAS approach, VIGINUM seeks to map the distribution network and identify the foreign source. It also adds two layers: identifying the content of the messages *and* the targeted sectors — focusing on the target in a societal sense, not purely a security sense. Including those layers acknowledges that not all targets will be conventional sources of national power and is an effort to understand what the messaging means. This approach is not explicitly focused on *demand*; however, by identifying the content of the messaging, it makes understanding the adversary's targeting logic more straightforward.

7 See https://mpf.se/psychological-defence-agency/about-us/our-mission.

Germany

Germany has focused its efforts on preventing interference in elections through the Central Office for Detection of Foreign Information Manipulation, operated jointly by the Federal Ministry of the Interior and Community, the Foreign Office, the Ministry of Justice, and the Press and Information Office. The German focus is on detecting digital disinformation campaigns as soon as patterns present — largely through social media and digital media sources — by leveraging cybersecurity tools and approaches.[8] This approach is narrower than the approach of the EEAS or Sweden because it is focused on detecting digital and social media campaigns specifically targeting elections. It is highly focused on the supply of disinformation, and less focused on the demand side.

Finland

Finland is often regarded as a global leader in fighting malign information campaigns, focusing on building social resilience through education and awareness of what malign information looks like. Finland has developed educational programming for its citizens — from primary school–aged to adults — that seeks to build media literacy skills so people of all ages can better understand what information operations look like (Monseau 2024). This approach is heavily focused on the *demand* side of malign information, by seeking to build resilience among the human population to prevent the supply of malign information from finding its intended audience. Finland expressed some optimism going into their 2019 elections, because it appeared that Russia was spending less effort on targeting Finnish society, according to a government official (Mackintosh 2019), which may indicate Russia recognizes Finland's high level of societal resilience, and the effectiveness of its demand-focused activities. Finland has very high rates of media and social media consumption from its population, and it also has high levels of overall education and societal trust in media outlets — the latter due, in part, to strong journalistic ethics and standards in reporting (Monseau 2024) — which have been identified as contributing factors that enable Finland's education-based resilience model to be effective (Moilanen, Hautala and Saari 2023).

8 See www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/disinformation-election-artikel.html.

Implications for Canada

Canada has taken measures to investigate interference in its elections and to defend against coordinated information campaigns. These are essential activities and should continue to evolve and expand to meet the threat, as appropriate. However, there are lessons for Canada based on the distinct nature of information operations and the experiences of other democracies.

The first and clearest lesson, is the need to treat information operations as a distinct activity from other threats such as cyber operations, military operations and terrorism. Information operations surely have linkages with other forms of war and statecraft. Our adversaries have shown their capability and willingness to combine information operations with other tools such as threats of violence and coercion as part of transnational repression. However, coercion and information are different tools, just as cyber and information are distinct tools — even though they can be combined with other tools. The often-insidious nature of information operations means they do not always generate the same level of public attention as other threats — especially in a democracy where diversity of opinion and discussion are rightly valued. This further underlines the need to draw attention to this kind of operation as distinct from others.

Second, Canada's focus on preventing interference in elections and countering radicalization to extremism are both important. However, it is clear from the lessons from the EEAS, Sweden, France and Finland that a broader approach can be taken. Canada should be sharing more public information on the specific structure, architecture and tactics used by states and organizations targeting Canada outside of elections and extremism only. Sharing more public information about how malign actors operate is important to both illustrate that the threat is real, and to provide citizens and organizations with awareness of how exactly malign actors seek to influence perception and attitudes. This is important for things such as protecting the integrity of our elections, though the nature of the threat is clearly broader than only electoral cycles.

Sharing public information should be taking place regularly, not only during election cycles or when criminal charges are laid against individuals.

Those efforts are essential, but the nature of the information threat today is ubiquitous. Criminal charges are inherently rearward looking (action after the information operation has taken place), and focusing only on electoral cycles enables malign information operations to shape discourse and consensus before and after the election — which is still unjustifiable interference in our domestic politics. The pace and speed of information in the global information ecosystem is such that focusing only on periodic problems is not enough. There is unlikely to be an end to malign information campaigns, and this means constant planning, information collection, analysis and presentation of findings to the public are required to raise overall awareness of the threat. If Finland is a guide, this approach reduces the overall supply of malign information because demand is reduced through public awareness.

Third, there should be more public discussion about the importance of taking active defensive measures to target and undermine those who are conducting information operations against Canada. This is not about fighting foreign disinformation and misinformation campaigns with our own disinformation and misinformation campaigns. Democracies cannot be good at democracy and disinformation at the same time, because disinformation represents a fundamental afront to principles of truth, accountability and the rule of law (Milburn and Sinnott 2021). Instead, defence could take the form of cyber measures against the infrastructure of information operations attackers, as outlined in the CSEC 2024–2025 annual report. It could also be taking the active information-sharing approaches used by EEAS or VIGINUM to show the architecture and tactics of those targeting Canada. By sharing this information with the public, Canada can clearly show exactly how adversaries are working to undermine our societies and institutions, which can help to reduce the demand for information operations.

In addition, Canada should consider actively confronting false narratives targeting our public discourse and debates. As a democracy, we should ensure that any counter-narrative effort should be clearly attributed to Canada, fact-based, transparent, and compliant with all applicable laws, regulations and ethical guidelines. Those countries conducting information operations against democracies rely, at least in part, on an assumption of lower awareness and organizational defences in democracies than in authoritarian states. Taking a more active role in defensive counter-narratives would help confront false or misleading information. It will also mean identifying how AI is being exploited to accelerate the pace of information operations targeting Canada, and how AI can be better used for detecting coordinated information operations — especially where bot networks, rather than genuine human engagement, are being used to artificially drive content trends.

Lastly, Canada should consider formalizing a whole-of-government approach to countering information operations. This could be something akin to the Swedish PDA's approach in sharing information and practical advice for citizens, or something conceptually similar to Canada's Integrated Threat Assessment Centre or Integrated National Security Enforcement Teams, where multiple departments and agencies contribute personnel and resources to addressing complex challenges. In the Canadian context, CSIS and CSEC have different mandates and responsibilities. We have parliamentary committees and special commissions for addressing discrete issues. However, any multi-agency approach should be broader than focusing only on threat assessment, active defensive operations or law enforcement. Addressing electoral interference or criminal prosecutions are important instruments in the information fight, but they are far from sufficient to addressing this complex threat. A detailed discussion of how to best develop a whole-of-government approach is beyond the scope of this piece and a subject that merits further research and debate. The approach taken by the PDA in Sweden is worth examining in more detail to identify lessons that could apply to Canada.

Conclusions

Technology is at the centre of current discussions about Canada's national defence and security. Canada will be buying new ships, submarines, fighter planes and early-warning aircraft, and building over-the-horizon radar systems to give us an awareness of threats. Canada will also make multi-billion-dollar investments in cybersecurity to protect the flow of information, especially as AI and quantum technologies mature and become more powerful (Department of Finance Canada 2025).

However, technology is only part of the challenge. Information operations constitute a threat distinct from others because they target the perceptions and attitudes of their audience. The NSICOP special report identified at least seven states that have targeted Canada with information operations. The threat is real.

Are those targeting Canada winning the information battle? The answer is not clear. What we do know is that those targeting Canada with information operations have clear objectives, are organized, and marshal resources and effort to deliver those operations. We also know that at least seven countries see targeting Canada as satisfying their international political objectives. Democracies are more vulnerable to information operations because of their openness and emphasis on freedom of expression. Those targeting us can use this openness against us, and they are likely pushing information operations harder than we are countering the threat.

Whatever course Canada chooses, it must begin with treating the information threat as distinct, not a subset of a different threat type. From there, any measures must balance protecting our national security and institutions with the democratic values of openness, freedom of speech and freedom of assembly. When countering foreign malign information operations undermines legitimate debate and freedoms, those seeking to target us win and Canadians lose.

This is assuredly a difficult, but essential, challenge to meet. Those targeting democracies with information operations are unlikely to stop so long as they see opportunity and payoff. For Canada and its allies, this means taking measures to identify malign information operations, to share information on their scope and scale, and to improve social resilience to undermine the demand for malign information.

Works Cited

Angus Reid Institute. 2024. "Foreign Interference: Two-thirds, including majority of CPC voters say all leaders should read NSICOP report." June 20. https://angusreid.org/foreign-interference-nsicop-trudeau-poilievre/.

Australian Broadcasting Corporation. 2019. "Toronto van attack suspect Alek Minassian tells police he is an 'incel' who accomplished 'his mission.'" September 27. www.abc.net.au/news/2019-09-27/toronto-van-attack-alek-minassian-incel-mission-new-video/11556138.

Benkler, Yochai, Robert Faris and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

Berger, J. M. 2018. *Extremism*. MIT Press.

Bernays, Edward. (1928) 2005. *Propaganda*. Mark Crispin Miller.

Bontridder, Noémi and Yves Poullet. 2021. "The role of artificial intelligence in disinformation." *Data & Policy* 3 (July): e32. https://doi.org/10.1017/dap.2021.20.

Braddock, Kurt. 2020. *Weaponized Words: The Strategic Role of Persuasion in Violent Radicalization and Counter-Radicalization*. Cambridge University Press.

CBC News. 2024. "Southwestern Ontario hospital cyberattack cost organizations at least $7.5M." August 30. www.cbc.ca/news/canada/windsor/southwestern-ontario-hospitals-cyberattack-1.7308623.

CSEC. 2025. *Annual Report: 2024–2025*. Cat No. D95-11E-PDF. Ottawa, ON: Government of Canda. https://publications.gc.ca/collections/collection_2025/cstc-csec/D95-11-2025-eng.pdf.

CSIS. 2021. *Foreign Interference Threats to Canada's Democratic Process*. Cat. No. PS74-17/2021E-PDF. July. Ottawa, ON: Government of Canada. www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html.

———. 2025. *CSIS Public Report 2024: Forty years of national security*. Cat. No. PS71E-PDF. March. Ottawa, ON: Government of Canada. www.canada.ca/content/dam/csis-scrs/images/2024publicreport/newest/Public_Report_2024-ENG.pdf.

Department of Finance Canada. 2025. *Canada Strong: Budget 2025*. Cat. No. F1-23/3E-PDF. November. Ottawa, ON: Government of Canada. https://budget.canada.ca/2025/home-accueil-en.html.

Donovan, Joan, Emily Dreyfuss and Brian Friedberg. 2022. *Meme Wars: The Untold Story of the Online Battles Upending Democracy in America*. Bloomsbury.

Eady, Gregory, Tom Paskhalis, Jan Zilinsky, Richard Bonneau, Jonathan Nagler and Joshua A. Tucker. 2023. "Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior." *Nature Communications* 14 62. https://doi.org/10.1038/s41467-022-35576-9.

Edwards, Don and Jackie Giunta. 2025. "Winning Without Fighting: Economic Power and Information Warfare (Part 2)," with David W. Barno and Rebecca Patterson, August 22, in *Irregular Warfare Podcast,* produced by Irregular Warfare Initiative, podcast 38:36. https://irregularwarfare.org/podcasts/winning-without-fighting-economic-power-and-information-warfare-part-2/.

EEAS. 2025. *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the architecture of FIMI operations.* March. Brussels, Belgium: EEAS. www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

Finkle, Jim. 2013. "Researchers say Stuxnet was deployed against Iran in 2007." Reuters, February 26. www.reuters.com/article/technology/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP/.

Gilah, Roland. 2025. "French Official Outlines Government Approach to Countering Foreign Online Operations." Institute of Global Politics, Columbia University, January 2. https://igp.sipa.columbia.edu/news/french-official-outlines-government-approach-countering-foreign-online-operations.

Gollom, Mark. 2014. "Michael Zehaf-Bibeau and Martin Couture-Rouleau: Their shared traits." *CBC News,* October 27. www.cbc.ca/news/canada/michael-zehaf-bibeau-and-martin-couture-rouleau-their-shared-traits-1.2812241.

Hogue, Marie-Josée. 2025. *Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions. Final Report. Volume 5: Recommendations to Better Protect Against Foreign Interference in Canada's Democratic Institutions and Processes.* January 28. Ottawa, ON: Privy Council Office. https://foreigninterferencecommission.ca/fileadmin/report_volume_5.pdf.

Hughes, Brian. 2019. "Band of Brothers: Marketing the Islamic State." In *The Media World of ISIS,* edited by Michael Krona and Rosemary Pennington, 145–66. Indiana University Press.

Jebb, Benjamin and Adam Darnley-Stuart. 2023. "Subversion: The Strategic Weaponization of Narratives," with Andreas Krieg and Andrew Whiskeyman, October 20, in *Irregular Warfare Podcast,* produced by Irregular Warfare Initiative and the Modern War Institute, podcast, 54:37. https://mwi.westpoint.edu/irregular-warfare-podcast-the-strategic-weaponization-of-narratives/.

Jones, Laura and Shawna Sinnott. 2021. "Information Operations for the Information Age: IO in Irregular Warfare," with Raphael Cohen and Brent Colburn, September 24, in *Irregular Warfare Podcast,* a collaboration between Modern War Institute and Princeton University's Empirical Studies of Conflict Project, podcast, 46:49. https://mwi.westpoint.edu/information-operations-for-the-information-age-io-in-irregular-warfare/.

Jonsson, Oscar. 2019. *The Russian Understanding of War: Blurring the Lines Between War and Peace*. Georgetown University Press.

Kapatani, Eleni, Androniki Christopoulou, Christos Berberidis and Vassilios Peristeras. 2021. "A systematic literature review on disinformation: Toward a unified taxonomical framework." *New Media & Society* 23 (5): 1301–26. https://doi.org/10.1177/1461444820959296.

Kertysova, Katarina. 2018. "Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered." *Security and Human Rights* 29 (1-4): 55–81. https://doi.org/10.1163/18750230-02901005.

Kruglanski, Arie W., Jocelyn J. Bélanger and Rohan Gunaratna. 2019. *The Three Pillars of Radicalization: Needs, Narratives, and Networks.* Oxford University Press.

Maan, Ajit. 2018. *Narrative Warfare.* Narrative Strategies Ink.

Mackintosh, Eliza. 2019. "Finland is winning the war on fake news. What it's learned may be crucial to Western democracy." CNN Special Report, May. https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

Malkopoulou, Anthoula and Alexander S. Kirshner, eds. 2019. *Militant Democracy and Its Critics: Populism, Parties, Extremism.* Edinburgh University Press Books.

Maschmeyer, Lennart. 2024. *Subversion: From Covert Operations to Cyber Conflict.* Oxford University Press.

Milburn, Andrew and Shawna Sinnott. 2021. "Competing for Influence: Operations in the Information Domain," with Lori Reynolds and Thomas Rid, January 16, in *Irregular Warfare Podcast,* a collaboration between Modern War Institute and Princeton University's Empirical Studies of Conflict Project, podcast, 41:09. https://mwi.westpoint.edu/competing-for-influence-operations-in-the-information-environment/.

Minister of National Defence. 2017. *Strong, Secure, Engaged: Canada's Defence Policy*. Cat. No. D2-386/2017E. Ottawa, ON: Government of Canada. www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html.

———. 2024. *Our North, Strong and Free: A Renewed Vision for Canada's Defence*. Cat. No. D2-668/2024E-PDF. Ottawa, ON: Government of Canada. www.canada.ca/en/department-national-defence/corporate/policies-standards/our-north-strong-free-renewed-vision-canada-defence.html.

Moilanen, Panu, Miriam Hautala and Dominic Saari. 2023. "Disinformation Landscape in Finland." EU DisinfoLab, May. www.disinfo.eu/wp-content/uploads/2023/05/Finland_DisinfoFactsheet.pdf.

Monseau, Marc. 2024. "Setting the Record Straight." *Scandinavian Review* (Winter): 36–51. www.amscan.org/wp-content/uploads/2025/04/Setting-the-Record-Straight-by-Marc-Monseau.pdf.

Moore, Elizabeth. 2018. "Alexandre Bissonnette's loved ones missed the signs. We can't make that mistake again." *Maclean's*, April 20. https://macleans.ca/facebook-instant-articles/alexandre-bissonnettes-loved-ones-missed-the-signs-we-cant-make-that-mistake-again/.

Mueller, Robert S. III. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Vol. 1 of 2. Washington, DC: US Department of Justice. www.justice.gov/storage/report_volume1.pdf.

Munk, Tine. 2024. *Memetic Warfare: Online Resistance in Ukraine*. Routledge.

Nederveen, Fook, Emma Zürcher, Rick Slootweg, Felicitas Hochstrasser and Stijn Hoorens. 2024. "From words to actions: An exploration and critical review of the concept of 'stochastic terrorism.'" Summary. Cambridge, UK: RAND Europe. www.rand.org/content/dam/rand/pubs/research_reports/RRA3200/RRA3232-1/RAND_RRA3232-1.summary-English.pdf.

NSICOP. 2024. *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions*. March. Ottawa, ON: Government of Canada. www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf.

Nye, Joseph S. Jr. 2011. *The Future of Power*. PublicAffairs.

O'Neill, Patrick Howell. 2022. "Russia hacked an American satellite company one hour before the Ukraine invasion." *MIT Technology Review*, May 10. www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

Palo Alto Networks. 2025. "Palto Alto Networks Report Reveals AI Is Driving a Massive Cloud Attack Surface Expansion." PR Newswire, December 16. www.prnewswire.com/news-releases/palo-alto-networks-report-reveals-ai-is-driving-a-massive-cloud-attack-surface-expansion-302642980.html.

Patterson, Rebecca, Susan Bryant, Ken Gleiman and Mark Troutman. 2024. *Winning Without Fighting: Irregular Warfare and Strategic Competition in the 21st Century*. Cambria Press.

Qiao Liang and Wang Xiangsui. (1999) 2015. *Unrestricted Warfare: China's Master Plan to Destroy America*. Translated from the Original People's Liberation Army Documents. Brattleboro, VT: Echo Point Books & Media.

Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.

Rogers, Carolyn. 2024. "Time to break the glass: Fixing Canada's productivity problem." Remarks at the Halifax Partnership, Halifax, Nova Scotia, March 26. Bank of Canada. www.bankofcanada.ca/2024/03/time-to-break-the-glass-fixing-canadas-productivity-problem/?#GAtop.

Roozenbeek, Jon and Sander van der Linden. 2024. *The Psychology of Misinformation*. Cambridge University Press.

Satter, Raphael. 2022. "Satellite outage caused 'huge loss in communications' at war's outset — Ukrainian official." Reuters, March 15. www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/.

Singer, P. W. and Emerson T. Brooking. 2019. *LikeWar: The Weaponization of Social Media*. Mariner.

Stanley, Jason. 2015. *How Propaganda Works*. Princeton University Press.

Ünver, Akın. 2023. *The Role of Technology: New Methods of Information Manipulation and Disinformation*. August. Istanbul, Türkiye: EDAM (Centre for Economics and Foreign Policy Studies). https://edam.org.tr/Uploads/Yukleme_Resim/pdf-29-08-2023-00-00-39.pdf.

US Department of Defense. 2016. "Strategy for Operations in the Information Environment." June. https://informationsecurity.info/wp-content/uploads/2021/04/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

Wagner, Benjamin C. and Richard E. Petty. 2022. "The Elaboration Likelihood Model of Persuasion: Thoughtful and Non-Thoughtful Social Influence." In *Theories in Social Psychology*, 2nd ed., edited by Derek Chadee, 120–42. John Wiley & Sons.

Wanless, Alicia. 2025. *The Information Animal: Humans, Technology and the Competition for Reality*. Oxford Academic. https://doi.org/10.1093/oso/9780197835319.001.0001.

Windisch, Beth. 2020. "Weaponized Words: The Strategic Role of Persuasion in Violent Radicalization and Counter-Radicalization," with Kurt Braddock, June 9, in *New Books in National Security*, produced by New Books Network, podcast, 57:21. https://newbooksnetwork.com/kurt-braddock-weaponized-words-cambridge-up-2020.

Woolley, Samuel C. 2020. "Bots and Computational Propaganda: Automation for Communication and Control." In *Social Media and Democracy: The State of the Field and Prospects for Reform*, edited by Nathaniel Persily and Joshua A. Tucker, 89–110. Cambridge University Press. www.cambridge.org/core/books/social-media-and-democracy/E79E2BBF03C18C3A56A5CC393698F117.

Young, Dannagal Goldthwaite. 2023. *Wrong: How Media, Politics, and Identity Drive Our Appetite for Misinformation*. Johns Hopkins University Press.

CIGI

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
cigionline.org