CASIS Essay Competition 2022 Submission

The Disinformation Case for a New Approach to Canadian Intelligence

By Leuven Wang

Undergraduate, University of Toronto

H.B.Sc. Statistics, Political Science, and Philosophy

To any fairly informed observer of current global political affairs, disinformation hardly needs an introduction. Successive news stories on Russian disinformation operations or the phenomenon of "fake news" have habituated our general awareness of the problem, one of many in a slate of foreign interference tools applied against democratic nations.

Yet simultaneously, society's understanding disinformation is often incomprehensive and caught in domestic political disputes. In a world where it is increasingly easy and attractive to fling accusations amidst a breaking reality, the risk of democratic discourse descending into a cynical spiral of "he said, she said" is not an unreasonable hypothetical. Consider, additionally, the blurred lines between malicious foreign disinformation operations versus misguided yet sincere domestic propellants. This equation of inherently distorted nature sums up to a messy issue, to say the least.

But disinformation is a disease with known treatments. And in applying them, the Canadian government now has an opportunity not just to defend but revitalise democracy. In this essay, I will argue that disinformation is a problem uniquely positioned to intersect with and be driven by other elements in Canada's threat environment. This overlap, along with its philosophically fundamental enmity to democracy, makes it an issue that requires a **whole-of-society response**. A potential Canadian solution to disinformation is one factor, among many, that calls for an integrated government strategy to national security that **works in tandem with foreign and domestic policy**. The intelligence community will continue to lead the charge in identifying and disrupting disinformation threats, but this integrated approach changes the elements and attributes expected from them. As part of this new strategy, intelligence policymakers have a rare opportunity to effectively counter disinformation and rethink their focus on **integration**, **policy transparency, the implementation of new technologies,** and other aspects of their service. Central to the success of this endeavour will be **a fresh, strategically conscious, diverse, and interdisciplinary workforce** dedicated to protecting Canada.

What I hope this essay will convey is the need for a new comprehensive approach to Canadian national security policy from the perspective of tackling disinformation. This is not to say that there are no other arguments for a similar policy. Indeed, I expect the increased frequency of other horrid threat amalgamations and the growing interconnectivity of societies to require more integrated solutions all around.

Our study will take the following path. First, I will examine the nature of disinformation and illustrate what makes it a unique constituent of the current threat matrix facing Canada. Secondly, I will discuss some theoretical and practised countermeasures to disinformation while being cognisant of Canada's unique composition and placement in the global order. I will then apply this newly gathered framework of solutions to determine the implications for a new Canadian national security strategy, including what roles intelligence services will play. In doing so, I aim to shed light on the essential elements and attributes that intelligence agencies will need to shift to today, to prepare for a new tomorrow.

The Nature of Disinformation

Foreign disinformation is not a new threat. There is a rich history of Soviet foreign information manipulation operations dating throughout the Cold War and falling under the

moniker “active measures”. This notably included projects like Operation INFEKTION, which tried to convince people that AIDS was invented by the American military[1], or the appropriation of peace movements through front organisations like the World Peace Council[2]. What is new is using the internet through social media, junk journalism, and other means of mass, decentralised communication to push these foreign-generated narratives. Several factors now compound the threat: its ease to manufacture relative to the scale of its outreach[3], the difficulty in tracing a source of origin[4], and the facilitation of echo chambers through algorithms[5] and communities[6] that tailor to personal content preferences. The barriers to launching effective disinformation campaigns have lowered while their audience and targeting capabilities have increased. Russia is thus far from the only offender. A 2019 Oxford study found a 150% increase over two years in the number of countries waging organised social media manipulation campaigns[7]. But the philosophical underpinnings and goals of disinformation operations remain the same.

That Russia has been fighting an information war to support its intrusion of Ukraine is no secret. One common narrative since 2014 is that Ukraine is a fascist state[8]. Such stories are easily unmasked and usually dismissed, at least in democratic Western countries like Canada. But they barely scrape the surface of how sophisticated disinformation operations can be. On 24 February 2022, the same day Russia began its invasion of Ukraine, an image started making its way around the internet. It showed a map of Europe down to the Persian Gulf and the Horn of Africa. Overlayed was a big, bold text that reads “*AIRSTRIKES IN THE LAST 48 HOURS*”, showing not only Russian actions in Ukraine but also Israeli attacks on Damascus, Saudi intervention in Yemen, and US airstrikes in Somalia. A bottom text called for viewers to “*CONDEMN WAR EVERYWHERE*”. It was an innocent anti-war graphic by itself, and over the next week, it arguably could have garnered millions of views, mainly from the left. What was not mentioned was that it was created by a media company, Redfish, with suspect ties to Russia[9][10].

There are several things to unpack here. Firstly, nothing featured in this piece is empirically untrue. The US and Israel did indeed respectively launch airstrikes on Somalia and Syria on those days[11][12]. But by equating a select and targeted American drone strike on jihadi terrorists with a full-scale invasion of a sovereign nation, the image generated a narrative that these actions possessed the same impact and moral weight. It also drew focus away from the Ukrainian crisis. Second is the choice of this image’s target audience. While disinformation has been chiefly associated with the far right of the political spectrum[13], this

---

[1] (Carvin, 2021b)
[2] (Rid, 2020)
[3] (Directorate-General for Communications Networks, Content and Technology (European Commission), 2018, p. 29)
[4] (Lim et al., 2019)
[5] (Briant, 2022)
[6] (Carvin, 2021a, p. 234)
[7] (Bradshaw & Howard, 2021)
[8] (Riehle, 2022)
[9] (Gilbert, 2022)
[10] Twitter has helpfully flagged Redfish as a Russian state-affiliated media source – a claim that Redfish unsurprisingly and adamantly denies on its social media.
[11] (Schmitt, 2022)
[12] (NEWS WIRES, 2022)
[13] (Carvin, 2021a, p. 238)

one primarily targeted the left. This reflects one of disinformation's overall goals of exploiting the divisions in a society[14][15][16], but it also reveals something much more sinisterly intimate: that it can hijack any of our prior intentions or principles, even one as innocuous as peace itself, and use it against us.

It also raises a more troubling question. Given that the focus of this piece of disinformation is not on the status of facts themselves but on a narrative that not only can be reasonably accepted by Canadian audiences but can also very likely be separately and independently generated by Canadians, how could we go about countering it, if at all? This case study seems to suggest that what we are facing is, at its core, not a battle over facts but a war over narratives. This is not to say that the propulsion of false information is irrelevant, but it suggests a need for us to shift our focus and understand where the common denominator of the nature of the threat manifests itself.

The Threat of Disinformation

Little has hitherto been spoken about the extent of the threat of disinformation. The effectiveness of known major recent disinformation operations in manipulating Western democratic populations has been debated by experts[17]. For example, while the Mueller report on Russian foreign interference activities in the 2016 US election mentioned that Russian-state social media accounts had collectively "reached tens of millions of US persons"[18], other analysts warn that to extrapolate conclusions from such figures is premature as it fails to account for the sort of content that was posted – only 8.4% of activity from the infamous Russian troll-factory Internet Research Agency was election related[19]. A finding shared at a 2017 Canadian Security Intelligence Service (CSIS) workshop on disinformation stated that the West's other great adversary, China, has been constrained in its foreign information operations by its lack of subtlety[20]. It is unclear how much that has changed since. Therefore, it is too early to say that foreign disinformation operations actively changed many minds in Western democratic countries.

The majority assessment seems to be that Canada has thus far escaped being the centre target of major state-led disinformation operations[21][22]. Nonetheless, as Carvin argues, we cannot afford to dismiss a threat simply because its worst outcomes have yet to be realised. A threat is a threat so long as it poses a danger to Canadian society and so long as it exists[23]. Authorities acknowledge this and place foreign interference through disinformation high on their priority lists[24][25]. There may be several reasons why this is the case and why

---

[14] (Ibid., p. 242)
[15] (*Who Said What? The Security Challenges of Modern Disinformation*, 2018)
[16] (Communications Security Establishment, 2021b)
[17] (Carvin, 2021a, p. 223)
[18] (Mueller, 2019, p. 26)
[19] (Rid, 2020)
[20] (*Who Said What? The Security Challenges of Modern Disinformation*, 2018, p. 76)
[21] (Carvin 2021a, p. 252)
[22] (Communications Security Establishment, 2021b, p. 29)
[23] (Carvin, 2021a, p. 223)
[24] (Canadian Security Intelligence Service, 2021)
[25] (Robinson, 2020, p. 81)

disinformation may be a standout candidate amongst the diverse elements occupying Canada's future threat matrix.

The first is disinformation's unique philosophical antagonism to democracy. Democracy relies on a healthy societal debate that proceeds in good faith. For that to happen, there needs to be an objective set of facts reflecting reality, which all partakers agree upon. By employing falsehoods and emphasising a focus on subjective narratives over empirical evidence, disinformation breaks the ground on which facts stand. Rather than relying on objective information to assess the merits of an argument, disinformation touts the usage of stories over evidence. Its direct appeal to victims' emotions and values shows its subjectivity. The Redfish image above appealed to an anti-war ideology without making readers assess why each military operation occurred. Other disinformation operations press emotive issues like race, globalisation, or immigration. In each case, the emphasis is on beliefs, narratives, and ideologies over analyses and facts. This creates a backward model to democracy where beliefs inform truths as opposed to the other way around. At that point, democratic discourse is impossible as there is no common ground of reality[26]. Without debate, democracy loses its foundation, path, and momentum. We risk being trapped in a "policy paralysis"[27] with governments, institutions, and citizens unsure whom to trust or how to proceed. While bombs, pandemics, and the growing threat of climate change exist as externalities that equally threaten all nations, democratic or otherwise, disinformation is particularly potent as a democracy killer.

Another way to understand disinformation's threat to Canada is to analyse it in tandem with our adversaries' foreign policy objectives. Russia, the traditional and most experienced wielder of disinformation, has used it not just to protect Putin's internal rule and reduce America's influence but also as a means to fracture NATO and the EU, portray itself as a responsible global power, and control the former Soviet states[28]. This is probably why the European Commission reported that a "continued and sustained disinformation" operation had occurred during the 2019 European Parliament election[29], why former Soviet states like Estonia, Latvia, and Lithuania have been the most confrontational in their counter-disinformation policies[30], and why other nations on Russia's periphery like Sweden[31] and Finland[32] have resolutely braced themselves for interference in their elections. It is also probably why Canada has managed to escape being the target of any known major Russian disinformation operations thus far.

But we might not be so lucky with liberal democracy's other great adversary, China. There is little doubt now that China is quickly rising to challenge America's position as the world's supreme power. The evidence for this includes projections of its economy to become the globe's largest within a decade[33], its rapid military modernisation program, its increasing defiance of international norms and tendency to act as a rule-setter rather than a rule-taker[34],

[26] (Angus, 2022)
[27] (Hulcoop et al., 2017)
[28] (Riehle, 2022)
[29] (Scott & Cerulus, 2019)
[30] (Hellman & Wagnsson, 2017)
[31] (Henley, 2017)
[32] (Mackintosh, 2019)
[33] (Magnus, 2021)
[34] (Lim, 2020)

amongst many others. While these may suggest a more assertive China, one that poses a significant threat to the liberal rules-based international order by which Canada has benefitted so much, analysts have speculated that China's foreign policy goal is not to displace America as the world's hegemon[35]. Instead, China seeks legitimacy or, at least, non-interference for its political-economic system and actions abroad. While this may imply that it does not necessarily want to dominate the West entirely and constantly, it does mean that it is willing to twist the international order or act intrusively to serve its national interests. Part of this may involve penetrating Western societies either to relieve foreign pressure on its actions or to promote its system so that we would not constrain it. Disinformation may very well be in its toolkit.

There are many reasons why Canada may thus turn into a target of Chinese disinformation operations. As an upholder of international liberal values, we are compelled to speak out when China violates international norms. It will seek to curb us on that. Canada also possesses thriving research and technology in areas valuable to China, such as biopharmaceuticals, artificial intelligence, quantum computing, and aerospace engineering[36]. It also remains an attractive investment and education destination for Chinese firms and students. The PRC thus has reasons to try and influence Canadian public perceptions on issues of doing business with China. The 2017 Chinese acquisition of two Canadian firms working on technologies with military applications, ITF Technologies and Norsat International, is proof of this[37]. Indeed, the 2020 CSIS public report explicitly called out China for attempting to conduct foreign interference in Canada "to support foreign political agendas or to deceptively influence Government of Canada policies, officials, or democratic processes"[38]. One example of this has been disinformation operations targeted at Canada's significant Chinese diaspora population through applications such as WeChat[3940].

New Zealand offers a chilling image of what could come to be in Canada. A 2018 submission made at another CSIS workshop evaluated that China had executed a "concerted" foreign interference campaign in New Zealand to influence its political process, suppress criticism of China, and facilitate espionage opportunities[41]. The effects were startling: a curtailing of freedoms for the Chinese diaspora, a silencing of debates about China, and a "corrupting influence" upon the New Zealand political system[42]. If the Chinese consider their actions there to be a success, then we could expect disinformation to grow as a state-based threat to Canada.

Of course, state-based threats are hardly the only ones facing Canada. As the COVID pandemic showed us, most countries and their intelligence apparatuses were wholly unprepared for a mass health crisis[43]. Similarly, climate change and its accompanying natural

---

[35] (Paltiel & Smith, 2020)
[36] (Vigneault, 2021)
[37] (Burton, 2021, p. 595)
[38] (Canadian Security Intelligence Service, 2021, p. 22)
[39] (Communications Security Establishment, 2021b)
[40] (Carvin, 2021a, p. 255)
[41] (*Rethinking Security: China and the Age of Strategic Rivalry Highlights from an Academic Outreach Workshop*, 2018, p. 75)
[42] (Ibid., p. 79)
[43] (Dahl, 2021)

disasters are increasingly being examined from the perspective of national security[4445]. At the same time, one cannot discount other actor-based threats such as terrorism, weapons proliferation, cybersecurity, or ideologically motivated violated extremism (IMVE). These threats vary in terms of probability and impact, with events such as global pandemics being considered high-impact-low-probability (HILP)[46] and climate change being understood as a force multiplier of other crises such as migration[47]. As such, the Canadian national security and intelligence community needs to analyse and prepare accordingly for each of these threats carefully.

But one feature that binds all of these threats in commonality is that almost any conceivable crisis they perpetuate can be exacerbated and appropriated through disinformation. For example, China used disinformation to sow doubts over the origins of the COVID virus[48] and the efficacy of vaccines[49], twisting a scientific issue into a matter of international and domestic politics. It is not unthinkable that an issue as already politicised as climate change, where international cooperation is so urgently needed and where national interests can be so heavily vested, can quickly become the victim of the next massive state-led disinformation campaign.

Other actor-based threats also intersect or originate from disinformation. For example, experts identify the most significant threats from IMVE to be those which manifest domestically[50]. They begin in an environment which facilitates societal dislocation and a growing political polarity, one which disinformation is perfectly attuned to exploit. As CSIS Director David Vigneault acknowledged, IMVE represents a societal problem[51]. While extremist beliefs might not originate from foreign disinformation operations, they can only be encouraged by it, and in turn, they may only perpetuate it. This also blends into the broader problem where it can be difficult to distinguish between domestic and foreign-based disinformation and, moreover, whether the solution to them should be one and the same. Similarly, cybersecurity and the advent of new technologies also intersect closely with modern disinformation as it operates mainly within the virtual space. The possibility of using AI to conduct disinformation operations is the most obvious potential here, and it will make attempts to track disinformation only harder[52]. Therefore, I argue that disinformation represents a unique threat to Canada's national security because of its singular potential to appropriate and exacerbate the damage of almost any other element in the threat environment. And because there will likely always be a threat facing Canada, we can reasonably expect disinformation operations to manifest themselves as a constant and sustained barrage.

To summarise, I argue that disinformation represents a unique danger among Canada's threat environment for three reasons. The first is that disinformation is particularly and fundamentally antithetical to democracy and attacks its very core. The second is that it has historically worked very well in tandem with the foreign policy objectives of the liberal

[44] (Davis, 2021)
[45] (Rigby, 2021)
[46] (Dahl, 2021)
[47] (Wilner, 2021)
[48] (Canadian Security Intelligence Service, 2021, p. 23)
[49] (Communications Security Establishment, 2021a)
[50] (Shull & Wark, 2021, p. 10)
[51] (Vigneault, 2021)
[52] (Carvin, 2021a, p. 258)

West's past greatest adversary, Russia and that it is equally suited to the foreign policy goals of the rising Chinese state, which is growing more adept at wielding it. Finally, I have noted that disinformation could frictionlessly accompany almost any crisis originating from many of the other elements on Canada's threat matrix and, in some cases, even further perpetuate them.

A Canadian Solution to Disinformation

How do we go about tackling disinformation? Thankfully, several real-life examples and theoretical models exist for us to learn from and emulate. In studying and applying them to a Canadian context, I conclude that a whole-of-society approach is needed, with an energetic and integrated government strategy leading the way.

Hellman and Wagnsson proposed a valuable framework for formulating government policies to counter foreign disinformation narratives built along two dimensions: engagement versus disengagement and inward versus outward targeting[53]. Engagement means confronting foreign narratives, while disengagement means leaning towards a more passive stance (in the most extreme case, doing nothing). Inward and outward targeting determined whether the government emphasised its focus on domestic or foreign audiences. These two dimensions combined created a window of roughly four policy groupings for governments to consider:

- Confronting – Engages against foreign disinformation narratives and projecting counternarratives toward foreign audiences.
- Naturalising – Projects its own counternarratives towards foreign audiences but does not focus on contrasting with the assaulting foreign narrative. Aims to act as a model and spread values for others to follow.
- Blocking – Engages with foreign narratives by blocking them from being exposed to domestic audiences.
- Ignoring – Neither espousing counternarratives nor blocking foreign narratives. Essentially doing nothing.

In assessing the appropriateness of each policy grouping, I considered three criteria: their effects on foreign relations, compatibility with a democratic society, and effectiveness in countering disinformation.

This author recommends a course of naturalisation as the best policy umbrella to pursue. The reasoning is as follows. Firstly, confronting is the most likely to result in increased tension and a deterioration in relations between Canada and the offending nation. While this may be necessary in some cases, Canada has many strategic interests where cooperation with adversaries is needed. An example of this is cooperating with China on trade, investment, and combatting climate change[54].

Secondly, blocking foreign narratives just because we may not like them or think they are wrong poses a significant threat to Canadians' right to free speech and open debate and risks silencing legitimate political concerns. This is especially as the blend between foreign

[53] (Hellman & Wagnsson, 2017, p. 157)
[54] (Singh, 2021)

disinformation operations and domestically backed narratives is growing increasingly fuzzier. The act of blocking views also has the risk of backfiring and giving those foreign narratives more attention and support.

Thirdly, the policy of ignoring foreign narratives is too weak and essentially allows the threat of disinformation to persist at our peril. The government has a responsibility to defend Canada's sovereignty against foreign interference. Therefore, naturalisation remains the only plausible course of action. This allows us to contest foreign narratives without stifling free speech, addressing the threat of disinformation while maintaining international relations where needed.

What would a naturalisation policy look like? What would a Canadian counternarrative be? My answer is that it would be the same narrative that millions of Canadians and people worldwide already buy into: that Canada is a strong, prosperous, morally conscious, free, and liberal nation. The merits of this narrative can be witnessed in the enduring friendships of our alliances, our advanced economy, the aspirations of our immigrants, and our commitment to good government.

Of course, to project this narrative onto the world, it must be true. If we are to act as a model, we must be a model. That is what differentiates our narrative from that of hostile disinformation operators. This involves addressing many of the fissuring domestic issues plaguing the country, such as rising costs, truth and reconciliation, economic and social inequality, and many others. Tackling these issues in tandem with national security means that a whole-of-society response is needed[55]. By doing so, the Canadian government can address disinformation and simultaneously minimise some of the other threats it exacerbates, as explained in the last section.

For example, as noted earlier, a lot of IMVE stems from societal discontent – an apparition that has been causally linked to poor economic status or the belief that a better future is impossible. Parallelly, adherence to conspiracy theories is commonly associated with feelings of powerlessness[56]. By providing societal opportunities to those most likely to fall into extremism and giving them reasonable hope for optimism, we could tackle the national security threats of ideological violence and disinformation concurrently on a structural rather than symptomatic level.

A whole-of-society response can thus give us the impetus to confront a multitude of domestic issues where momentum might not otherwise exist. Besides emphasising the national security benefits of economic revitalisation, it could also act as the springboard to reducing political polarisation, thereby sealing another gap exploited by disinformation and rejuvenating our democratic discourse.

A whole-of-society approach is also useful not just in considering national security in sync with other issues but also in providing us with a broader array of tools to combat it. Taiwan, a nation[57] which has always lived in the shadow of invasion from China, completed a remarkable democratic election in 2020 in which civil society played a vital role in

[55] (Rigby, 2021)
[56] (Linden, 2013)
[57] Did I stutter?

combatting disinformation[58]. Acting in concert with non-national security policies also allows us to structurally embed the best permanent solution to disinformation: education. Finland, another nation that has always existed on the periphery of a larger, hostile neighbour, emphasises media literacy and critical thinking in its schooling system from an early age[59]. Such developed skills would make disinformation fail at its most elementary stage: the human mind.

A whole-of-society method would facilitate a more effective partnership between government and civil society actors. This could help increase overall societal understanding of disinformation. Much work in uncovering disinformation networks has been done using tools provided through open-source intelligence (OSINT) by academic communities such as the Citizen Lab at the University of Toronto[6061]. In their research, they noted that their reliance on OSINT limits their ability to draw conclusive links between disinformation operations and their perpetrators. Nevertheless, intelligence services and researchers have an opportunity to share information, tools, and techniques. Furthermore, as cyber power plays an integral role in the fight against disinformation, the Canadian government may also partner with researchers and Canada's highly sophisticated technology industry to develop increased capabilities. The UK has already adopted such an approach in its new integrated national security policy[62].

Of course, much of the above could only be achieved with energetic political leadership from the top down. Thus, this whole-of-society strategy necessarily implies a whole-of-government approach. Much like the aforementioned UK integrated policy, Canada should rethink its national security policy and consider it alongside its foreign, defence, aid, and economic policies, to name a few[636465]. This entails a concentrated centralisation of the national security apparatus and an expanded definition of national security[66] that clearly explains its importance and connection to various policy sectors where it previously may not have been obvious.

All of this hints at the possibility of a national security or foreign policy that, in part, both drives and is driven by domestic policy. While this may sound counterintuitive in the face of the many geopolitical threats we face, it is actually very reasonable.

For example, a common narrative of Russian and Chinese disinformation operations and propaganda directed against the US is its poor record of racial inequality. Such racial issues also exist in Canada, in parallel with its historical and persisting treatment of indigenous populations. Adversaries to the West may thus seek to exploit the colonial and racist treatment of minorities by Western powers to sow divisions within Canadian society or strain relations with nations in the Global South. In the case of China, which itself has a vivid history of colonial loss that resonates to this day, they may even seek to create a shared post-

---

[58] (*When Election Interference Fails*, 2020)
[59] (Mackintosh, 2019)
[60] (Hulcoop et al., 2017)
[61] (Lim et al., 2019)
[62] (UK Cabinet Office, 2021, p. 40)
[63] (Shull & Wark, 2021, p. 4)
[64] (Wark, 2021)
[65] (Rigby, 2021)
[66] Ibid.

colonial narrative. In a country as ethnically and racially diverse as Canada, this may be a problem as it threatens to divide us into tribalism. Therefore, the Canadian government needs to take issues like racial inequality or truth and reconciliation with renewed seriousness. In considering these issues from a national security perspective, we can find fresh determination to solve them, and in resolving them, we can drive forward a more united whole-of-society foreign and national security policy.

Nor would Canada be the only nation with a foreign policy driven in part by domestic policy. Besides the integrated UK policy, the American Build Back Better plan, which started as a domestic agenda centred around national infrastructure, is lending its tagline to the upcoming American-led G7 initiative to provide an infrastructure partnership to low- and middle-income countries, in competition with China's Belt and Road Initiative[67]. Leaders in the UK[68] and Canada[69] have already appropriated the title to describe their own agendas for recovery.

There is another benefit to pursuing a whole-of-society approach alongside an integrated government strategy. In choosing naturalisation and forming our own strategic narrative, we have an opportunity to identify our policy goals and actions clearly. While we recognise that a balance may be needed and that sometimes more confrontational or engaging manoeuvres will be needed on the part of the government to combat disinformation, this strategy relegates such actions to the short term and informs our overarching priorities. A prudent government would recognise, as the UK has done[70], that in some cases, we would need to engage with adversaries such as China, which might attract the disapproval of the national security community. In democratic governments, a common pitfall is that there will be competing agendas and interests among departments and personnel, to the detriment of the overall outcome. This strategy will curb that and minimise the damage done to our overall strategic interests, including, first and foremost, our national security.

The formulation of having a foreign policy driven in part by domestic policy also has the additional advantage of helping us retain our foreign policy sovereignty. Canadian domestic issues are unique to Canada. In conducting this strategy, we will not be placing ourselves at odds with our traditional allies over issues such as human rights or defence. Nor would we be hanging onto their coattails at our own expense.

A New Canadian Intelligence Paradigm

Where does Canada's intelligence apparatus come into all of this? This section will examine the Canadian intelligence community's unique role in uncovering, attributing, and stopping disinformation operations. I will also look at an area where it has been steadily trying to augment: stakeholder outreach to both partners and the larger Canadian society. I will then discuss some of the structural, ethical, technological, and human attributes the intelligence community needs to adopt in order to fulfil those two mission branches.

---

[67] (The White House, 2021)
[68] (UK Cabinet Office, 2021, p. 3)
[69] (Press, 2022)
[70] (UK Cabinet Office, 2021, p. 26)

A policy guided on naturalisation has been advocated as a way to minimise the adoption of hostile foreign narratives in Canada and combat disinformation by fomenting a subtle pushback. However, it cannot be twisted into a brainwashing propaganda war happening behind the scenes from the citizenry. Governments, democratic and autocratic, push forward their own narratives all the time, both covertly and overtly. Naturalisation only calls for a more concerted effort to tie narratives on different topics together and to promote them with greater vigour in the interests of national security. While motivated in part by national security concerns, the general narrative should be best promoted through other realms such as foreign, aid, and economic policies.

The national security and intelligence community should remain focused on foreign intrusions at home. While promoting our own narrative as a subtle pushback to disinformation could serve as an excellent blanket to counter it, there still remains the need to act preventatively and defensively where foreign interference makes its incursions. Therefore, we still have to uncover and disrupt active foreign interference operations in Canada. The intelligence community will continue to operate at this frontline of Canada's defence, playing the primary role in exposing foreign disinformation campaigns. As mentioned earlier, OSINT researchers have encountered limitations to how conclusively they could attribute disinformation operations to a specific actor. This leaves agencies such as CSIS or CSE best equipped to confront the threat.

The CSIS Act already provides the legal mechanism for the agency to monitor and analyse threats such as foreign interference[71], which state-induced disinformation falls under. Similarly, the CSE's "Part A" mandate authorises it to collect foreign intelligence via signals intelligence (SIGINT)[72]. This intelligence would include covering threats such as foreign interference. Additionally, the CSE's "Part C" mandate would allow them to provide technical and operational assistance to agencies like CSIS in detecting and attributing disinformation operations[73]. If disinformation grows in size and sophistication due to technology, as we expect it to do[74], then requests for technical expertise from the CSE would only increase alongside it.

The discovery and attribution of disinformation is only one half of the process. Limiting its damage is the other half. While the CSE has been authorised, under certain conditions, to conduct computer network attack (CNA) operations[75] that can potentially disrupt disinformation networks, this tool should be used restrictively and carefully. Technological solutions such as this are usually reactive[76] and could create adverse ramifications. There are ethical objections to blocking speech and nuances to conducting offensive cyber operations. The worst-case scenario is that such an action would backfire and legitimise whatever piece of disinformation it was attempting to contain.

Instead, the focus should be on continuing the whole-of-society philosophy that we have adopted and strengthening the communication links between the intelligence community and national security stakeholders – especially outside the government. The intelligence

[71] (Littlewood, 2020, p. 45)
[72] (Robinson, 2020, p. 74)
[73] (Ibid., p. 81)
[74] (Carvin, 2021a, p. 258)
[75] (Robinson, 2020, p. 77)
[76] (Lim et al., 2019)

community has started to become aware of this, as evidenced by outreach initiatives such as the aforementioned CSIS workshops or this contest. Since the pandemic's beginning, CSIS has briefed more than 225 organisations on possible national security threats and how to protect themselves[77]. This approach should be taken with the threat posed by disinformation. Government agencies, corporations, NGOs, institutional bodies, and the general public should be informed about the narratives commonly propelled in foreign disinformation operations, how they are transmitted, and how they could directly harm each stakeholder.

Structural Elements and Attributes

What elements and attributes would Canada's intelligence community need? I begin this section of the paper by examining the structural features that should be adopted to facilitate this new approach to combatting disinformation. Some of them have already been hinted at or discussed in this paper, but for the sake of completeness, they will be mentioned again and expounded further.

Suffice to say, the integrated government strategy carrying this whole-of-society approach necessitates an integration and centralisation of the intelligence community itself. This is far from a new idea. Since 9/11, Canada's national security reforms have focused on greater integration[78]. This drove initiatives like the Integrated Terrorism Assessment Centre (ITAC) or the Integrated National Security Enforcement Teams (INSETS). Nevertheless, this has not been enough to keep pace with the development of challenges over the last twenty years[79]. The pandemic, like 9/11 did before it, has brought the importance of consistent information and intelligence sharing back to the forefront, this time with non-traditional stakeholders like public health agencies. We have only begun to think about what elements of integration the mixed threat environment of the future will require from us. Initiatives such as One CSE, which seek to internally integrate all of the agency's mandates[80], are a good start but need to be both emulated elsewhere and intensified.

Intelligence integration in the fight against disinformation becomes important for two reasons. First, as noted above, the overlapping mandates between CSIS and CSE in combatting foreign interference and the mostly cyber nature of disinformation operations means that CSIS and the CSE will increasingly have to cooperate in identifying and attributing disinformation campaigns. Therefore, there is an operational requirement for greater integration among the intelligence agencies. Secondly, if the intelligence agencies are to effectively execute their other half of the mission, communicating the threat of disinformation to stakeholders outside of their community, they must generate a cohesive message that can be easily understood. Subsequently, there is a need for an integrated intelligence analysis and product dissemination process.

One of the other greatest difficulties in modern intelligence is getting leaders to listen[81]. Given that this whole-of-society approach requires energetic political leadership and

[77] (Geddes, 2021)
[78] (Littlewood, 2020, p. 55)
[79] (Wark, 2021)
[80] (Communications Security Establishment, 2021a)
[81] (Dahl, 2021)

a sturdy understanding of national security, it is therefore equally as important as integration to centralise intelligence outputs at a high level. To successfully convey the weight of the disinformation threat and sufficiently motivate the national security imperative of this whole-of-society approach, there needs to be constant advocacy of national security priorities at the top branches of politics. This ensures a focused and carefully scrutinised message to political leadership that cannot be relegated. It also assures that the national security dimension would be understood from the top down in driving foreign, aid, economic, and other domestic policy agendas.

This can be achieved by solidifying and enhancing a critical component of Canada's national security apparatus that already exists: the position of the National Security and Intelligence Advisor (NSIA)[8283]. This means grounding the office in legislation and giving it the prerogative to direct the intelligence community's priorities and focus. An alternative or complementary method would be creating a cabinet-level committee analogous to the American National Security Council[8485]. This achieves the twin goals of enhancing integration outside the intelligence community between various government ministers and departments and retaining the centralised focus on national security.

Another structural feature to be considered for Canada's intelligence community is creating a dedicated foreign intelligence service. This, too, is not a new idea and has been subject to some debate[8687]. From the perspective of combatting disinformation, there are two reasons for doing this. Firstly, the naturalisation policy involves us going abroad to promote our narrative. This naturally necessitates an understanding of the target audiences of foreign nations. While our intelligence community themselves would not advance the promotion of our narrative, they could provide policymakers with the information needed to craft a thoughtful approach that would not be considered hostile or intrusive abroad.

Secondly, our adversaries' use of disinformation as a tool reflects a more significant foreign-based threat. Domestic actors may espouse disinformation, but its existence when foreign is a symptom of a larger foreign interference initiative. Therefore, we must understand our adversaries' "capabilities, intentions, and activities"[88]. CSIS is currently legally limited in the type of foreign intelligence it can collect, and the CSE is restricted to SIGINT. In evaluating whether there is a need for greater foreign intelligence, we should account for the intelligence we already receive, including from our foreign partners such as in the Five Eyes, and the cost of such an initiative. This paper will not delve further into this subject, only suggesting that the foreign origins of disinformation signify an increased requirement to understand foreign state goals and plans.

Therefore, Canada's intelligence community has three main structural attributes where change needs to be accelerated or considered. The first is the quality of integration between the intelligence agencies to ensure operational cooperation. More importantly, the intelligence community's message to stakeholders needs to be concise and coordinated.

---

[82] (Rigby, 2021)
[83] (Shull & Wark, 2021, p. 4)
[84] (Rigby, 2021)
[85] (Shull & Wark, 2021, p. 4)
[86] (Wark, 2021)
[87] (Littlewood, 2020, p. 51)
[88] (Ibid., p. 48)

Secondly, to drive the whole-of-society approach with an integrated government push from the top-down, there needs to be a centralisation of national security understanding delivered at the very top of the political food chain. This could mean an enhancement of the NSIA office or the creation of a cabinet-level national security council. Finally, we should reconsider whether we are heading into an age of sharpened geopolitical difficulties, marked by an intensified need for foreign intelligence that can be resolved with a dedicated Canadian foreign intelligence service.

Ethical Elements and Attributes

Our intelligence agencies must always uphold the safeguarding of Canadian democracy as their core principle and motivator. Additionally, to effectively carry out their mandate and protect the Canadian public, they must retain its trust. To accomplish this whilst combatting disinformation, there are two ethical attributes of pivotal importance: transparency and inclusion.

If the aforementioned narrative is true, then as Canadians, acting ethically and responsibly is important to us in and of itself. The truthfulness of this statement distinguishes our promotion of this narrative from mere propaganda. But even in the unthinkable scenario where this fails to convince us of the need to act ethically, there is an alternative realist argument which argues for an intelligence community built upon a solid ethical foundation.

It is that in a world of competing narratives, our objective is to draw people to ours. That happens most effectively when they identify with the values and ideals of our narrative and are inspired by witnessing them in action. To this end, it is essential for all the components of this government, including the intelligence community, to act as ethically as possible. Moreover, people need to be able to see this. Therefore, transparency from Canada's intelligence community is vital to building trust and winning through the naturalisation policy.

Full transparency in an area as sensitive as national security can never be possible. Instead, the key is to build a framework that facilitates as much accountability as possible[89]. But transparency can come through many outlets. This includes information on how mandates and authorities are interpreted and translated into practices[90], how oversight is implemented, etc... With regard to countering disinformation, policy transparency will be of paramount importance. This means informing Canadians about the "strategic issues impacting national security and current and future efforts and plans for addressing those issues"[91].

Policy transparency is of special significance because it is more than just public oversight. It is also public education. In publicly exposing, explaining, and discussing strategic threats like disinformation, intelligence services improve society's knowledge of them[92]. They also demonstrate their trust in the Canadian public to take defensive precautions

[89] (*Open Government Partnership (OGP) Global Summit Summary of National Security Panels*, 2019)
[90] (National Security Transparency Advisory Group, 2020, p. 7)
[91] (Shull & Wark, 2021, p. 24)
[92] (National Security Transparency Advisory Group, 2021, p. 12)

themselves. This achieves dual goals of strengthening societal resilience and receiving reciprocal public trust.

It is crucial for intelligence agencies not just to talk about transparency as an abstract concept but to operationalise it. This means designing open indicators that measure transparency and placing mechanisms to collect and report on them systematically. On policy transparency, the National Security Transparency Advisory Group (NS-TAG) has suggested possible indicators like the proactive disclosure of policies, threat assessments, or how technologies like AI are being used[93].

There is also an opportunity to invite societal inputs on transparency in highly specialised areas like data governance. The cyber element of disinformation means intelligence operations to track it will likely rely on a lot of data[94]. Naturally, there will be concerns about issues ranging from privacy[95] to the ethical use of data on questions like discrimination or biases[96]. Intelligence agencies have an opportunity to engage with outside organisations reliant on data to share insights into frameworks on governance. Similarly, they may consult with academic circles on mitigating biases within data to prevent outcomes such as statistical discrimination.

This ties into the second ethical element which must be demanded from the Canadian intelligence community: inclusion. Like any public agency, the national security and intelligence community must reflect the citizenry that it serves. Canada is a powerfully diverse country, so our services need to bear this in mind in executing their duties. The above example of discrimination reminds us of this need. The NS-TAG noted in its report that

> "*many members of Indigenous, Black, racialised, marginalised, and other minority communities mistrust national security agencies, and the nature of their interactions with these government bodies often exacerbate these tensions.*"[97]

As mentioned earlier, foreign disinformation operators commonly exploit racial and ethnic tensions in their narratives. This is done to undermine societal trust in Western governments. Therefore, there is a strong national security imperative to make our intelligence apparatus more inclusive and diverse. Conversely, inclusion offers a compelling opportunity to reinforce one of the central tenets of Canada's would-be narrative: a society united in common ideals instead of tribalism.

The attributes of transparency and inclusion are thus irretrievably linked. Both are important ethical dimensions to Canada's future intelligence community. Both can find their rationale in national security imperatives of maintaining the public's trust, ensuring societal cohesion, and promoting Canada's strategic narrative to counter disinformation. But moreover, they are both motivated by what is morally right.

---

[93] (Ibid., p. 7)
[94] (*New Challenges for Strategic Intelligence – Canada, United States, Private Sector*, 2019)
[95] (Vigneault, 2021)
[96] (National Security Transparency Advisory Group, 2020, p. 8)
[97] (Ibid., p. 9)

Technological Elements and Attributes

The virtual nature of modern disinformation operations, primarily waged on social media, means that technology will naturally play a huge component in any attempts to address it. Investigations and analyses will become more data driven[9899]. From this perspective, the biggest challenge to the intelligence community will be shifting through the mountainous amounts of data available to discern which are useful for generating comprehensive and informed intelligence products[100]. Needless to say, agencies will have to keep up with the latest developments in techniques and technologies, particularly in artificial intelligence and other big data tools[101].

This paper will not go further into technical details surrounding the technologies intelligence agencies should adopt. However, it will emphasise that the application of technology requires careful thought and technical understanding at the policy stage, which might currently be lacking.

For example, concerns about biases and discrimination through data analyses have already been mentioned. These might exist for a variety of non-intentional reasons. For example, historically marginalised racial groups could be under or overrepresented in particular categories of datasets. The resulting algorithmic analysis could present predictive results widely distinguished by racial inputs, a sort of computational racial profiling. These biases could persist even if we were to manually set the algorithm to ignore race as a factor – machines could use proxy variables. This problem could easily manifest itself in an example of trying to track a disinformation network. Since many foreign disinformation operations target diasporas[102] within a particular ethnicity, an algorithm trying to trace a disinformation operation could be viewed as racially biased.

Policymakers have exhibited signs of being aware of such problems and the need to recognise the limitations of tools such as AI[103]. But they are less attuned to how to address or mitigate them.

One proposal is to favour and focus on explainable AI[104]. Generally speaking, this is a much more mature view than simply viewing AI as a catch-all solution to data problems. However, the absence of further discussion beyond that betrays a lack of technical understanding of what the term "explainable AI" means or its effectiveness in the intelligence context.

The terms explainable and interpretable AI are often used interchangeably, but they denote vastly divergent things. The latter uses relatively open, transparent, and humanly understandable algorithms to perform its analyses. This results in a situation where human users can understand, to a degree of general confidence, what is happening inside them, for

---

[98] (Vigneault, 2021)
[99] (*New Challenges for Strategic Intelligence – Canada, United States, Private Sector*, 2019)
[100] (Robinson, 2020, p. 80)
[101] Ibid.
[102] (Carvin, 2021b)
[103] (Hershkovitz, 2019)
[104] (*Artificial Intelligence, Big Data, and Change in the Canadian Intelligence Community*, 2019)

example, which variables are being weighted heavily. The trade-off is that these algorithms are usually less accurate than more complex ones.

In contrast, an explainable AI model uses more complex models which, in the case of deep learning, could contain billions of nodes. These models are impossible to understand humanly. They are used to generate predictions from the data. A second interpretable algorithm then approximates the result of this initial algorithm. The hope is that the second algorithm could then explain which variables were the most important in making these initial predictions. This way, the accuracy of predictions is retained while we receive an explanation for them.

Strictly speaking, however, this "explanation" is not actually an explanation for the original predictive model – it occurs after the predictive process[105]. Therefore, there is no guarantee that the explanative model provided by the explainable AI is correct – nor is there any way to check[106]. Therefore, explainable AI fails to deliver on the accountability or transparency that we might demand from data analysis tasks in intelligence. The alternative is to use interpretable AI at the cost of accuracy.

This example is meant to show that policymakers need a technical understanding of the technological systems they plan to embed into the intelligence process. Only then could they begin to debate their appropriateness. Certain tasks requiring high predictive accuracy could not be relegated to less complex AI models. Other times, where normative judgements of justice or fairness are present[107], as they often are in national security, interpretable AI may be more suitable.

What is essential for policymakers to understand is that technology can never reduce a choice outside the responsibilities of a moral agent. Therefore, intelligence agencies need to carefully consider questions about how technologies like AI are being used in their processes to complement or aid human analysts[108].

There are three main areas to account for. Firstly, policymakers need a general technical understanding of AI's limitations regarding their accuracy or biases. The importance of this has already been explained. Secondly, they must be aware of the changing disinformation threat environment and how that feeds into AI processes. The blend between foreign and domestic disinformation networks means that they will have to be wary of the origins of data processed by these machines, often autonomously. Failure to do so could not only impact the accuracy of predictions but also risks legal violations as they begin to inadvertently collect domestic data. Finally, to ensure accountability and transparency, policymakers need to decide where moral responsibility lies in the intelligence process when decisions are aided by technology[109]. Do they reside with the analyst user, the developer, or the executive who oversaw their implementation into the process?

What this section has aimed to convey is the importance of both technical knowledge and process planning in the implementation of technology in intelligence agencies. The need

[105] (Babic et al., 2021)
[106] Ibid.
[107] Ibid.
[108] (Babic et al., 2020)
[109] Ibid.

to keep up to date with the latest tools and techniques is self-evident. The question of how to use them requires non-technical managers to embrace understanding both small details and big picture questions. This brings me to the final and arguably most important element of Canada's intelligence community: its people.

Human Elements and Attributes

The other sections have tangentially contributed to our conception of the human elements required from Canada's intelligence community in the future. For example, an ethical commitment to inclusion naturally implies a diverse workforce that reflects the breadth of Canada's cultural background. Similarly, our examination of technology needs revealed that policy planners must think holistically and understand how technical details fit within their larger processes. These inferences show that the first three pillars of attributes needed for Canada's intelligence agencies will be tied together by the fourth pillar, human elements.

The first attribute needed from future intelligence community members will be an increased level of interdisciplinary thinking. This is important for two reasons. Firstly, it supports inter and intradepartmental integration, a structural change which we have already discussed. This is not to suggest that each individual must be a master of all trades and able to take on multiple roles in the intelligence process. Instead, the goal is for each member of the process to be cognisant of the needs of other roles, thereby anticipating what is useful and required from them in their own work. This streamlines integration in the analysis phase by promoting situational understanding. It could also facilitate a large-scale cultural shift in a system where public servants are often incentivised to hoard specialised information rather than share it[110].

Secondly, as explained in the technology section, there is a need for policymakers and process designers to understand the technical details of the tools they are embedding. Conversely, analysts and developers need to know and provide feedback on how effective their analyses, and the technologies being used to help produce them, are towards building a cohesive strategic assessment. An interdisciplinary setting would ask policy planners to dive into details while exposing operational team members to the overarching policy priorities and visions. This results in knowledge sharing that can build a more effective intelligence process.

Aside from, but complementary to, interdisciplinary thinking, our response to disinformation will require a more robust understanding of it. To this end, it would be beneficial for the intelligence community to hire individuals with the same cultural background as our state adversaries. This helps us better understand the paradigms, cultures, and philosophies of the places where these foreign narratives originate from. This complements the goal of inclusion and takes advantage of Canada's diverse societal makeup. In flipping what our adversaries consider to be an exploitable point of tribalism, we become more equipped to dispel hostile narratives. The individuals we hire from these backgrounds would be familiar with the traditions and philosophies of their ancestral lands, but they would have consciously chosen to remain loyal to Canada. It is worth studying how and why they

[110] (National Security Transparency Advisory Group, 2020, p. 6)

made that choice. This not only identifies the weaknesses of foreign propaganda narratives but also nourishes our own strategic narrative and makes it all the more compelling.

Therefore, it is clear that human attributes will be the fundamental drivers and enablers of almost any structural, technological, or ethical changes. Though it is not realistic to expect a fully interdisciplinary workforce, it is both possible and vital that personnel learn to be cognisant and situationally conscious of what others in the intelligence process need and expect. This drives integration and incentivises information anticipation and sharing. As investigations become more data-driven and the reliance on technology grows, there manifests a pressing need for policy planners to understand the parameters wherein such tools can be applied.

Additionally, the fight against disinformation requires us to philosophically understand foreign narratives and counter them with our own strategic narrative, as demanded by the policy of naturalisation. This is most successful when we extract ideas from a diverse workforce able to empathise with our adversaries. It is also vital for each operational analyst to understand how their work builds up to this overarching strategic goal so that they might more effectively calibrate their outputs.

Conclusion

This essay began with a study of the nature of foreign disinformation operations. The term "disinformation" itself is, strictly speaking, dishonest, as our example showed that disinformation is not always empirically untrue. We noted that disinformation could appropriate any value or principle, even one as innocuous as peace itself, for its strategic purposes. Its subjective nature and appeal to emotions and ideologies over facts and analyses suggested that the core of the problem lay not in the dissemination of false facts themselves but in opposing narratives. Therein lies the threat.

Regardless of the effectiveness of foreign disinformation operations, their mere existence as a threat cannot be allowed to continue without opposition. We identified three elements that make disinformation a unique component of the threat environment. The first is its fundamental incompatibility with democracy by the fact that its constant subjectivity precludes a healthy democratic discourse. The second is that from a foreign policy standpoint, our state adversaries are historically well-versed and eager to deploy it due to its convenience. Finally, we noted that disinformation commonly intersects with, or compounds, other elements in the threat environment. For example, it could drive IMVE, and during the pandemic, it notably impeded effective responses such as by doubting the efficacy of vaccines.

To counter the disinformation narratives, we applied a two-dimensional model structured around engagement-disengagement and inward-outward targeting. We judged that a suitable response to disinformation would need to account for three criteria: its effects on foreign relations, compatibility with a democratic society, and effectiveness in countering disinformation. In applying this framework, it was determined that a policy of naturalisation would be the most appropriate Canadian response. This policy would have us project our own counternarrative to combat disinformation but, at the same time, shy away from aggressively contrasting ourselves or seeking confrontations with adversaries. This retains the free flow of

information necessary in a democratic society, leaves open the door to cooperation with otherwise competing states on common strategic interests, and would hopefully dispel the influence of foreign narratives in Canada.

To promote a convincing counternarrative espousing the benefits of Canada's liberal democratic system would entail it being truthful. This implies that there is now a national security imperative to resolve domestic issues such as education, social inequality, or truth and reconciliation. In tackling these issues, the Canadian government can not only close the divisive fissures that disinformation seeks to exploit and exacerbate but also minimise threats from other sources like the societal discontent that drives IMVE. This wholesale approach can only be accomplished when the entirety of Canadian society is included. In doing so, we are equipped with additional tools to combat disinformation, such as collaborative initiatives with academia and private sector researchers to understand the phenomena better.

This whole-of-society approach sufficiently motivates the government to resolve many of these domestic issues with renewed vigour. It necessitates an integrated government strategy where departments and portfolios previously unrelated to national security would understand their stake in it. The infant blueprint for such a coordination already exists in examples like the UK's integrated review of security, defence, development, and foreign policy. The benefits of consolidating these areas and others extend far beyond the response to disinformation. Moreover, they would allow the government to prioritise its objectives and determine overarching goals by which to design a flexible strategy. In doing so, Canada minimises losses that might otherwise result from internally conflicting interests and drives forward a sovereign security and foreign policy suited to its interests.

The role of Canada's intelligence community in this integrated approach is twofold. Firstly, it will continue to identify, expose, and attribute foreign disinformation operations as it did before. Secondly, it should serve as the primary official source by which stakeholders, both inside and outside government, are conveyed information about the threat. This involves educating them on the narratives commonly propelled in foreign disinformation operations, how they are transmitted, and how they could directly cause harm within each respective area.

The new integrated government strategy warrants structural changes within Canada's intelligence community. Firstly, the technical nature of modern disinformation and the shared mandate to prevent foreign interference means that CSIS and the CSE will increasingly cooperate in the future. This would be expedited if there was greater integration within the intelligence community itself to support operations and investigations. Secondly, to concisely convey threat information to external stakeholders and intelligence clients, the intelligence community needs to consolidate its message. This requires a centralisation of analyses and strategic threat assessments. To underscore the weight of the national security imperative and ensure that all government departments within this integrated government strategy understand their role in it from the top down, this centralisation should occur at the highest political level. An enhancement in the powers of the NSIA office or the creation of a cabinet-level national security council are two suggestions for this. Thirdly, our adversaries' evident preference for disinformation as a convenient weapon and other geopolitical developments should motivate us to ask whether we are entering a new era of international relations with a

developed need for foreign intelligence. This could mean creating a dedicated Canadian foreign intelligence service, although we offer no conclusive argument here.

The Canadian government, including its intelligence agencies, must also make ethical commitments to transparency and inclusion to lend credence to its work. This is important for two reasons. Firstly, naturalisation aims to influence people into believing our counternarrative. This is best served when they can witness the ethical principles we adhere to in action. Secondly, the Canadian public must trust intelligence agencies for them to effectively execute their mandates – especially when it comes to the second task of being the authoritative source in briefing the nation on threats. Transparency can be achieved through several means, including clarifying the legal jurisdictions within which intelligence services can operate. But of particular importance is policy transparency. This means openly discussing the strategic threats facing Canada and the measures used to combat them. This has the dual purpose of promoting trust and societal understanding of the threat. Inclusion also promotes societal trust by making our intelligence agencies reflective of Canada's diverse and boisterous population. This seals gaps that disinformation actors might seek to exploit and strengthens our understanding of divergent philosophies.

The increased importance and volume of data in intelligence investigations also signifies the challenges of implementing new technologies. Here, the need for agencies to embrace tools such as AI is self-evident. However, intersections with ethical concerns complicate the matter. Fears of discrimination arising from data biases are reasonable and must be addressed thoughtfully. As the discussion of explainable AI has shown us, the focus here should be on both what technologies to acquire as well as how to implement them. This requires policymakers who will design future intelligence processes to have a technical understanding of the limitations of such tools. Moreover, they must recognise that an ethical choice can never be wholly relegated to machines. Therefore, there is a constant need to examine how tools are being used, for example, what data is fed into them and who bears the moral responsibility for these machines' outputs.

All of these structural, ethical, and technological changes demanded of future intelligence agencies revolve around people. Indeed, the future Canadian intelligence community will be defined by its employees. Firstly, an interdisciplinary mindset should drive all members to understand the community's overarching strategic goals, their role in the mission, and what others expect from them in terms of information and analyses. This facilitates integration and knowledge sharing at the operational level. It also improves the design of the intelligence process as stakeholders become aware of how the effectiveness of their decisions is limited within other areas. For example, as mentioned above, policymakers need a technical understanding of technologies to see where they are most appropriately useful. Conversely, analysts and developers need to understand what sort of results are expected from these tools and where they currently fall short. All of this builds to a more situationally cognisant intelligence community where individuals step beyond their specialised roles and understand the importance of their contributions to the overall project.

Our efforts against disinformation also require us to think carefully about its philosophy and how that relates to the nature of our own strategic narrative. To this end, it would be helpful to create an intelligence community that takes advantage of Canada's diversity. Individuals coming from the same backgrounds as our adversary nations could help

us understand the appeal behind disinformation narratives and what, in the end, compelled them to choose ours. This aligns with our ethical commitment to inclusion and is symbolic of the wider whole-of-society approach we have advocated for in this paper.

The disinformation case for a whole-of-society approach to national security is far from the only one. Other threats like the pandemic have proven the need for an integrated government strategy and increased intelligence sharing both within and outside government. What this paper has done is provide one argument, among many, that calls for a rethinking of Canada's national security policy. The importance of this endeavour cannot be overstated. Yet despite its urgency and sometimes, its direness, there is cause for optimism. The route painted in this paper to combat disinformation could end in not just a repudiation of foreign efforts to interfere in Canada but a rejuvenation of our precious liberal democracy.

Finally, this whole-of-society approach could signal a new method of thinking on national security policy. Part of living in a democracy means accepting a shared moral responsibility for its outcomes. By expanding the definition of national security and making each Canadian understand their integral role and contribution towards its mission, we make Canada a bit stronger and each Canadian a bit freer.

References

Angus, C. (2022, February 22). *Lessons from the Convoy: We Are Losing the War on Disinformation*. Centre for International Governance Innovation. Retrieved April 23, 2022, from https://www.cigionline.org/articles/lessons-from-the-convoy-we-are-losing-the-war-on-disinformation/

Artificial Intelligence, Big Data, and Change in the Canadian Intelligence Community. (2019, November). CASIS-ACERS. https://casis-acers.ca/wp-content/uploads/2020/01/2019-CASIS-Symposium-Summary.pdf

Babic, B., Cohen, I. G., Evgeniou, T., & Gerke, S. (2020, December 15). When Machine Learning Goes Off the Rails. *Harvard Business Review*. Retrieved April 26, 2022, from https://hbr.org/2021/01/when-machine-learning-goes-off-the-rails

Babic, B., Gerke, S., Evgeniou, T., & Cohen, I. G. (2021). Beware explanations from AI in health care. *Science*, *373*(6552), 284–286. https://doi.org/10.1126/science.abg1834

Bradshaw, S., & Howard, P. (2021, July). *The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation*. Oxford Internet Institute. https://www.oii.ox.ac.uk/news-events/reports/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/

Briant, E. (2022). Global Information and Digitalized Influence in a Data-driven World. *The Journal of Intelligence, Conflict, and Warfare*, *4*(3), 105–109. https://doi.org/10.21810/jicw.v4i3.4156

Burton, C. (2021). Canada's Relationship with China. In R. W. Murray & P. Gecelovsky (Eds.), *The Palgrave Handbook of Canada in International Affairs* (pp. 587–608). Palgrave Macmillan.

Canadian Security Intelligence Service. (2021, April). *CSIS Public Report 2020*. Public Works and Government Services Canada. https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report.html

Carvin, S. (2021a). *Stand on Guard: Reassessing Threats to Canada's National Security (Munk Series on Global Affairs)*. University of Toronto Press.

Carvin, S. (2021b, November 3–5). *The Post-Covid Information Environment* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=6CSfwmItxeM

Communications Security Establishment. (2021a, June). *Communications Security Establishment Annual Report 2020–2021*. https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021

Communications Security Establishment. (2021b, July). *Cyber threats to Canada's democratic process : July 2021 update*. Canadian Centre for Cyber Security. https://cyber.gc.ca/en/cyber-threats-canadas-democratic-process-july-2021-update

Dahl, E. J. (2021, November 3–5). *Warnings Unheeded: Intelligence Lessons from the Pandemic* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=6CSfwmItxeM

Davis, J. (2021, November 3–5). *The Structure of Canada's Intelligence Community: Prepared for a Precarious Future?* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=fqRVzpvh7C8

Directorate-General for Communications Networks, Content and Technology (European Commission). (2018, April). *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*. Publications Office of the European Union. https://data.europa.eu/doi/10.2759/0156

Geddes, T. (2021, November 3–5). *The Impact of the Pandemic on the National Security Community* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=EUGWkWiLVSg

Gilbert, D. (2022, March 4). *Millions of Leftists Are Reposting Kremlin Misinformation by Mistake*. Vice. Retrieved April 21, 2022, from https://www.vice.com/en/article/wxdb5z/redfish-media-russia-propaganda-misinformation

Hellman, M., & Wagnsson, C. (2017). How can European states respond to Russian information warfare? An analytical framework. *European Security*, *26*(2), 153–170. https://doi.org/10.1080/09662839.2017.1294162

Henley, J. (2017, November 28). *Russia waging information war against Sweden, study finds*. The Guardian. Retrieved April 23, 2022, from https://www.theguardian.com/world/2017/jan/11/russia-waging-information-war-in-sweden-study-finds

Hershkovitz, S. (2019, November). *The Future of Intelligence*. CASIS-ACERS. https://casis-acers.ca/wp-content/uploads/2020/01/2019-CASIS-Symposium-Summary.pdf

Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M., & Deibert, R. (2017, May). *Tainted Leaks Disinformation and Phishing With a Russian Nexus*. The Citizen Lab. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

Lim, G., Maynier, E., Scott-Railton, J., Fittarelli, A., Moran, N., & Deibert, R. (2019, May). *Burned After Reading Endless Mayfly's Ephemeral Disinformation Campaign*. The Citizen Lab. https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/

Lim, P. (2020). Sino-Canadian relations in the age of Justin Trudeau. *Canadian Foreign Policy Journal*, *26*(1), 25–40. https://doi.org/10.1080/11926422.2019.1641118

Linden, S. V. D. (2013, September 1). *Why People Believe in Conspiracy Theories*. Scientific American. Retrieved April 23, 2022, from https://www.scientificamerican.com/article/why-people-believe-conspiracy-theories/

Littlewood, J. (2020). The Canadian Security Intelligence Service. In S. Carvin, T. Juneau, & C. Forcese (Eds.), *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community* (pp. 45–71). University of Toronto Press.

Mackintosh, E. (2019, May). *Finland is winning the war on fake news. Other nations want the blueprint*. CNN. Retrieved April 23, 2022, from https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

Magnus, G. (2021, December 28). From economic miracle to mirage – will China's GDP ever overtake the US? *The Guardian*. Retrieved April 2, 2022, from https://www.theguardian.com/business/2021/dec/28/from-economic-miracle-to-mirage-will-chinas-gdp-ever-overtake-the-us

Mueller, R. (2019, April). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. US Department of Justice. https://www.justice.gov/archives/sco/file/1373816/download

National Security Transparency Advisory Group. (2020, November). *National Security Transparency Advisory Group Initial Report: What We Heard In Our First Year*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2020-nstag-irwwh/index-en.aspx

National Security Transparency Advisory Group. (2021, November). *The Definition, Measurement and Institutionalization of Transparency in National Security*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-dntn-msrmnt-trsprncy-ns/index-en.aspx

New Challenges for Strategic Intelligence – Canada, United States, Private Sector. (2019, November). CASIS-ACERS. https://casis-acers.ca/wp-content/uploads/2020/01/2019-CASIS-Symposium-Summary.pdf

NEWS WIRES. (2022, February 24). *Israeli air strikes kill three Syrian soldiers near Damascus, Syrian media says*. France 24. Retrieved April 21, 2022, from https://www.france24.com/en/middle-east/20220224-israeli-air-strikes-kill-three-syrian-soldiers-near-damascus-syrian-media-says

Open Government Partnership (OGP) Global Summit Summary of National Security Panels. (2019, May). Public Safety Canada. Retrieved April 25, 2022, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ogp-glbl-smmt/index-en.aspx

Paltiel, J., & Smith, S. N. (2020, October). China's Foreign Policy Drivers Under Xi Jinping: Where Does Canada Fit In? *Behind the Headlines*, *68*(11). Retrieved April 23, 2022, from https://thecic.org/chinas-foreign-policy-drivers-under-xi-jinping-where-does-canada-fit-in/

Press, J. (2022, February 25). *Documents show Trudeau warned of issues linked to "build back better" pledge*. CTVNews. Retrieved April 23, 2022, from https://www.ctvnews.ca/politics/documents-show-trudeau-warned-of-issues-linked-to-build-back-better-pledge-1.5796040

Rethinking Security: China and the Age of Strategic Rivalry Highlights from an Academic Outreach Workshop. (2018, May). Canadian Security Intelligence Service. https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry.html

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare* (Illustrated ed.). Farrar, Straus and Giroux.

Riehle, K. P. (2022). Information Power and Russia's National Security Objectives. *The Journal of Intelligence, Conflict, and Warfare*, *4*(3), 62–83. https://doi.org/10.21810/jicw.v4i3.3791

Rigby, V. (2021, November 3–5). *The Structure of Canada's Intelligence Community: Prepared for a Precarious Future?* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=fqRVzpvh7C8

Robinson, B. (2020). The Communications Security Establishment. In S. Carvin, T. Juneau, & C. Forcese (Eds.), *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community* (pp. 72–89). University of Toronto Press.

Schmitt, E. (2022, February 24). *US Carries Out First Airstrike in Somalia Since August*. The New York Times. Retrieved April 21, 2022, from https://www.nytimes.com/2022/02/24/us/politics/somalia-shabab-us-airstrike.html

Scott, M., & Cerulus, L. (2019, June 16). *Russian groups targeted EU election with fake news, says European Commission*. POLITICO. Retrieved April 23, 2022, from https://www.politico.eu/article/european-commission-disinformation-report-russia-fake-news/

Shull, A., & Wark, W. (2021, December). *Reimagining a Canadian National Security Strategy*. Centre for International Governance Innovation. https://www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/

Singh, A. (2021, November 3–5). *The Evolution of Canada's Threat Environment* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=6CSfwmItxeM

The White House. (2021, June 12). *FACT SHEET: President Biden and G7 Leaders Launch Build Back Better World (B3W) Partnership* [Press release]. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/12/fact-

sheet-president-biden-and-g7-leaders-launch-build-back-better-world-b3w-partnership/

UK Cabinet Office. (2021, March). *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*. The Crown. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

Vigneault, D. (2021, February 9). *Remarks by Director David Vigneault to the Centre for International Governance Innovation*. Canada.Ca. Retrieved April 23, 2022, from https://www.canada.ca/en/security-intelligence-service/news/2021/02/remarks-by-director-david-vigneault-to-the-centre-for-international-governance-innovation.html

Wark, W. (2021, November 3–5). *The Structure of Canada's Intelligence Community: Prepared for a Precarious Future?* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=fqRVzpvh7C8

When Election Interference Fails. (2020, January 29). Council on Foreign Relations. Retrieved April 23, 2022, from https://www.cfr.org/blog/when-election-interference-fails

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

Wilner, A. (2021, November 3–5). *Foresight for Intelligence: Preparing for a Precarious Future* [Presentation]. Security and Intelligence Studies Symposium, Ottawa, Canada. https://www.youtube.com/watch?v=fqRVzpvh7C8