SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

The securitisation of foreign disinformation

Nicole J. Jackson

nicole_jackson@sfu.ca

https://orcid.org/0000-0002-4108-2650

School for International Studies, Simon Fraser University, Hastings St, V6J4Y2, Vancouver, Canada

Abstract

This paper analyses the Canadian government's foreign and security policy responses to Russian disinformation in the context of the Russo-Ukrainian war. It asks whether, how, and why the government has securitised the "crisis of Russian disinformation." The paper first briefly reviews literature on the Copenhagen's School's "securitisation" theory and how it has been used to explain responses to other crises. It then adopts the framework to contextualise the Canadian federal government's official rhetoric, and then to categorise government policies and actions. The sources consulted include government actors' reports and stated intentions and policies from 2022 to 2024. Adopting a securitisation framework reveals that Russian disinformation has been rhetorically securitised by government actors as an existential threat to national security and democratic integrity which requires urgent action. Within a context of cascading risks, the government has taken a range of distinct yet reinforcing policies and actions, some more comprehensive than others. The paper argues that together this "pervasive rhetorical securitisation" and "ad hoc practical securitisation" comprise the Canadian government's ongoing process of partial securitisation. This process is legitimising different methods of governance: security and warfare communications (to address threats to national defence and security), democratic resilience (to address threats to democracy), and, most controversially, blocking and sanctioning (to signal discontent to the Russian regime). The analysis further reveals that each approach has different benefits and limits. The paper concludes that the securitisation process is incomplete compared to the government's rhetoric, with no over-arching organisation or strategy. It outlines implications for future research.

Keywords

securitisation, Russian disinformation, information manipulation, responses to foreign disinformation, Canada and the war in Ukraine

Article info
Received: 1 November 2023
Revised: 24 June 2024
Accepted: 25 June 2024
Available online: 1 August 2024

Citation: Jackson, N.J. (2024) 'The securitisation of foreign disinformation', *Security and Defence Quarterly*, 46(2), pp. 118–138. doi: 10.35467/sdq/190799.

Introduction

This paper investigates how the Canadian federal government has responded to Russian information manipulation[1] in general, and more specifically to Russian state disinformation,[2] in the context of the Russo-Ukraine war (ongoing since February 2022). This is an important question because Canada is one of the major international actors supporting Ukraine in the war, and Canada's most recent actions to counteract information manipulation have taken place within the context of this conflict. The war is being fought with traditional military weapons and also an array of non-traditional methods, including the manipulation of information and contests over control of information transmission. However, in Canada, foreign disinformation has only relatively recently become a major issue in public discourse. How has the government portrayed and responded, or not, to foreign disinformation to date during the current war in Ukraine? Why? What are the implications?

To better understand the Canadian federal government's responses specifically towards *Russian* disinformation, the paper first briefly reviews the literature on Copenhagen School's framework of "securitisation"[3] and how it has been used to explain responses to other crises. It suggests that applying a securitisation framework to disinformation can similarly highlight how the "crisis of disinformation" is rhetorically framed, and acted upon, as a "threat" to security and democratic integrity. The paper then adopts the framework, first to briefly explore Canada's official rhetoric, and second to categorise and analyse Canadian policies and actions.

While the author has previously examined Canadian government rhetoric on misinformation and disinformation from 2014 to 2020, here the federal government's *security and foreign policy*[4] rhetoric and actions specifically concerning Russian disinformation are analysed in the context of the war in Ukraine (February 2022 to date). The sources used to analyse these government responses include key government actors' reports, stated intentions and policies from 2022 to 2024 as well as relevant academic and policy papers.[5] The paper does not aim to outline all the evidence and controversies about

[1] *This paper uses "informational manipulation" as the broad term, including mis-, mal-, and disinformation. Overall, each category of mis-, dis-, and mal-information represents a type of informational manipulation. However, there is no one uniform definition of mis-, dis-, and mal-information, reflecting their complexity, how they are applied in different contexts, and the reality that they can be difficult to separate from one another. For the definitions used in this paper, for mis-, dis-, and mal-information, see FN 3.This paper further focuses on Russian state information manipulation, that is, information that originates from the Russian state or state-affiliated actors. However, the paper acknowledges the difficulties in drawing clear lines between foreign and domestic disinformation, given the intertwined nature of the information ecosystem, which also helps to explain some of the challenges confronting government responses. For a discussion of definitions, see Jackson (2022), Jacush (2022), Laidlaw (2022).*

[2] *This paper uses the UNESCO definition which states that disinformation is information that is false, and the person who disseminates it knows that it is false. Disinformation is deliberate, intentional, and thus includes when people are actively disinformed by malicious actors. Misinformation is information that is false, but the person who is disseminating it believes that it is true. Mal-information is the information that is based on reality, but used to mislead and inflict harm on a person, organisation, or country (Ireton, 2018). This paper uses Russia to mean Russian state-affiliated actors, although it does not dismiss the role of "lone wolf" dis-informers and Russian state inspired and recycled disinformation and misinformation.*

[3] *This is an extensive literature that examines, questions, and critiques securitisation as rhetoric or "speech acts" (Buzan et al., 1998) used to gain "a special right to use whatever means" (Wæver, 1995, p. 55). The Copenhagen School's securitisation framework highlights the different actors involved in articulating a threat, what they are labelling a threat (the "referent object"), the language they use, the "audience" they are addressing, and the different responses taken or not taken.*

[4] *As opposed to government attempts to regulate social media companies, for example, which are important but not addressed here.*

[5] *The main security and foreign policy departments and agencies in the government include Global Affairs Canada (GAC), the Ministry of Defence (MoD), Canadian Armed Forces (CAF), Canadian Security and Intelligence Services (CASIS), Department of Public Safety and Emergency Preparedness Canada, The Communications and Security*

Russian (or other) disinformation in Canada or in Ukraine. It contextualises Canada's counter-disinformation policies and actions and acknowledges that it can sometimes be hard to separate out responses to Russian disinformation related to war in Ukraine from responses to foreign disinformation in general. Nevertheless, the scope of the paper has been narrowed, where possible, to Canada's responses to Russia's deliberate disinformation as deployed on the battlefield in Ukraine and towards Russia's broader geopolitical information manipulation within the wider geopolitical conflicts.[6] This allows a focus on responses to Russian disinformation during the war in Ukraine.

The paper shows how and why, within a greater context of compounding crises, Canadian government's security and foreign policy actors have referred to Russian disinformation during the war in Ukraine as a threat to national security and democratic integrity as well as to other "referent objects," such as identity. These are perceived to be in danger and vulnerable to threats at multiple levels (individual, state, societal, and global). Simultaneously, in practice, many government actors have initiated distinct, yet reinforcing policies and have taken separate yet parallel actions in response to Russian disinformation in Ukraine.

I argue that together, this "pervasive rhetorical securitisation" and "ad hoc, practical securitisation" (my terms) comprise the Canadian government's ongoing *process* of *partial securitisation* of Russian disinformation. This process, while contributing to increasing public awareness and understanding, has increased communication and collaboration among government actors about Russian disinformation. Rhetoric and actions are legitimising different methods of governance: *security and warfare communications* (to address threats, national defence, and security), *democratic resilience* (to address threats to democracy, its individuals, society, and institutions), and, most controversially, *blocking and sanctioning* (to signal discontent to the Russian regime, and to impose costs and deter mostly Russian actors perceived to be instigating or heightening "the threat"). The paper's application of the securitisation framework highlights key benefits and limits and concludes that responses *overall* remain partially securitised.

The paper is organised as follows: First, it briefly examines key findings about how securitisation has been adopted as a framework to understand crises. It suggests that securitisation can help researchers to explain the evolution of government rhetoric and practical responses to foreign disinformation as well as to clarify their benefits and limits. The paper then adopts a securitisation lens to establish how Canada's government has rhetorically framed Russian disinformation during the war in Ukraine. Next, more comprehensively, it categorises and outlines the benefits and limits of Canada's multifaceted, yet still piecemeal responses.

Securitisation as a framework to understand government's rhetoric and responses to crises and their possible benefits and limits

To analyse Canada's responses, this paper draws on the Copenhagen School's framework of "securitisation," which examines how and why existential threats can

Establishment (CSE) as well as the Department of Canadian Heritage, and the decision-making bodies the Prime Minister's Office (PMO) and Privy Council of Canada (PCO).

[6] *As above, the paper acknowledges foreign disinformation's complex ties to related but inadvertent and not deliberate "diffusion" of misinformation and mal-information, that is, information based on an element of truth but used to mislead and harm. Moreover, it acknowledges the difficulties of drawing clear lines between foreign and domestic disinformation, given the complex nature of the information ecosystem.*

dominate political agendas during crisis situations and legitimise policies that would generally not be taken. Many scholars of securitisation are interested in how issues become labelled, or framed discursively, as urgent threats. They argue that it is not enough for an issue to be politicised for securitisation to occur. Rather, securitisation develops during a "state of exception" that gives rise to actions that would not normally be taken if it is accepted by a significant audience (Buzan *et al.*, 1998). Conversely, threats can be "de-securitised" or normalised, usually within a less exceptional context. Both securitisation and de-securitisation have been understood as processes, and scholars have explored how, over time, they can shape and legitimise different kinds of governance (whether more top-down or bottom-up, or more militarised or more democratic, for example), with different power dynamics (enabling some actors over others) and various levels of accountability.

There are controversies, including claims that securitisation is a western-centric concept that does not travel well to authoritarian states and that there is an absence of a gendered concept of security (Hansen, 2000). Securitisation has been critiqued for being a realist tool that elites use to harness people's fears and create policies for their own profit (e.g. Al-Arian, 2021), but it has also been argued that securitisation is often coupled with vulnerabilities as well as threats, and thus may reflect weaknesses and not strength (Markiewicz, 2023). Scholars continue to use, critique, and expand upon the original framework, arguing, for example for more contextualisation, more attention to how the audience engages in the securitisation process (Balzacq, 2005; Côté, 2016; Williams, 2011), and for further consideration of how different "performances" can address distinct audiences (Salter, 2008). The concept also continues to be adopted by scholars to explore *ethical* accounts ("progressive" or "regressive," or racist securitisations) for how and why some actors variously exceptionalise, normalise, or desecuritise specific challenges and their implications (Diez, 2023; Howell and Richter-Montpetit, 2020).

In this paper, securitisation is adopted as a tool to help analyse whether and how Russian disinformation has been understood as a threat or risk during the time of crisis (war in Ukraine), how the Canadian government responded, and what are the implications. An advantage of adopting securitisation as a framework is that it draws attention to specific actors (here, government actors) who address specific issues (the "referent object," in this case, Russian disinformation), and also to how they understand and frame the issue and act upon it. This includes exploring language and rhetoric, policies and "emergency" actions (other than what would be a normal process in that context) and the "audience" they are addressing (here, the Canadian public) (Buzan *et al.*, 1998). Many scholars, including the ones mentioned above, interrogate and critique securitisation and focus on the role of linguistic frames, discourse, or images to show how a threat is "constructed." For others, the securitisation process (also) includes the role of "governmental practices" that can spread "unease," apprehension or a feeling of heightened risk (Bigo, 2002). These practices can occur within both "routinised" (Adamides, 2020) and "everyday" actions (Bourbeau, 2014).

This paper focuses on how the Canadian government constructs and gives meaning to Russian disinformation, and argues that it does so through speech, policy, *and* action. It suggests that these are intertwined and together form the Canadian government's overall securitisation process. Of course, perceptions and insecurities are responsive to the material world, but they are also constructed (Diez, 2023). Therefore, to understand responses to disinformation, it is important to try to understand *what* Russia and other actors are doing and *why*, but it also matters how the Canadian government (alongside other key actors) understands, portrays, and responds to the challenge of disinformation through rhetoric, performances, or other actions.

The securitising framework is also used here to help highlight the possible benefits and limits of rhetoric and practices, and the dangers of both "over-securitising" and "under-securitising" a complex and evolving issue. The benefits of rhetorical securitisation have been shown to include "calling attention" to an issue that otherwise might have been neglected. This might result in new and more robust policies or actions that legitimise different forms of security governance, whether top-down and elite-centric or bottom-up and prioritising individuals over the collective (Diez, 2023). At the same time, exceptionalising an issue could lead to practical "over-securitisation" and the dominance of some actors and responses, to the detriment, for example of other more appropriate actors or more productive or ethical actions. More top-down and even less-accountable governance can be understood as necessary in a crisis to the detriment of long-term and human-centred considerations. Applied to disinformation, rhetorical "over-securitisation" could in theory construct a (false or hyper) state of emergency, instead of a heightened (and possibly justified) feeling of insecurity that provokes much needed action. In a perceived state of alarm, actions could be more easily justified that might harm freedom of speech or limit different or dissenting views (e.g. over-regulation, an extreme example of which would be to close off the Internet). In democracies, such as Canada's, such actions would be particularly counterproductive, and could harm the very democratic trust and credibility that disinformation threatens and that governments are seeking to foster and protect.

Conversely, rhetorically "under-securitising" disinformation might lead to public complacency (the "audience" might not accept the urgency or significance of the issue), lack of funding for critical research, or the disempowering of actors who may have unique skills and tools to address a crisis or a vulnerability. Applied to disinformation, a government's under-securitisation of the challenge might lead, for example to either no actions at all ("giving up" in the face of uncertainty and fears) or the absence of organisation and strategy necessary for a change. A lack of action could fail to bolster society's resilience to information manipulation, or fail to empower actors (civil society, private actors, government departments, etc.) with relevant skills. A key question, therefore, is how have Canadian government actors (along with other actors, since governments do not act in a vacuum) responded to disinformation during a time of crisis (here the Ukraine war), and have they responded without over- or/and under-securitising the challenge? What are the benefits and limits of securitising acts? Is the securitisation process incomplete or comprehensive?

The next section examines the Canadian government's official rhetoric about disinformation during the war in Ukraine and shows that national security and democracy are among a wide range of "referent objects" (to use the language of the securitisation framework) perceived to be at risk and vulnerable to informational manipulation, reflecting the government's many fears and uncertainty over how to respond. Of course, these government perceptions reflect a particular geopolitical context that includes Russia's actions in Ukraine (and beyond), and Canada's official interests in support of Ukraine. They also reflect evolving understandings about information manipulation challenges generally, based on new research and Canadian events.

Contextualising the Canadian government's rhetorical securitisation

The Canadian government's public expressions of concern about misinformation and disinformation in general, and more specifically Russian disinformation, did not begin with the current war in Ukraine. For approximately the past decade, including at least 8 years *before* Russia's invasion of Ukraine in February 2022, many governments, along with other public, private, and civil society actors actively considered, and widely debated, whether and how best to respond to a broad spectrum of information manipulation (Wardle and Derakshan, 2017) both domestic and foreign (Heer *et al.* 2021; Lesher *et al.*, 2022). The Canadian government participated in these debates, which evolved over time with increasing evidence and allegations of a wide range of Russian, and many other foreign (including, but not only, Chinese, Indian, and Iranian) and domestic actors' information manipulation as well as electoral and other interference around the world (there is an enormous amount of literature here, e.g. Bradshaw and Howard, 2018). As this author has previously argued, from 2014 (Russia's annexation of Crimea) onwards, the Canadian government began to label both deliberate foreign disinformation and more general misinformation as urgent security challenges while addressing its (mostly) Canadian audience (Jackson, 2018, 2022). The question here is how Canadian government rhetoric has continued to evolve since Russia's invasion of Ukraine in February 2022. This is important to understand because the securitisation framework suggests that when successful government rhetoric can convince audiences (here the Canadian public), spur on responses and shape outcomes.

Indeed, beginning with the days leading up to Russia's invasion, Canadian government rhetoric about disinformation noticeably increased and became (even) more focused on Russia. Confronted with Russia's military encirclement of Ukraine in February 2022, Canada, along with many of its allies, began to highlight and debunk Russian disinformation (at the time, Putin claimed that he would not invade) and to portray it as an existential threat to Ukraine and Ukrainians (their lives, sovereignty, freedom, and independence). As the war continued, the Canadian government increased its warnings to Ukrainians and Canadians, responding over time to Russia's evolving and multifaceted attempts to control communications and influence (e.g. the Canadian Centre for Cyber Security, 2022). Of course, Russia's brutal military actions in Ukraine explain why the Canadian government became increasingly united in its portrayal to the Canadian public of multiple threats related to Russia. In response, the Canadian government presented a clear and consistent understanding that Russia was waging an unjustified war and was spreading strategic disinformation. Russia's informational manipulation was perceived as integral to its many underlying aggressions and further justified Canada's official position to build solidarity and support for Ukraine, its people, and its sovereignty, and impose "costs" on Russia (Government of Canada, 2023e).

Canadian government rhetoric on Russian disinformation (as opposed to its rhetoric on the general topic of disinformation) therefore evolved and grew during this specific crisis, a war in which Russia, as well as other states and non-state actors, became increasingly known for trying to manipulate information in their favour (Organization for Economic Cooperation and Development [OECD], 2022). Russian state and Russian-affiliated actors used targeted disinformation on the battlefield in Ukraine to try to shape the military outcome and win the war on the ground (Martinez, 2024; McGlynn, 2023). There is also evidence that Russian actors manipulated information more generally to "win" (or retain their advantage over) the wider geopolitical conflict (Cadier, 2022; Erlich and Garner, 2023). In the latter examples, it can be reasonably speculated that Russia has tried to influence individuals' emotions and thinking about the war and the conditions necessary for peace to lessen support for Ukraine and shape decision-makers' actions or lack of action (even if the results of Russia's attempts remain disputed). The Canadian government website claims that Russia spreads disinformation for various reasons (to support its objectives, to discredit opponents, and to spread confusion or distrust) and through many means (official communications, state-sponsored media, social media, and proxy sources; Government of Canada, 2024a). False narratives, often built upon a "nugget of truth," deliberate "information flooding," and distractions have become common, as has the unwitting spread of misinformation (see, e.g. Fridrichová, 2023; Savelyev, 2024; Tolz and Hutchings, 2023). In these ways, the reach of Russian disinformation in the war has extended beyond verifiable disinformation. What are often subjective disagreements have been amplified, seemingly influencing individuals' perceptions (in this case, about the war). Moreover, within the rapidly and ever-evolving complex context of this war in which Canada and many other states have been indirectly involved, and the reality of constant and multi-directional information manipulation, the distinction between foreign and domestic has been blurred, adding to the many challenges of how to respond. The disinformation challenge, therefore, has extended from direct harm, which threatens human life on the battlefield, to more diffuse transnational effects, such as the erosion of trust in the information environment and in governments' actions. These findings are congruent with a large amount of literature which examines how Russia and other states and actors take advantage of the many means and effects of information manipulation as part of their "grey zone" or hybrid warfare activities to achieve geopolitical and strategic objectives.[7]

Beyond Russia's actions in Ukraine, the Canadian government's evolving responses on Russian disinformation have been further shaped by new evidence about Russia's involvement in compounding "polycrises," including food, energy, migration, and health as well as rising right-wing extremism and social polarisation (Lawrence *et al.*, 2022; Zeitlin *et al.*, 2019). Since Russia's invasion of Ukraine in 2022, there have been more allegations and more evidence linking Russia to "foreign interference" efforts (if not results) around the world. These include attempts to influence elections, transnational repression, intelligence leaks, and seemingly more aggressive hacks and cyberattacks. While similar evidence and speculations existed before the Russo-Ukraine war, more research and evidence appeared in these years, including about Russian actors' unsuccessful efforts to influence elections in Canada, their attempts to exploit the COVID-19 crisis (see, e.g. Bajaj and Momani, in press; Boucher *et al.*, 2022; Bridgman *et al.*, 2022; Fife and Chase, 2023; McQuinn *et al.*, 2023) and the Ottawa "Freedom Convoy" truck protests and blockades (Laidlaw, 2022; Orr Bueno, 2023). At the same time, there have been new public revelations concerning other foreign actors (Iranian, Chinese, and Indian) targeting and harassing Canadian Members of Parliament, prospective politicians, and members of Canada's diaspora communities (McMahon, 2023; Trauthig, 2024; Wark, 2024). Each of these examples of foreign influence or interference is unique and has involved different actors, targets, and means along the supply chain of information manipulation. The point here is that public revelations and discussions about information manipulation and foreign interference have further focused government's attention on the wider topic and contributed to the securitisation process by raising alarms about its complexity, speed, and reach.

Within these contexts of cascading risks, the Canadian government's threat perceptions expanded to a seemingly ever-wider range of "referent objects" at many levels (local, national, regional, and global; Government of Canada, 2022b). In an increasingly securitised environment of threats and perceived vulnerabilities, the government portrayed Russian disinformation specifically as a danger to Canada's international and security interests (geopolitical, economic, humanitarian as well as the "rules-based international order," the concept of sovereignty, self-determination, and inviolability of borders, and even territory in the Arctic) (House of Commons, Parliament of Canada, 2023). Beyond national and international security, Russian disinformation was referred to as a challenge to democracy in Canada and its allies and to institutions, such as free media and elections, as well as to individuals and societies' whose freedom was threatened by relying on a diminishing variety of reliable sources of news and information (Government of Canada, 2024f).

[7] *For a review of the hybrid warfare literature, see Johnson (2018), and on Russia in Ukraine, see, for example Bachmann, Putter and Duczynski (2023), Ionita (2023), Krainikova (2023).*

Canada's "ontological security" (Kinnvall, 2018), and its identity, norms and values were portrayed as being at risk. On the government website created to showcase Canada's extensive responses to the war in Ukraine, Russian disinformation was claimed to be undermining "peace, prosperity and individual freedoms" and to be "harmful" "especially in times of crisis" (Government of Canada, 2023a).

To sum up, Russian disinformation during the war to date (mid 2024) has been rhetorically securitised because it was presented as an existential threat with the clear implication that substantial responses were needed. Indeed, the government directly attributed its wide-ranging concerns about the Kremlin's use of disinformation during its invasion of Ukraine as an explanation for "why we are stepping up efforts to counter disinformation at home and abroad using a fact-based approach that is rooted in transparency" (Government of Canada, 2023b). Russian disinformation was not a subject of political contestation (unlike the wider and more fraught topic of foreign interference on which decision-makers did not so closely echo the language of security and intelligence practitioners). However, there is a theoretical danger, highlighted by the securitisation framework, that Russian disinformation may have been too widely rhetorically securitised (i.e. with too many referent objects said to be at risk). This may diminish trust in government if it is perceived as not taking robust actions that live up to the promises of its rhetoric.

Below we ask whether the Canadian government's actions during war in Ukraine have been consistent with this expansive rhetoric? Have new policies and actions widely (or partially) securitised Russia disinformation and how? Are they legitimising new practices?

The Canadian government's practical securitisation: Security and warfare communications, democratic resilience, and blocking and sanctioning

Just as Russia's invasion of Ukraine in February 2022 propelled new government rhetoric and public discourse on the topic of foreign disinformation, it also inspired many government actors to further develop policies and take new actions. Before 2022, the focus had been on Canadian elections and how to protect them (Jackson, 2022). Since then, new legislation on elections has been proposed,[8] but many other responses have related more directly to Russian actions in the war in Ukraine. This section uses the securitisation framework to explore how different government actors have responded to different threats that disinformation may pose and whether they have extended or created new policies and actions. This reveals major policies and actions within the government's process of ad hoc practical securitisation. Along with the accompanying "pervasive rhetorical securitisation" examined above, these practices are legitimising three major methods to manage disinformation during the war: (1) Security and warfare communications (focused on threats to Ukrainian national security and defence), (2) democratic resilience (focused on threats to Ukrainian and Canadian democracy, its individuals, society, and institutions), and (3) blocking and sanctioning (focused on signalling disapproval to supporters of Putin's regime and their information manipulation in the war). The paper highlights the benefits

[8] *For example, most recently proposed amendments to the Canada Elections Act, including expanding the ban on foreign influence during the election period to vote or refrain from voting for a particular candidate or party to include potential candidates and to always apply, as well as clarifying prohibitions on impersonation and false statements to affect election process or results include content created by AI Democratic Institutions: "Proposed Amendments to the Canada Elections Act" (Government of Canada, 2024b).*

and drawbacks within each of these categories. It shows that while securitisation practices have a wide scope, some are partial and incomplete (and could benefit from more action), while others are comparatively comprehensive.

(1) Bolstering *security and warfare communications and democratic resilien*ce in Ukraine

First, the war in Ukraine and the urgent need to "respond to the aggressor" have spurred new and decisive top-down actions, particularly in information gathering and sharing, and in communications to protect national security and democratic resilience in Ukraine. Perhaps unsurprisingly in the context of war (which is a "hyper state of emergency"), these securitising "acts" have been some of the most comprehensive taken by the Canadian government and they are in the process of legitimising new methods to respond to disinformation during conflicts. Adopting a securitisation lens also emphasises that these (still democratic) actions are both justified and incomplete, given the enormous scale of the challenge and in reference to the expansive rhetorical securitisation explored above.

Canada's Armed Forces (CAF) and the civilian Department of National Defence have spearheaded Canada's responses in Ukraine. These have mostly focused on helping to strengthen Ukraine's military and security communications and information gathering. However, a range of other Canadian government actors have also taken initiatives aimed at bolstering Ukraine's democratic and societal resilience. Most of these efforts have taken place within and alongside wider international efforts to support Ukraine in the war (Jackson, 2024).

On the battlefield, which includes most of Ukraine, manipulated information can be an existential threat, a matter of life and death. Canada's military and security responses have therefore aimed to help create, share, and promote an accurate understanding of facts "on the ground" in the war. Early recognition of this challenge came in 2014, with Russia's annexation of Crimea, and led to Canada training 35,000 members of the Ukrainian army and security forces. The training included how to use surveillance to establish facts on the ground and how to take down Russian radars and drones (Department of National Defence [DND], 2022). Subsequently, as part of Canada's multifaceted assistance to support Ukraine's defence and security, and in support of North Atlantic Treaty Organization's (NATO) Operation REASSURANCE, the CAF, the DND, the Communications Security Establishment Canada (CSE), and Telesat sent Ukraine military equipment, including drone cameras and (funding for) high resolution satellite imagery (Aiello, 2023). Today, Canada's military securitisation is set to continue with the new federal budget (2024) pledging $3.5 billion to expand Operation REASSURANCE and another $4 billion in military assistance to Ukraine. Canada's military presence in Latvia is also to be doubled from 1000 to 2200 troops by 2026, supported with new military equipment (Trudeau, 2024b). While this paper does not examine effectiveness, questions remain whether Canadian responses in Ukraine can be expanded with the new promised funding, and whether other actions are missing (e.g. more aggressive and controversial top-down actions, such as pre-emptive cyber attacks).

Both the CSE and DND have further contributed to greater efforts to bolster Ukraine's technical resilience, for example in cyber space, an enabler of Russian dis(information) and a target in the war (DND, 2023). The CSE has been able to increase its manoeuvrability in this war since the 2019 CSE Act allowed "active, defensive" responses to foreign actors outside Canada, although the details of its actions abroad remain secret.[9] Beyond providing this technical aid and equipment, Canada helped to further strengthen Ukraine's strategic communications capacity. As explored below, Canada did this while aligning its own official messaging on Russian disinformation with that of its NATO allies and other coalition partners. Most obviously successful here were the "pre-emptive" selective declassification of intelligence and the public sharing of information by the United States and its allies (including Canada) to "debunk" Russia's (especially early) war plans (Edelman, 2022).

Simultaneously, Canadian government's actions have aimed to reinforce Ukrainian civilians' immediate and longer-term democratic "resilience" to Russian distortions and lies, and to increase awareness and share accurate information. For example, Global Affairs Canada's (GAC) Peace and Stabilisation Operations Programme (PSOPs) and Canadian development assistance and loans supported activities highlighting facts concerning Russian actions in the war (Government of Canada, 2024c). Canada also continued its contributions to international efforts to strengthen Ukraine's information and media environment, providing more direct support to civil society and human rights organisations (Trudeau, 2024a). Equally significant, Canada collaborated with Ukrainian and international partners to provide evidence in support of allegations of Russian war crimes, crimes against humanity and genocide. For example, Canada supported the Organisation for Security and Cooperation in Europe's (OSCE) fact finding mission (FFM), referred the situation to the International Criminal Court (ICC), and aided Ukraine's application against Russia to the International Court of Justice (ICJ). Canada also co-sponsored and advocated for UN General Assembly resolutions that condemned Russia's aggression against Ukraine, censured the resulting humanitarian consequences, and suspended Russia from the Human Rights Council (HRC). These are the attempts to increase the *social costs* of norms, for example through the "calling out" of bad behaviour, and to increase the *negative costs* by imposing or augmenting reputational costs to incentivise restraint (Wilner, 2011, 2014).

The benefits of these acts of practical securitisation are that the military and civilian actors are working separately but in parallel alongside Canada's allies to help Ukrainians obtain, communicate, and share accurate information. Military and security actors have unique skills and knowledge relevant to countering information manipulation. Canadian civilian actors have positively contributed to immediately countering Russian disinformation (by providing facts and context) and to longer-term bolstering of democratic resilience. At the same time, the war and the information manipulation (from Russia and other actors) are continuing, and Canada could profit to expand these steps to deter disinformation (Jackson, 2024). Adopting a securitisation lens, however, also warns that responses (progressive securitisations) should be mindful of unintended consequences and to carefully protect freedom of speech and legitimate dissenting views (which the Ukrainian government has tried to control, for example through national broadcasts. This may be understandable in the middle of the war but may have negative consequences over time).

[9] *In June 2019, the Canadian government passed major national security legislation, including outlining how the CSE could lawfully operate. Those updates are found in Bill C-59, The Communications Security Establishment Act: National Security Act, 2017 (House of Commons, Parliament of Canada, 2019).*

(2) Strengthening *democratic resilience to* protect Canada's *democracy*

The second method of governance being legitimised by Canada's securitisation process includes actions designed to strengthen Canada's democratic resilience. Indeed, most Canadian actions are about immediately responding at home to Russian rhetoric about the war while also bolstering long-term protection of Canada's democracy, including its individuals, society, and institutions, which are perceived to be threatened.

Actions therefore have been taken within Canada that focused primarily on a domestic audience. Here, a growing range of government actors have joined in the effort to bolster individual and societal resilience through monitoring, reporting, coordinating, and educating. They have sought to develop more public awareness about disinformation regarding Russia and Ukraine by modernising strategic communications; developing institutional resilience through better monitoring, sharing, and coordinating information within both government and internationally; and promoting healthier information ecosystems by supporting media and educational programmes. Thus, a range of new policies that are reflective of the government's rhetoric of securitisation have been initiated, strengthened, organised, and funded. However, the securitisation of Canada's democratic resilience remains ad hoc and limited, both in comparison with the government's expansive rhetoric and in light of its stated need to build "whole of government" or "whole of society" responses. As a recent CSE document argues that Canada can expect unprecedented activity by foreign actors in its cyber and information space and more can be done (Communications Security Establishment Canada [CSE], 2023).

Since Russia's invasion of Ukraine, Canada has increased its efforts to debunk disinformation in the war and to promote and share a "common set of facts" or shared understanding of the "threat landscape." These actions are inherently political and aligned with the government's rhetorical securitisation and its condemnation of Russia's "unprovoked and unjustified" military actions. Over time, Canadian government departments and agencies have joined in an increasingly unified, if still largely ad hoc, strategic communications effort to expose, refute, and delegitimise Russian state's justifications, narratives, and other communications about the war. The Canadian government has published fact sheets to counter falsehoods and misleading narratives, and regularly updates a website that outlines Russian "false claims" about the invasion alongside "government approved facts" (Government of Canada, 2024d). The CSE has used social media, including Twitter, to expose and counter Russian "false claims" and doctored images on state and social media (CSE, 2022). Abroad, Canadian embassies and Canada's Task Force Latvia, for example, have also increased their public outreach efforts to counter "malicious" narratives, including those designed to undermine Canada's support for Ukraine, for example, claims that NATO instigated the war (Wattie, 2020). Other government actors have worked bilaterally, for example with the United Kingdom, the United States, Japan, and Germany, to further develop global public awareness about disinformation regarding the war in Ukraine and citizens' possible exposure to it.

While the reach of these efforts may be limited (e.g. there is no research about how many Canadians check the government websites or how their thinking is affected), the messages are echoed by media and regional organisations in Canada and its allies. For example, since the war, NATO, and the European Union (EU) (through its EastStratCom Task Force's EU vs Disinfo) have added to their databases and websites of debunked Russian state narratives and lies. As a result, Canadian (and western) public awareness about disinformation has likely grown as government communicators, whether from GAC and Canadian Forces Intelligence Command, have become more active, especially on social media. These recent advancements are welcomed by some, including those concerned by earlier scandals involving CAF and DND strategic communications (Boudreau, 2022). However, the military's practical securitisations have also been criticised for being woefully inadequate to the challenge and partial in their narrow focus on Russia in Ukraine (Boudreau, 2023). Some experts therefore continue to argue for more consistent and contextualised real-time government communications to tackle disinformation in general (Waldman, 2023). However, exactly what types of messages are acceptable, and from whom and how to best deliver them without fuelling societal mistrust, remains up for debate.

The Canadian government has also continued to increase its *institutional* efforts and strengthened partnerships to better monitor and share information about mis/disinformation in general, and to coordinate responses, both within the government and internationally. Most prominently, after Russia's invasion, GAC's Rapid Response Mechanism (RRM), which coordinates roles of the Group of Seven (G7), and shares reports and best practices, was awarded a further $13.4 million over 5 years "to further strengthen coordination between countries in identifying, and responding to, foreign threats to democracy, including state-sponsored disinformation" (Government of Canada, 2023c). The RRM has since increased its engagement with civil society and social media platforms, and in August 2022, an East European unit was formed as part of new Canadian measures designed to support Ukraine and punish Russia through deeper international collaboration (CTV News, 2022). The RRM provides a model for other Canadian departments seeking more collaboration and coordination, although its securitising actions have been limited in the sense that they have largely (but not only) focused on Russia. The new but small Protecting Democracy Unit inside the Privy Council of Canada (the main body that reports directly to the Prime Minister's Office) may be able to improve communication and coordination, especially between bureaucrats (intelligence providers) and policy-makers, which have been found to be lacking on the broader topic of foreign disinformation and interference (Juneau and Carvin, 2024). Of course, it is difficult to develop overall government accountability because disinformation is a "whole of government" (and society) challenge.

The government has also expanded other institutional partnerships dealing with disinformation internationally, but these remain limited to mostly Canada's close allies. For example, through its role in both the G7 and NATO, Canada now shares information with the EU through the Rapid Alert System (RAS) on disinformation and has expanded its participation with NATO's Strategic Communications Centre of Excellence and the Hybrid Centre of Excellence, both of which have added a focus on disinformation in the Ukraine war. In another example, in September 2023, Canada launched the Global Declaration on Information Integrity Online at the United Nations. Signed by twenty-seven countries, it promises steps towards establishing norms and measures, including legislation, to address information integrity and platform governance (Government of Canada, 2023f). Canada has also developed bilateral initiatives, for example with Germany, Japan, and France, as well as with NGOs, such as the United States' *Alliance for Securing Democracy* and the United Kingdom's *Resist*, to further develop global public awareness about disinformation regarding the war in Ukraine and citizens' possible exposure of it. Although it is too early to judge the effectiveness of these and other multilateral actions they are promising, largely because they address the transnational nature of the challenge.

There are also other major government-sponsored efforts, but they are outside the foreign and security scope of this paper. These include promoting a healthy media ecosystem[10] and encouraging critical thinking through education.[11] Such efforts are part of a widely defined, widely touted but still fragmentary and incomplete "whole of society" security approach that also includes global partnerships, such as the Media Freedom Coalition, the High-Level Panel of Legal Experts on Media Freedom, as well as Heritage Canada's Digital Citizen's Initiative, whose 2.5 million call for proposals targets Ukraine specifically and funds initiatives that help people identify misinformation and disinformation online (Trudeau, 2022). To quote a government website, "We know an engaged and informed public is the best line of defence in our efforts to fight disinformation and protect our democracy" (Heritage Canada, 2022). Yet this nascent approach, which gives agency to people rather than the government, remains underdeveloped (especially in comparison with countries, such as Finland).

(3) Blocking and *sanctioning*

The third and the most controversial approach to disinformation includes the government's attempts to block and sanction. Rather than being focused on protection from threats to Ukraine or to Canada's democracy, these actions are targeted at signalling disapproval to supporters of Putin's regime and their information manipulation in the war. Specifically, this is done by government blocking media outlets and sanctioning "disinforming agents." Adopting the lens of securitisation here focuses attention on unanswered questions. Are these the most appropriate responses, have they been consistently applied, and what are the possible unintended consequences, including for government trust and credibility?

In March 2022, after Russia invaded Ukraine, the Canadian Radio-television and Telecommunications Commission (CRTC) removed Russian state-directed Russia TV (RT) and RT France from the list of non-Canadian programming services and stations authorised for distribution in Canada. As a result, broadcasters in Canada are no longer legally permitted to carry the channel whose misinformation and disinformation was, and still is, claimed by the government not to be "in the public's interest" nor consistent with Canada's broadcasting standards because it is "undermining Ukrainian sovereignty" and "threatening Canadian democracy" (Canadian Radio-television and Telecommunications Commission [CRTC], 2022). This is an attempt to technically deny disinformation and also to deter by "punishment" because it penalises and makes a negative example of RT's choice of content and its failure to adhere to journalistic norms. It demonstrates political will to support Ukraine, although it may have limited effects because RT's information is reposted on other platforms. It also risks raising public scepticism because these actions are not uniformly applied to other "news" agencies (Jackson, 2024).

Since the beginning of war in Ukraine, the Canadian government has also threatened and imposed "costs" on the perpetrators of disinformation. As part of a broader coalition, Canada's government has imposed targeted sanctions in the information realm against mostly Russian as well as Ukrainian and Belarusian "agents of disinformation." These have included members of Russia's elite and close associates of the regime and their family members, state media organisations, such as TASS, Sputnik, Ria Novosti, Russia's

[10] *For example, championing free and fair media, Canada became co-chair with The Netherlands of the Media Freedom Coalition, and in July 2019, as inaugural co-chair along with the United Kingdom, Canada helped to initiate the high level panel of legal experts on media freedom.*

[11] *Since 2020, the government has funded to the tune of $8.5 million for a whole series of programmes, including the Digital Citizen Initiative (Canadian Heritage, 2022).*

department of defences' TV Zvezda, and think tank Russkiy Mir Foundation.[12] The sanctions charges have included "spreading and sanctioning disinformation and propaganda," "attempting to justify Russian attempts to annex part of Ukraine," "assisting the Russian regime in undermining the principles of state sovereignty," and being "responsible for spreading false narratives that serve as pretexts for the Russian regime's unjustifiable war" (Government of Canada, 2022a). These sanctions continue to be imposed to date (2024), and while they demonstrate political will to support Ukraine and limit its ability to garner support for its war, blocking and sanctioning may also "over-securitise" and fuel societal mistrust about the role of government in regulating the freedom of speech.

Conclusion: Assessing Canada's responses through the securitisation framework

To sum up, the paper contributes to the sparse academic literature about Canada with an original analysis that uses the framework to explain and make key critiques of the government's rhetoric and actions. It shows that the Canadian government's threat construction is an ongoing process in which many government actors have rhetorically and practically exceptionalised "the crisis of Russian disinformation" within a context of cascading risks. Overall, Canadian government actors in foreign and security fields have partially securitised Russian disinformation during the war in Ukraine through "pervasive rhetorical securitisation," and "ad hoc practical securitisation," coming from a place of vulnerability not strength (Markiewicz, 2023). Russian disinformation has been rhetorically securitised in that it has been presented to the public as an existential threat to Canadian and Ukrainian national security and democratic integrity which requires urgent new steps. This has helped to shatter any existing complacency and propel new policy.

Simultaneously, the government has taken ad hoc and parallel actions, which, while still incomplete, fit within the government's increasingly urgent and wide threat articulation. It has empowered and funded some foreign and security government actors which have spurred further new (still democratic) actions. Together, ad hoc practical securitisations and rhetorics are legitimising new short- and long-term approaches to manage the challenge: top-down security and warfare communications management as seen in the responses in Ukraine; government-sponsored bottoms-up democratic resilience to protect Ukrainians and Canadians and their institutions; and government blocking and sanctioning to signal deterrence to the Russian regime.

Nevertheless, Russian disinformation remains only partially securitised. This is because practical securitisation acts have been carried out but the process is incomplete, compared to the government's own very wide threat construction. Government's actions are fragmentary, some are more partial and some are more comprehensive. Applying a lens of securitisation also reinforces the argument that more can (and must) be done to manage this enormous, complex, and evolving challenge. However, at the same time, it warns of the government's limits in addressing different aspects of the challenge and calls attention to possible unintended consequences. These include unethical "regressive" securitisations that may harm freedom of speech by limiting debate and dissenting views being heard and challenged, and that may also undermine the government's credibility.

Finally, despite many advancements, Canada's securitisation process also remains *overall* under-securitised in that there is neither an over-arching organisation nor an ethical or

[12] The Government of Canada maintains a searchable database of sanctions imposed since Russia's invasion. (Government of Canada, 2024e).

long-term strategy to respond to Russian disinformation (let alone to foreign disinformation, which has until recently received much less attention[13]). Canada's new Defence Strategy (2024) acknowledges that in a time of increasing strategic competition, adversaries can exploit vulnerabilities in the cyber and information domains through hybrid or grey zone attacks (DND, 2024, p. 20) and that new defence approaches are needed (DND, 2024, p. 46). There is an opportunity to develop a "whole of government" framework or strategy to address foreign disinformation.

This paper also contributes to the literature on the Copenhagen School's securitisation framework by applying it to responses to Russian disinformation in the context of the war in Ukraine. This case study reinforces the literature that explores securitisation as a complex process that includes both rhetorical and practical securitisations. It shows that the securitisation process can include more partial and more comprehensive acts. It can legitimise different approaches, each with its own benefits and limits. While acts of securitisation may occur, the overall process may still be incomplete or under-securitised. Here, the securitisation process is reflective of the language of "urgency" and the threats and vulnerabilities portrayed. However, it remains overall incomplete in addressing the depth and range of the "referent objects" at risk, and unfinished due to the lack of overall organisation and strategy.

A limitation of this paper is that, for reasons of scope, it does not include an exploration of other actors (private actors, other governments, etc.) involved in responding to disinformation. Future scholars could research these areas, including how different audiences are engaging in the securitisation process. It also remains to be seen whether, over time, actions to confront disinformation fundamentally change the governance of the challenge or are simply performances which lead to change that is not sustained and to policy that is not robust.

Funding

This research received no external funding.

Data Availability Statement

Not applicable.

Acknowledgements

The author gratefully acknowledges the journal's two referees for their careful comments on two drafts. Information from a couple of sections of this paper will be published in the author's chapter in a forthcoming referred book by Bajaj and Momani (Jackson, In press).

Disclosure statement

No potential conflict of interest was reported by the author.

The author read and agreed to the published version of the manuscript.

References

Adamides, C. (2020) *Securitization and desecuritization process in protracted conflicts: the case of Cyprus.* Cham: Palgrave. doi: 10.1007/978-3-030-33200.

Aiello, R. (2023) 'Here is how Canada spent $1 billion in military aid for Ukraine since the war began', *CTV News*, 23 February. Available at: https://www.ctvnews.ca/politics/here-is-how-canada-spent-1b-in-military-aid-for-ukraine-since-the-war-began-1.6286404 (Accessed: 21 June 2024).

[13] *Bill C-70 received royal assent on 24 June 2024. It introduces the Foreign Influence Transparency and Accountability Act (FITAA) and new legislative amendments which add to the government's new toolkit to counter foreign interference.*

Al-Arian, A. (2021), 'The "war on terror" and the disciplining of American Muslims', *Al Jazeera.* Available at: https://www.aljazeera.com/opinions/2021/9/11/the-war-on-terror-and-the-disciplining-of-american-muslims (Accessed: 21 June 2024).

Bajaj, S.G. and Momani, B. (In press) *Misinformation, disinformation and democracy in the digital age: A Canadian perspective.* Toronto: University of Toronto Press.

Balzacq, T. (2005) 'The three faces of securitization: Political agency, audience and context', *European Journal of International Relations*, 11(2), pp. 171–201. doi: 10.1177/1354066105052960.

Bigo, D. (2002) 'Security and immigration: Toward a critique of the governmentality of unease', *Alternatives*, 25(S1), pp. 63–92. doi: 10.1177/03043754020270S105.

Boucher, J.-C., Edwards, J., Kim, J., Badami, A. and Smith, H . (2022 June) 'Disinformation and Russia-Ukrainian war on Canadian social media,' *SPP Briefing Paper*, 15, p. 16. Calgary, Alberta: School of Public Policy Publications, University of Calgary.

Boudreau, B. (2022) *The rise and fall of military strategic communications at national defence 2015–2021: A cautionary tale for Canada and NATO, and a roadmap for reform.* Calgary, Alberta: Canadian Global Affairs Institute.

Boudreau, B. (2023) *Understanding DND/CAF research and capability needs to deter and limit the impacts of (adversary) (dis)information: A critical self-examination.* Ottawa, Ontario: Defence and Research Development Canada (DRDC).

Bourbeau, P. (2014) 'Moving forward together: Logics of the securitization process', *Millenium: Journal of International Studies*, 43(1), pp. 187–206. doi: 10.1177/0305829814541504.

Bradshaw, S. and Howard, P.N. (2018) 'The global organization of social media disinformation campaigns', *Journal of International Affairs*, 71(1.5), pp. 23–32.

Bridgman, A., Lavigne, M., Baker, M., Bergeron, T., Bohonos, D., Burton, A. et al. (2022) *Mis- and disinformation during the 2021 Canadian Federal election*, final report of the Canadian Election Misinformation Project, Media Ecosystem Observatory, March 31. Available at: https://www.mediatechdemocracy.com/all-work/mis-and-disinformation-during-the-2021-canadian-federal-election (Accessed: 21 June 2024).

Buzan, B., Wæver, O. and de Wilde, J. (1998) *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner, pp. 1–240. doi: 10.1515/9781685853808.

Cadier, A., Roache, M., Tewa, S., Labbe, C., Padovese, V., Schmid, R., O'Reilly, E., Richter, M. et al. (2022) *Russia-Ukraine disinformation tracking center*. News Guard. Available at: https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/ (Accessed: 2 November 2022).

Canadian Centre for Cyber Security (2022) *National cyber threat assessment 2023–2024*. Canadian Centre for Cyber Security. Available at: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024 (Accessed: 21 June 2024).

Canadian Heritage (2022) *Government of Canada reinforces support to organizations to help counter harmful disinformation*, News release, March 16. Available at: https://www.canada.ca/en/canadian-heritage/news/2022/03/government-of-canada-reinforces-support-to-organizations-to-help-counter-harmful-disinformation.html (Accessed: 21 June 2024).

Canadian Radio-television and Telecommunications Commission (CRTC) (2022) *Broadcasting decision 2022-68*, March 16. Available at: https://crtc.gc.ca/eng/archive/2022/2022-68.htm (Accessed: 1 May 2023).

Communications Security Establishment Canada (CSE) (2022) *Update on Russia-backed disinformation*. Available at: https://x.com/cse_cst/status/1514246874890395654 (Accessed: 21 June 2024).

Communications Security Establishment Canada (CSE) (2023) *Cyber threats to Canada's democratic process: 2023 update*. Available at: https://www.cyber.gc.ca/sites/default/files/cyber-threats-canada-democratic-process-2023-update-v1-e.pdf (Accessed: 21 June 2024).

Côté, A. (2016) 'Agents without agency: Assessing the role of the audience in securitization theory', *Security Dialogue*, 47(6), pp. 541–558. doi: 10.1177/0967010616672150.

CTV News (2022) *Canada to create team to counter Russian disinformation: Trudeau*, 23 August. Available at: https://www.ctvnews.ca/politics/canada-to-create-team-to-counter-russian-disinformation-trudeau-1.6038389 (Accessed: 21 June 2024).

Department of National Defence (DND) (2022) *Defence Minister Anita Anand announces deployment of Canadian armed forces to train Ukrainian soldiers in the United Kingdom*, 4 August. Available at: https://www.canada.ca/en/department-national-defence/news/2022/08/defence-minister-anita-anand-announces-deployment-of-canadian-armed-forces-to-train-ukrainian-soldiers-in-the-united-kingdom.html (Accessed: 1 February 2023).

Department of National Defence (DND) (2023) *Operations*. Available at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-plans/departmental-plan-2023-24/planned-results/operations.html (Accessed: 1 April 2023).

Department of National Defence (DND) (2024) *Our north, strong and free: A renewed vision for Canada's defence*. Available at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html (Accessed: 21 June 2024).

Diez, T. (2023) 'Progressive and regressive securitisation: Covid, Russian aggression and the ethics of security', *Central European Journal of International and Security Studies*, 17(2), pp. 22–43. doi: 10.51870/PXRR478.

Dov Bachmann, S.-D., Putter, D. and Duczynski, G. (2023) 'Hybrid warfare and disinformation: A Ukraine war perspective'. *Global Policy*, 14, 858–869. doi: 10.1111/1758-5899.13257.

Edelman, E.S. (2022) *The pros and cons of 'deterrence by disclosure'*, The Dispatch, 21 February. Available at: https://thedispatch.com/article/the-pros-and-cons-of-deterrence-by/ (Accessed: 21 June 2024).

Erlich, A. and Garner, C. (2023). 'Is pro-Kremlin disinformation effective? Evidence from Ukraine', *The International Journal of Press/Politics*, 28(1), pp. 5–28. doi: 10.1177/19401612211045221.

Fife, R. and Chase, S. (2023) *China views Canada as a 'high priority' for interference: CSIS report*, Globe and Mail, 1 May. Available at: https://www.theglobeandmail.com/politics/article-china-targets-mps-csis/ (Accessed: 21 June 2024).

Fridrichová, K. (2023). 'Mugged by reality: Russia's strategic narratives and the war in Ukraine.' *Defense & Security Analysis*, 39(3), pp. 281–295. doi: 10.1080/14751798.2023.2201018.

Government of Canada (2022a) *Canada sanctions additional Russian propaganda agents*, 17 October. Available at: https://www.canada.ca/en/global-affairs/news/2022/10/canada-sanctions-additional-russian-propaganda-agents.html (Accessed: 20 November 2022).

Government of Canada (2022b) *National cyber threat assessment 2023–2024.* Available at: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024 (Accessed: 21 June 2024).

Government of Canada (2023a) *Economic, humanitarian and development assistance, and security and stabilization support – Russia's invasion of Ukraine*. Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-dev.aspx?lang=eng (Accessed: 1 March 2023).

Government of Canada (2023b) *Canada's efforts to counter disinformation – Russian invasion of Ukraine.* Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng (Accessed: 10 January 2023).

Government of Canada (2023c) *Rapid response mechanism Canada: Global affairs Canada.* Available at: https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng (Accessed: 2 March 2023).

Government of Canada (2023e) *Canada and the Russian invasion of Ukraine.* Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-situation.aspx?lang=eng (Accessed: 21 June 2024).

Government of Canada (2023f) *Global declaration on information integrity online.* Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/declaration_information_integrity-integrite.aspx?lang=eng (Accessed: 21 June 2024).

Government of Canada (2024a) *Russia's use of disinformation and information manipulation.* Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng (Accessed: 21 June 2024).

Government of Canada (2024b) *Proposed amendments to the Canada Elections Act.* Available at: https://www.canada.ca/en/democratic-institutions/news/2024/03/proposed-amendments-to-the-canada-elections-act.html (Accessed: 21 June 2024).

Government of Canada (2024c) *Agreement on security cooperation between Canada and Ukraine.* Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/agreement-ukraine-accord.aspx?lang=eng (Accessed: 21 June 2024).

Government of Canada (2024d) *Countering disinformation with facts – Russian invasion of Ukraine*. Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng (Accessed: 21 June 2024).

Government of Canada (2024e) *Sanctions – Russian invasion of Ukraine*. Available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-sanctions.aspx?lang=eng (Accessed: 21 June 2024).

Government of Canada (2024f) *Protecting Canada's democratic institutions*. Available at: https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions.html (Accessed: 21 June 2024).

Hansen, L. (2000) 'The little Mermaid's silent security dilemma and the absence of gender in the Copenhagen School', *Millennium,* 29(2), pp. 285–306. doi: 10.1177/03058298000290020501.

Heer, T., Heath, C., Girling, K. and Bugg, E. (2021) *Misinformation in Canada: Research and policy options*, Evidence for Democracy, 27 May. Available at: https://evidencefordemocracy.ca/sites/default/files/reports/misinformation-in-canada-evidence-for-democracy-report_.pdf (Accessed: 1 March 2023).

Heritage Canada (2022) *Government of Canada reinforces support to organizations to help counter disinformation*, 16 March. Available at: https://www.canada.ca/en/canadian-heritage/news/2022/03/government-of-canada-reinforces-support-to-organizations-to-help-counter-harmful-disinformation.html (Accessed: 1 March 2023).

House of Commons, Parliament of Canada (2019) *National Security Act, 2017*. Available at: https://www.parl.ca/Content/Bills/421/Government/C-59/C-59_4/C-59_4.PDF#page=71 (Accessed: 21 June 2024).

House of Commons, Parliament of Canada (2023) *Up to the Task: Strengthening Canada's security posture in relation to Russia*, Report of the Standing Committee on Public Safety and National Security, March. Available at: https://www.ourcommons.ca/Content/Committee/441/SECU/Reports/RP12018647/securp07/securp07-e.pdf (Accessed: 21 June 2024).

Howell, A. and Richter-Montpetit, M. (2020). 'Is securitization theory racist? Civilizationism, methodological whiteness, and antiblack thought in the Copenhagen School', *Security Dialogue*, 51(1), pp. 3–22. doi: 10.1177/0967010619862921.

Ionita, C-C. (2023) 'Conventional and Hybrid Actions in the Russia's Invasion of Ukraine.' *Security and Defence Quarterly*, 44(4), pp. 5–20. doi: 10.35467/sdq/168870.

Ireton, C. and Posetti, J. (2018) *Journalism, fake news and disinformation*. UNESCO Series on Journalism Education, 15. Paris: UNESCO.

Izabella, M. (2024) *Plotting the Battlefield: Russia's Use of Language and Memory to Legitimize Aggression Against Ukraine. Undergraduate Honors Theses.* William & Mary. Paper 2107. Available at: https://scholarworks.wm.edu/honorstheses/2107 (Accessed: 21 June 2024).

Jackson, N. (2018) 'Canada, NATO, and global Russia', *International Journal*, *73*(2), pp. 317–325.

Jackson, N. (2022) 'The Canadian government's response to foreign disinformation: Rhetoric, stated policy intentions, and practices', *International Journal,* 76(2), pp. 544–563. doi: 10.1177/00207020221076402.

Jackson, N. (2024) 'Deterrence and disinformation: Communicating deterrence in a non-linear media environment', *Defence Strategic Communications*, 13, pp. 95–130. Riga: NATO Strategic Communications Centre of Excellence. doi: 10.30966/2018.RIGA.13.6.

Jackson, N. (In press) 'Canada's response to foreign disinformation in the context of the Russia-Ukraine war: Collective efforts and performance' in Bajaj, S.G. and Momani, B. (eds.) *Misinformation, disinformation and democracy in the digital Age: A Canadian perspective.* Toronto: University of Toronto Press.

Jacush, A. (2022) 'The blurred lines of peace and war – An analysis of information operations use by the Russian Federation in CEE', *Journal of Slavic Military Studies*, 35(2), pp. 157–180. doi: 10.1080/13518046.2022.2139071.

Jade, M. (2024) 'Russian Propaganda Tactics in Ukraine's Newly Occupied Territories.' *Russian Analytical Digest,* 21(313), pp. 1–16. doi: 10.3929/ethz-b-000673162.

Johnson, R. (2018) 'Hybrid war, and its countermeasures: A critique of the literature', *Small Wars and Insurgencies*, 29(1), pp. 141–168. doi: 10.1080/09592318.2018.1404770.

Juneau, T. and Carvin, S. (2024) *Opinion: Canada's intelligence providers and policymakers don't understand each other*, The Globe and Mail, 30 May. Available at: https://www.theglobeandmail.com/opinion/article-canadas-intelligence-providers-and-policymakers-dont-understand-each/ (Accessed: 21 June 2024).

Krainikova, T. and Prokopenko, S. (2023) 'Waves of disinformation in the hybrid Russian-Ukrainian War.' *Current Issues of Mass Communication*, 33, pp. 12–25. doi: 10.17721/cimc.2023.33.12-25.

Kinnvall, C. (2018) 'Ontological insecurities and postcolonial imaginaries: The emotional appeal of populism', *Humanity & Society*, 42(4), pp. 523–543. doi: 10.1177/0160597618802646.

Laidlaw, Emily B. (2022) *Commissioned paper: Mis- dis- and mal-information and the convoy: an examination of the role and responsibilities of social media*', Public Order Emergency Commission, September. Available at: https://publicorderemergencycommission.ca/files/documents/Policy-Papers/Mis-Dis-and-Mal-Information-and-the-Convoy-Laidlaw.pdf (Accessed: 21 June 2024).

Lawrence, M., Janzwood, S. and Homer-Dixon, T. (2022) *What is a global polycrisis and how is it different from a global risk?* Discussion Paper 2022-24I. Victoria, BC: The Cascade Institute. Available at: https://cascadeinstitute.org/technical-paper/what-is-a-global-polycrisis/ (Accessed: 21 June 2024).

Lesher, M., Pawelec, H. and Desai, A. (2022) *Disentangling untruths online*: *Creators, spreaders and how to stop them*. OECD Going Digital Toolkit Notes, No. 23. Paris: OECD Publishing. doi: 10.1787/84b62df1-en.

Markiewicz, T. (2023) 'The vulnerability of securitisation: The missing link of critical security studies', *Contemporary Politics*, 30(2), pp. 199–220. doi: 10.1080/13569775.2023.2267371.

McMahon, D. (2023) *Maligned influence and interference in Canada*. Calgary, Alberta: Canadian Global Affairs Institute, July. Available at: https://www.cgai.ca/maligned_influence_and_interference_in_canada (Accessed: 21 June 2024).

McQuinn, B., Kolga, M., Buntain, C. and Courchesne, L. (2023) *Enemy of my enemy: Russian weaponization of Canada's far right and far left to undermine support to Ukraine*, Conflict Report Series. Regina Saskatchewan: Centre for Artificial Intelligence, Data, and Conflict (CAIDAC). March. Available at: https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf?index=true (Accessed: 2 April 2023).

Organization for Economic Cooperation and Development (OECD) (2022) *Disinformation and Russia's war of aggression against Ukraine*, 3 Nov. Available at: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/ (Accessed 1 February 2023).

Orr Bueno, C. (2023) 'Russia's role in the far-right truck convoy: An analysis of Russian state media activity related to the 2022 Freedom Convoy', *The Journal of Intelligence, Conflict, and Warfare*, 5(3), pp. 1–22. doi: 10.21810/jicw.v5i3.5101.

Salter, M. (2008) 'Securitization and desecuritization: A dramaturgical analysis of the Canadian air transport security authority', *Journal of International Relations and Development*, 11, pp. 321–349. https://doi.org/10.1057/jird.2008.20.

Savelyev, Y. (2023) 'Untruthful claims, real war, dire consequences: understanding the narrative of the Russian invasion of Ukraine', *Journal of Contemporary Central and Eastern Europe*, 31(2), pp. 467–480. doi: 10.1080/25739638.2023.2198831.

Tolz, V. and Hutchings, S. (2023) 'Truth with a Z: Disinformation, war in Ukraine, and Russia's contradictory discourse of imperial identity', *Post-Soviet Affairs*, 39(5), pp. 347–365. doi: 10.1080/1060586X.2023.2202581.

Trauthig, I. (2024) *Diaspora communities and computational propaganda on messaging apps*, Policy Brief No. 183, 11 January 11. Waterloo, ON: Centre for International Governance Innovation (CIGI). Available at: https://www.cigionline.org/publications/diaspora-communities-and-computational-propaganda-on-messaging-apps/ (Accessed: 21 June 2024).

Trudeau, J. (2022) *Statement by the prime minister on world press freedom day*, 3 May 3. Available at: https://pm.gc.ca/en/news/statements/2022/05/03/statement-prime-minister-world-press-freedom-day (Accessed: 2 February 2023).

Trudeau, J. (2024a) *Canada announces additional support for Ukraine*, Canadian Commercial Corporation. Available at: https://www.ccc.ca/en/announcements/canada-announces-additional-support-for-ukraine/ (Accessed: 21 June 2024).

Trudeau, J. (2024b) *Our north, strong and free: A renewed vision for Canada's defence*, 8 April. Available at: https://www.pm.gc.ca/en/news/news-releases/2024/04/08/our-north-strong-and-free-renewed-vision-canadas-defenc (Accessed: 21 June 2024).

Wæver, O. (1995) 'Securitization and desecuritization', in Lipschutz, R.D. (ed.) *On security.* New York, NY: Columbia University Press, pp. 46–87.

Waldman, S. (2023) 'Narrative as a force multiplier in the information battlefield', Maternowski, C. and Malhotra, A. (eds.), *Cutting Through the Haze: Grey Zone Operations and Contemporary Threats* (The Canadian Army Journal and NATO Association of Canada), Summer, pp. 32–34.

Wardle, C. and Derakshan, H. (2017) *Information disorder: Towards an interdisciplinary framework for research and policy making*, Council of Europe Report DGI. Available at: http://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf (Accessed: 1 February 2023).

Wark, W. (2024) *Foreign interference online: Where disinformation infringes on freedom of thought*, Policy Brief No. 3, 22 January. Waterloo, ON: Centre for International Governance Innovation (CIGI). Available at: https://www.cigionline.org/publications/foreign-interference-online-where-disinformation-infringes-on-freedom-of-thought/ (Accessed: 21 June 2024).

Wattie, C. (2020) 'Bringing a knife to a gunfight: Canadian strategic communications and information operations in Latvia, operation reassurance 2019–2020', *Canadian Military Journal* (Government of Canada, National Defence, Canadian Defence Academy). Available at: http://www.journal.forces.gc.ca/vol21/no1/page55-eng.asp (Accessed: 21 June 2024).

Williams, M.C. (2011) 'Securitization and the liberalism of fear', *Security Dialogue*, 42(4–5), pp. 453–463. doi: 10.1177/0967010611418717.

Wilner, Alex S. (2011) 'Deterring the undeterrable: Coercion, denial, and delegitimization in counterterrorism', *Journal of Strategic Studies* 34(1), pp. 3–37. doi: 10.1080/01402390.2011.541760.

Wilner, Alex S. (2014) 'Contemporary deterrence theory and counterterrorism: A bridge too far', *New York University Journal of International Law and Politics*, 47, pp. 439–462.

Zeitlin, J., Nicoli, F. and Laffan, B. (2019) 'Introduction: The European Union beyond the polycrisis? Integration and politicization in an age of shifting cleavages', *Journal of European Public Policy*, 26(7), pp. 963–976. doi: 10.1080/13501763.2019.1619803.