

# ENEMY

OF MY

# ENEMY

RUSSIAN  
WEAPONIZATION  
OF CANADA'S  
FAR RIGHT AND  
FAR LEFT TO  
UNDERMINE  
SUPPORT TO  
UKRAINE

Brian McQuinn  
Marcus Kolga  
Cody Buntain  
Laura Courchesne

MARCH  
2023

A joint report by the Centre for Artificial Intelligence, Data, and Conflict,  
University of Maryland College of Information Studies, and Digital Public Square

# CONFLICT REPORT SERIES

ENEMY  
of my  
ENEMY

MARCH 2023

RUSSIAN  
WEAPONIZATION  
OF CANADA'S  
FAR RIGHT AND  
FAR LEFT TO  
UNDERMINE  
SUPPORT TO  
UKRAINE



The Centre for Artificial Intelligence, Data, and Conflict (CAIDAC) is a research organization dedicated to studying social media's impact on conflict, political violence, and war. We analyze state and non-state actors' evolving social media strategies and their influence on domestic and international perceptions. CAIDAC draws on artificial intelligence research tools to understand how malicious actors weaponize social media and what moderation efforts could curtail dangerous or illegal activities. CAIDAC is a global network of researchers, practitioners, and humanitarians. Aided by machine learning and artificial intelligence tools, our team strives to find new research approaches through deep integration of their respective disciplines. CAIDAC's conflict report series translates academic research into policy briefs that provide analysis of emerging issues.

For further information about CAIDAC or this report, please write to the Centre for Artificial Intelligence, Data, and Conflict at the Politics and International Studies Department, University of Regina, 3737 Wascana Parkway, Regina, Saskatchewan, Canada, S4S 0A2, or visit our website at [tracesofconflict.com](https://tracesofconflict.com).

Digital Public Square (DPS) is a not-for-profit organization dedicated to serving communities in need. Its team has spent nearly a decade learning how to create meaningful engagement using good technology that prioritizes privacy, dignity, and respect. From building platforms that track political accountability to empowering new voices countering violent online narratives — and even creating new ways for neighbourhood communities to reach decisions — DPS has created tools that enable people to more safely explore complex ideas at scale.

The University of Maryland College of Information Studies (UMD iSchool) is a leading research and teaching college in the field of information science. Our faculty, staff, and students are expanding the frontiers of how people access and use information and technology in an evolving world — in government, education, business, and more. We offer five academic degree programs and lead cutting-edge research, specializing in library sciences, curation, data analytics and visualization, human-computer interaction, youth experience, computational linguistics, smart cities and connected communities, social computing, cybersecurity and privacy, diversity and inclusion, and the future of work. Located just outside of Washington, DC, our faculty, staff, and students have unmatched research, internship, and career opportunities.

Copyright © 2023 by the Centre for Artificial Intelligence, Data, and Conflict and Digital Public Square, University of Maryland College of Information Studies, and Digital Public Square

All rights reserved.

Printed in Canada.

## **Design**

Annalisa Raho | ARDesign + ARCommunication

## **Disclaimer**

The analysis and conclusions in this publication are solely those of the authors. In no case should they be considered or construed as representing an official position or policy of any individual or organization supporting the research it contains.

## **Acknowledgements**

This report relied on the support of many, including feedback from colleagues in CAIDAC's global network and at the University of Regina. Research for this report was generously supported by Dr. Max Schmeiser, Heritage Canada, Department of National Defence Research Initiative, Defense Advanced Research Projects Agency, and the University of Regina.

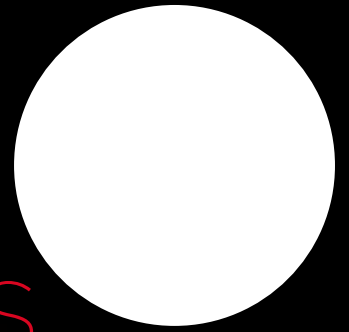
**Suggested citation:** Brian McQuinn, Marcus Kolga, Cody Buntain, and Laura Courchesne. "Enemy of My Enemy: Russian Weaponization of Canada's Far Right and Far Left to Undermine Support to Ukraine." Conflict Report Series. Centre for Artificial Intelligence, Data, and Conflict. March 2023.

# CONTENTS

Executive Summary	1
I. Background	
Russia's Ramped-up Information Operations	5
II. Methodology	
Mapping Russian Disinformation Campaigns on Social Media	7
III. Analysis	
Twitter's Russian-Aligned Ecosystem	9
IV. Recommendations to Combat Russian Disinformation in Canada	15

Close-up of gun in Donetsk, Ukraine (photo by Martin Trabalik, C

# LIST OF FIGURES



<b>Figure 1</b>	The political orientation of the core Russian-aligned accounts	10
<b>Figure 2</b>	Comparing Canadian Russian-aligned accounts, Canadian Members of Parliament, and the most prominent Twitter accounts in Canada	11
<b>Figure 3</b>	The Russian-aligned ecosystem	12
<b>Figure 4</b>	Daily tweet production by each set of accounts (January 2021 to October 2022)	13
<b>Figure 5</b>	Comparing daily Russian tweet production (January 2021 to September 2022)	14



# EXECUTIVE SUMMARY

**R**ussia invaded Ukraine with overwhelming force one year ago, ending seventy years of peace in Europe. The war has devastated the country, killed hundreds of thousands of Ukrainians and Russians, and displaced more than 15 million people.<sup>1</sup> Russia's initial invasion failed, further isolating its president, Vladimir Putin. The result is a grinding war of attrition, with Russia shifting its strategy to target civilian infrastructure,<sup>2</sup> including hospitals and electricity grids, which are violations of international humanitarian law.<sup>3</sup> Canada has deep ties to Ukraine and is home to one of the largest Ukrainian diaspora communities in the world. In response to the invasion, the Canadian government has provided over CDN 4.5 billion in humanitarian and military aid<sup>4</sup> while strongly supporting NATO,<sup>5</sup> the most potent military opposition to Putin.

International assistance is essential to Ukraine's survival. Putin recognizes this vulnerability and actively seeks to undermine support for Ukraine among Western democracies. One of his primary weapons in this fight is online influence campaigns pushed through Western-owned social media platforms such as Twitter, YouTube, and Facebook.<sup>6</sup> The Russian government and its proxies have a long history of intervening in the politics of other countries — most famously, meddling in the 2016 United States (US) elections.<sup>7</sup>

In the aftermath of that election, Canada began recognizing the threat of Russian influence operations and has slowly developed a research and policy response to address the inherent social and political threats posed by foreign interference efforts.<sup>8</sup> This report builds on previous research on Russian influence operations within and outside Canada.<sup>9</sup> We contribute to these studies by identifying a previously unexplored Russian strategy in Canada: the

---

1 “Ukraine War: US Estimates 200,000 Military Casualties on All,” BBC, 10 November 2022; Erol Yayboke, Anastasia Strouboulis, and Abigail Edwards, “Update on Forced Displacement around Ukraine,” Critical Questions, Center for Strategic and International Studies, 3 October 2022; “Ukraine: Russian Attacks on Critical Energy Infrastructure Amount to War Crimes,” Latest News, Amnesty International, 20 October 2022.

2 James Kariuki, “Russia’s Systematic Attacks on Ukrainian Civilian Infrastructure Are Unacceptable, and Must End,” Statement by Ambassador James Kariuki at the Security Council briefing on Ukraine, Government of the United Kingdom and Northern Ireland, 23 November 2022.

3 Lara Hakki, Eric Stover, and Rohina J. Haar, “Breaking the Silence: Advocacy and Accountability for Attacks on Hospitals in Armed Conflict,” *International Review of the Red Cross* 102, no. 915 (2020): 1201–26.

4 “Canada Disburses \$450 Million in Loans to Ukraine,” *News Release*, Department of Finance Canada, 17 August 2022; “Prime Minister Announces Additional Military assistance for Ukraine and Additional Sanctions Against Russia,” News Release, 14 November 2022, Office of the Prime Minister, Government of Canada.

5 The North Atlantic Treaty Organization (NATO) is a defence pact established after World War II between the United States, Canada, and Europe. For further details see <<https://www.nato.int>>.

6 W. Lance Bennett and Steven Livingston, “The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions,” *European Journal of Communication* 33, no. 2 (2018): 122–39.

7 Paul Mozur, Adam Satariano, and Aaron Krolik, “An Alternate Reality: How Russia’s State TV Spins the Ukraine War,” *The New York Times*, 15 December 2022; for earlier examples, see Thomas Boghardt, “Soviet Bloc Intelligence and Its AIDS Disinformation Campaign,” *Studies in Intelligence* 53, no. 4 (2009): 1–24.

8 Nicole J. Jackson, “The Canadian Government’s Response to Foreign Disinformation: Rhetoric, Stated Policy Intentions, and Practices,” *International Journal* 76, no. 4 (2022): 544–63; Jean-Christophe Boucher, Jack Edwards, Jenny Kim, Abbas Badami, and Henry Smith, “Disinformation and Russian-Ukrainian War on Canadian Social Media,” University of Calgary School of Public Policy briefing paper, Vol. 15:16, June 2022.

9 Ahmed Al-Rawi, “How Did Russian and Iranian Trolls’ Disinformation Toward Canadian Issues Diverge and Converge?” *Digital War* 2 (2021): 21–34; Barry Cartwright, Richard Frank, George Weir, and Karmvir Padda, “Detecting and Responding to Hostile Disinformation Activities On Social Media Using Machine Learning and Deep Neural Networks,” *Neural Computing and Applications* 34, no. 18 (2022): 15141–63; Aengus Bridgman, Mathieu Lavigne, Melissa Baker, Thomas Bergeron, Danielle Bohonos, Anthony



Ukrainian Motherland Monument

weaponization of both Canada’s far-right and far-left movements to undermine international support for Ukraine.

Far-right and far-left communities in Canada are increasingly polarized.<sup>10</sup> Their rhetoric has shifted from differences over policy to framing opponents as enemies who pose an existential threat to Canada. The Russian government continually monitors Western societies for divisive issues to exploit. Once such issues are identified, Russian mouthpieces and proxies inject and amplify these narratives in our information environment to intensify political divisions.<sup>11</sup> The war in Ukraine is no exception. Wittingly or not, these apparent enemies on the political far left and far right have found common ground: undermining public support for Canadian financial, humanitarian, and military aid to Ukraine. While far-right communities have increasingly aligned with Vladimir Putin’s anti-globalist, xenophobic, and nationalist rhetoric, the far left has historically aligned with Moscow’s anti-Western and anti-NATO propaganda since the earliest days of the Cold War.<sup>12</sup> These communities are among Canada’s most active online political communities.<sup>13</sup> Together, they represent a potent strategy for the Russian government to intensify its attack against Canadian support for Ukraine.

This report presents research by the Centre for Artificial Intelligence, Data, and Conflict (CAIDAC) and Digital Public Square (DPS) detailing Russian efforts to influence Canadians’ perceptions of the war in Ukraine over the last two years. Specifically, we examined Russian information campaigns tailored to Canadian audiences on Twitter and the supportive ecosystems of accounts that amplify them. We defined “supportive ecosystem” to include any account on Twitter that either retweeted Russian narratives or posted content subsequently shared by leading pro-Russian accounts. By 2023, this ecosystem included at least 200,000 Twitter accounts that have shared content with millions of Canadians since the war began.<sup>14</sup>

---

Burton, Katharine McCoy, et al. “Mis- and Disinformation in the 2021 Canadian Federal Election,” Canadian election misinformation project, OSF Preprints, 2022; Boucher et al. “Disinformation and Russian-Ukrainian War on Canadian Social Media”; Philip Mai, Alyssa N. Saiphoo, Anatoliy Gruzd, and Felipe Bonow Soares, “Russian Propaganda Is Making Inroads with Right-wing Canadians,” *The Conversation*, 17 July 2022; “Disinformation Roulette: The Kremlin’s Year of Lies to Justify an Unjustifiable War,” Global Engagement Center report, United States Department of State, 23 February 2023.

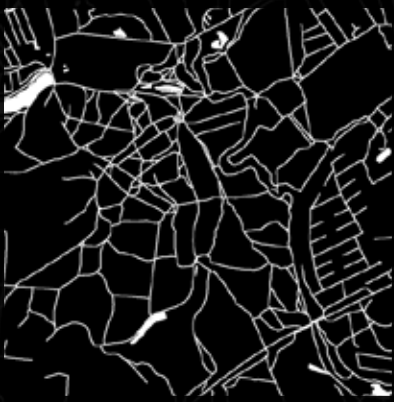
10 Anatoliy Gruzd and Jeffrey Roy, “Investigating Political Polarization on Twitter: A Canadian Perspective,” *Policy and Internet* 6, no. 1 (2014): 28–45; Samuel Tanner and Aurélie Campana, “‘Watchful Citizens’ and Digital Vigilantism: A Case Study of the Far Right in Quebec,” *Global Crime* 21, nos. 3–4 (2020): 262–82.

11 Marcus Kolga, “Confusion, Destabilization and Chaos: Russia’s Hybrid Warfare Against Canada and Its Allies,” Canadian Global Affairs Institute, October 2021.

12 Barbara Perry and Ryan Scrivens, *Right-wing Extremism in Canada* (Cham, Switzerland: Springer, 2019); Steve Hewitt, “Cold War Counter-terrorism: The Evolution of International Counter-terrorism in the RCMP Security Service, 1972–1984,” *Intelligence and National Security* 33, no. 1 (2018): 67–83.

13 “CSIS Public Report 2019,” Canadian Security Intelligence Service, 2020, Government of Canada

14 This is a conservative estimate. The size of the ecosystem was calculated using various methods such as mapping all



Our analysis found that Russian influence operations integrated sophisticated narratives with incendiary images and videos tailored to Canadian audiences. These narratives rapidly evolved, responding to emerging news events in Ukraine, Canada, and Russia. The responsive nature of the campaign indicates a nuanced and well-funded Russian effort. We reviewed the narratives promoted by this ecosystem regardless of whether they had any basis in fact. Russian influence narratives blended fabrications, conspiracies, and half-truths to amplify their messages.<sup>15</sup> We opted to study all narratives pushed by these accounts to identify Russia's underlying strategy and how they were amplified in the broader ecosystem.<sup>16</sup> Understanding the supporting role of unsuspecting Canadians allows us to design better interventions to

limit the impact of Russian influence operations.

Our analysis confirms findings from earlier studies on Russian influence operations in Canada and the United States.<sup>17</sup> The results provide evidence for the following conclusions about Russian efforts to undermine Canadian support for Ukraine:

***1) Russian influence operations weaponized Canada's far-right and far-left communities.***

The vast majority of the influential Canadian accounts amplifying Russian influence campaigns are far right or far left in orientation.<sup>18</sup> This provides compelling evidence that, knowingly or not, these accounts enable Russian efforts to undermine Canadian support for Ukraine. The rate, breadth, and volume of the narratives produced by the Russian campaign suggest a highly organized and well-funded effort by the Russian government and its proxies.<sup>19</sup>

***2) Far-right and far-left networks are among the most active online political communities.***

Russian disinformation targeting Canadians received engagement from over 200,000 accounts on Twitter.<sup>20</sup> These networks were among Canada's most prolific and influential political communities online. To assess these networks' potential influence, we compared them to the online community engaging with Canada's 338 Members of Parliament (MPs) on Twitter and a sample of twenty influential Twitter accounts in Canada. Compared to the political community engaging with MPs, these Russian-aligned networks produced twenty-seven times more content and three times as much engagement. Even when compared to Canada's twenty most influential accounts on Twitter, these accounts produced significantly more content but were followed by fewer accounts.

***3) Average Canadians amplify Russian influence operations.***

We identify Canada's Russian-aligned ecosystem's core group of ninety accounts with an outsized influence, which is in keeping with other online social networks.<sup>21</sup> Meanwhile, the proportion of "average Canadians" in

---

that retweeted the most influential accounts at different points in time.

15 Adam B. Ellick and Adam Westbrook, "Operation Infektion: Russian Disinformation from the Cold War to Kanye," *New York Times*, 12 November 2018.

16 "Disinformation and Russia's War of Aggression Against Ukraine: Threats and Governance Responses," Policy Responses, Organisation for Economic Co-operation and Development, 3 November 2022.

17 Al-Rawi, "How Did Russian and Iranian Trolls' Disinformation toward Canadian Issues Diverge and Converge?"; Cartwright, Frank, Weir, and Padda, "Detecting and Responding to Hostile Disinformation Activities"; Bridgman, et al. "Mis- and Disinformation in the 2021 Canadian Federal Election"; Boucher et al., "Disinformation and Russian-Ukrainian War on Canadian Social Media"; Mai, Saiphoo, Gruzd, and Bonow Soares, "Russian Propaganda Is Making Inroads."

18 We evaluated each of the core accounts and determined their political alignment. For further details of this process, see the methodology section.

19 Mozur, Satariano, and Krolik, "An Alternate Reality: How Russia's State TV Spins the Ukraine War."

20 This is a conservative estimate. The size of the ecosystem was determined using multiple approaches such as mapping the accounts retweeting the most influential accounts in the ecosystem at different points in time.

21 David Lazer, Matthew Baum, Yochai Benkler, Adam Berinsky, et al., "The Science of Fake News," *Science* 359, no. 6380 (2018):1094–96.





the broader ecosystem makes up 83.3 percent of the network, presenting policy-makers with challenges and opportunities.<sup>22</sup> Innovative media educational efforts, like online trivia pages such as [ukrainetrivia.com](http://ukrainetrivia.com), have successfully improved users' knowledge of Ukraine and the conflict. These efforts would be further improved by increased collaboration with cognitive scientists who study disinformation.

We document how a small network of ninety active Russian-aligned accounts can co-opt and engage massive online communities. Without the help of these tacit supporters, who are often supporting unknowingly, these narratives would not find traction in Canada. The support of average Canadians makes these pro-Russian information campaigns possible. Even more worryingly, this amplification by average Canadians is crucial to expanding the size of the network taking part in the Russian-aligned ecosystem. Effective monitoring of the Russian-aligned ecosystem will require government and social media companies to support and engage with civil society, which is often better at identifying how foreign actors circumvent existing laws and policies.

#### ***4) Russia's disinformation is tailored to capture Canadian audiences.***

Previous research has shown how the Russian government's disinformation and propaganda ecosystem identifies audiences in a country and builds narratives that resonate within them. We found similar tactics used in Canada with messages and narratives tailored to far-right and far-left communities. Examples of those narratives include the following:

- "Canada's foreign policy is controlled by Ukrainian Canadians."
- "Canadian sanctions are responsible for inflation and rising energy costs."
- "Canadian sanctions are responsible for growing global food shortages."
- "If Canadians want to cooperate with Russia on climate and Arctic issues, then we must return to diplomacy."
- "Ukraine is corrupt and doesn't deserve our support."
- "Russia is de-Nazifying Ukraine."
- "NATO is responsible for the war."
- "Western support for Ukraine should stop because it will cause nuclear Armageddon."

#### ***5) Pro-Russian accounts ramped up influence operations in Canada three months before the invasion.***

We have strong evidence that Russian information operations in Canada ramped up their production of disinformation three months before the invasion of Ukraine. This included a fourfold increase of pro-Russian government narratives attacking support for Ukraine and Canadian democratic institutions. There is also evidence that there has been a steady increase in the volume of tweets of Russian government narratives.

This report has four main sections. The first provides a brief background on the Russian invasion one year ago and previous research on Russian influence operations in Canada. The second section provides additional background on the methodologies used to generate our analysis. The third section provides supporting analysis and evidence for our six conclusions. The final section outlines five recommendations for the Canadian government and social media companies to respond to the report's findings.

---

<sup>22</sup> In this report, we define "average Canadians" as any Twitter account with a below-average follower count compared to the other Canadians in the data set, which was a median of 1,318 as of October 2022.

## Section 1

# BACKGROUND

## Russia's Ramped-up Information Operations

Over the past fifteen years, the Russian government intensified its online influence operations globally, targeting democratic nations and countries that were formerly part of the Soviet Union.<sup>23</sup> In 2007, Russia tested its new information and cyber capabilities by targeting Estonia, where it amplified ethnic tension and disrupted the country's digital infrastructure with denial-of-service (DoS) attacks.<sup>24</sup> Since then, the Russian government and its proxies have meddled in over a dozen elections worldwide with information and influence operations, including the 2016 US presidential election.<sup>25</sup> During the COVID-19 pandemic, Russian information operations amplified and promoted vaccine hesitancy and anti-lockdown narratives in Canada as part of Russia's worldwide efforts to exploit the pandemic and intensify its effects in the democratic world.<sup>26</sup>

There is growing evidence that Russia ramped up its information operations as it ordered military buildup along its western border with Ukraine and Belarus in the latter half of 2021. Russian spokespersons and information operations denied any intention to invade Ukraine in the months before 24 February 2022. Once the invasion began, however, these same spokespersons justified Russia's "special military operation" as an effort to "de-Nazify" Ukraine. For months before the invasion, online influence operations prepared the ground for this shift, advancing disinformation campaigns on the neo-Nazi policies and roots of Ukraine's government.<sup>27</sup>

Western democracies have responded to Russia's invasion of Ukraine by imposing significant sanctions on Russia's ability to import Western goods, including dual-use technologies that could be used to build or repair weapons. The foreign assets of many Russian businesses, oligarchs, and kleptocrats have been frozen, and in Canada, they face the threat of being seized and forfeited.

Western governments have continued to donate billions of dollars of technologically advanced precision weapons to Ukraine. The delivery of these weapon systems and nonlethal aid has significantly contributed to Ukraine's military capacity and the failure of Putin's military objectives.<sup>28</sup> Public backing for Ukraine in Western countries is important for sustaining that aid, which is one reason that Russian disinformation narratives have shifted to blaming Canadian and allied sanctions for global inflation and the rising cost of energy.<sup>29</sup> The emerging global

23 For additional information on influence operations, see Meysam Alizadeh, Jacob N. Shapiro, Cody Buntain, and Joshua A. Tucker, "Content-based Features Predict Social Media Influence Operations," *Science Advances* 6, no. 30 (20 July 2020).

24 Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, 29 May 2007.

25 Gregory Eady, Tom Paskhalis, Jan Zilinsky, Richard Bonneau, Jonathan Nagler, and Joshua A. Tucker, "Exposure to the Russian Internet Research Agency Foreign Influence Campaign on Twitter in the 2016 US Election and Its Relationship to Attitudes and Voting Behavior," *Nature Communications* 14, no. 62 (2023): 1–11.

26 Robin Emmott, "Russia Deploying Coronavirus Disinformation to Sow Panic in West, EU Document Says," *Reuters*, 18 March 2020; "Russian Embassy in Canada Promotes Vaccine Disinformation," *Disinfowatch*, 18 January 2021.

27 "Disinformation and Russia's War of Aggression Against Ukraine."

28 Andrew E. Kramer, "With Western Weapons, Ukraine Is Turning the Tables in an Artillery War," *The New York Times*, 1 November 2022.

29 See, for example, "Disinfo: Western Sanctions Are the Cause of Inflation" on the EUvsDisInfo website <<https://euvsdisinfo.eu/report/western-sanctions-are-the-cause-of-inflation>>.



A member of the Ukrainian special forces in silhouette while a gas station burns after Russian attacks in the city of Kharkiv on 30 March 2022 (photo by Fadel Senna/AFP via Getty Images)

food crisis, caused by Russian destruction and appropriation of Ukrainian agricultural infrastructure and the blockade of Ukrainian ports, is also blamed on Canadian and Western sanctions.<sup>30</sup>

In June 2022, a team of researchers at the School of Public Policy at the University of Calgary identified narratives that Russia has used to influence Western communities.<sup>31</sup> Many of these narratives remain central to Russian influence operations. They include: (1) blaming NATO's expansion for sparking the war — that is, that Canada and the West have no moral superiority to condemn Russia's invasion of Ukraine because of the war in Afghanistan; (2) how Canada and other Western nations have forced Europe into the conflict to benefit from it; and (3) how the West is supporting fascists in Ukraine. There are also narratives of eroding trust in Canada's democratic institutions.

Similarly, a poll of 2,048 Canadians conducted by Digital Public Square and Nanos Research found that most of those polled could correctly identify official Russian government narratives about the war in Ukraine. However, at least 25 percent were unsure or unable to identify Russian disinformation narratives — suggesting that some Canadians remain vulnerable to foreign information warfare. For example, 36 percent of respondents either believed that NATO was responsible for the war in Ukraine or were unsure. A majority of those polled are concerned that Russia represents a threat to Western democracy.

<sup>30</sup> See, for example, “Disinfo: Western Sanctions Are the Cause of Inflation.”

<sup>31</sup> Boucher et al., “Disinformation and Russian-Ukrainian War on Canadian Social Media.”



# Section 2

# METHODOLOGY

## Mapping Russian Disinformation Campaigns on Social Media

---

The data we used to research the online behaviours presented here were acquired through Twitter’s academic research application programming interface (API) and a three-year qualitative study of Russian disinformation campaigns on social media. The quantitative analysis employs a network-based methodology developed by CAIDAC in previous studies.<sup>32</sup> This method relies on conflict experts to identify prominent accounts in a network and then uses those accounts to map the broader ecosystem engaging with those accounts.<sup>33</sup> The method differs from other Canadian studies that relied on data sets identified by others or used keyword phrases or hashtags to identify content related to Russian disinformation.<sup>34</sup>

We rely on this approach to mapping actor networks for three reasons. First, large-scale information operations (like those we studied here) rely on co-opting online communities of “average users” to be effective.<sup>35</sup> We do not try to disentangle which parts of the ecosystems are organic online communities and which are the orchestrated campaign, choosing instead to study the ecosystem as a whole. Studying this broader ecosystem allows us to examine both the strategies of pro-Russian accounts and, crucially, how their narratives resonate within specific social media communities.

Second, state actors and their direct proxies, like Russia’s Internet Research Agency, are crucial to driving information operations.<sup>36</sup> But there is growing evidence that other actors are also indispensable to foreign information operations. For instance, “information activists” devote substantial personal resources to a cause for individual financial or social gain.<sup>37</sup> While studies focused exclusively on one actor, or even one type of actor, are valuable for understanding their strategy, such approaches potentially miss other actors equally crucial to influencing public sentiment.

Finally, large-scale online ecosystems are dynamic systems that evolve and adapt over time. These systems’ emergent behaviours are distinct from any coordinated manipulation. As our methods become more sophisticated, we hope to disentangle coordinated campaigns from the organic behaviour of online communities that inadvertently or intentionally help support interference by political actors.

For this case, part of our team, led by Marcus Kolga, conducted a three-year study examining Russian disinformation campaigns across several Western democracies, including Canada, the US, and the European Union.<sup>38</sup> The

---

32 Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, “Powered by Twitter? The Taliban’s Takeover of Afghanistan.” Centre for Artificial Intelligence, Data, and Conflict, 2022.

33 Samuel Stehle, “Mapping Mediascapes: Exploring the Semantic and Geographic Spaces of Catalonia’s 2015 Independence Movement Through Digital News,” *The Professional Geographer* 73, no. 1 (2021): 150–59.

34 Darren L. Linvill and Patrick L. Warren, “Troll Factories: The Internet Research Agency and State-Sponsored Agenda-Building,” Resource Centre on Media Freedom in Europe, June 2018; Boucher et al., “Disinformation and Russian-Ukrainian War on Canadian Social Media.”

35 Kate Starbird, Ahmer Arif, and Tom Wilson, “Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations,” *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (2019): 1–26.

36 Andrew Dawson and Martin Innes, “How Russia’s Internet Research Agency Built Its Disinformation Campaign,” *The Political Quarterly* 90, no. 2 (2019): 245–56.

37 Starbird, Arif, and Wilson, “Disinformation as Collaborative Work.”

38 For further information, see the “About” Disinfo Watch section <<https://disinfowatch.org/about/>>.

research monitored overt Russian government actors such as Russian Television (RT), Sputnik News, and Kremlin spokespersons through open-source intelligence methods (OSINT). Researchers then analyzed how specific stories were picked up, shared, and amplified in various pro-Russian ecosystems across different countries. Initially, the team selected forty-eight prominent Twitter accounts promoting and amplifying Russian government-aligned narratives with Canada-related narratives. These accounts were then used to map their supportive ecosystem: those accounts that either liked, reposted, or had material posted by the prominent Twitter accounts. Tweets from these accounts were collected from 24 February 2021 to 31 January 2023. This period allowed the team to analyze the ecosystem for a year before the invasion.

To measure the potential influence of the accounts central to the pro-Russian ecosystem, we compared them to two other sets of accounts: (a) the online community that engages with Canada's 338 Members of Parliament on Twitter and (b) a list of Canada's most influential Twitter users. These account lists were compiled through published lists. These baselines helped assess how influential and prolific the pro-Russian accounts were by comparing their account follower count, tweet production, and accounts they followed.



Kyiv, Ukraine, vector map

## Section 3

# ANALYSIS

## Twitter's Russian-Aligned Ecosystem

The analysis is based on a six-month study of the supportive ecosystem of over 200,000 accounts amplifying pro-Russian narratives in Canada.<sup>39</sup> This broader ecosystem was mapped through network analysis of Twitter accounts interacting with the seed accounts, for instance, by retweeting posts. We studied the broader system because recent research has shown that foreign influence operations are collaborative undertakings that require a support network to spread and amplify messages.<sup>40</sup> Understanding the role that unsuspecting Canadians play in this support network is crucial to designing better interventions to limit the impact of foreign influence. The analysis provides compelling evidence for the following conclusions:

### ***1) Russian influence operations are weaponizing Canada's far right and the far left.***

The analysis mapped the supportive ecosystem that amplifies narratives pushed by the Russian government and its proxies on Twitter. As we described earlier, this ecosystem included at least 200,000 accounts that retweeted or liked these narratives. Network mapping software then identified the ninety most influential accounts in the ecosystem. Our analysts were familiar with most accounts, having tracked Russian influence operations in Canada for the last three years. The team removed thirty-three accounts for which the user's location could not be determined. Of the remaining accounts, the largest group of users were based in Canada (47%), with the US (23%), Russia (19%), UK (7%), Austria (2%), and Australia (2%) making up the remainder.

The team then reviewed the accounts based in Canada and found that the overwhelming majority (92.6%) belonged to either far-right or far-left voices. In total, nine accounts were characterized as far-left (33.3%) while sixteen accounts were categorized as far-right (59.3%). See Figure 1.<sup>41</sup> The remaining accounts (7.4%) could not be classified along the traditional right and left political spectrum as they often exposed views from both extremes of the political spectrum. These accounts may signal the emergence of new political orientations.

The centrality of these accounts to the Russian influence operations in Canada provides compelling evidence that far-right and far-left communities have been co-opted to undermine Canadian support for Ukraine. These results mirror the findings of a 2016 study in the US that mapped the online communities for and against Black Lives Matter protests in 2016.<sup>42</sup> In that case, Russian-aligned accounts amplified polarization by playing a central role in both the far-right and far-left communities online.

<sup>39</sup> This is a conservative estimate. We calculated the size of the ecosystem using various methods such as mapping all accounts that retweeted the most influential accounts at different points in time.

<sup>40</sup> Starbird, Arif, and Wilson, "Disinformation as Collaborative Work."

<sup>41</sup> Categorizing accounts as either far right or far left is a subjective assessment. However, most of the accounts in this study were well-known to our team, making the determination relatively straightforward. For the remaining accounts, our analysts looked at account networks for evidence of support for certain narratives and slogans that have been promoted or amplified by groups on the far left and far right. For further discussion of the challenge of measuring extremism, see John M. Berger, *Extremism* (Cambridge, MA: MIT Press, 2018).

<sup>42</sup> Starbird, Arif, and Wilson, "Disinformation as Collaborative Work."

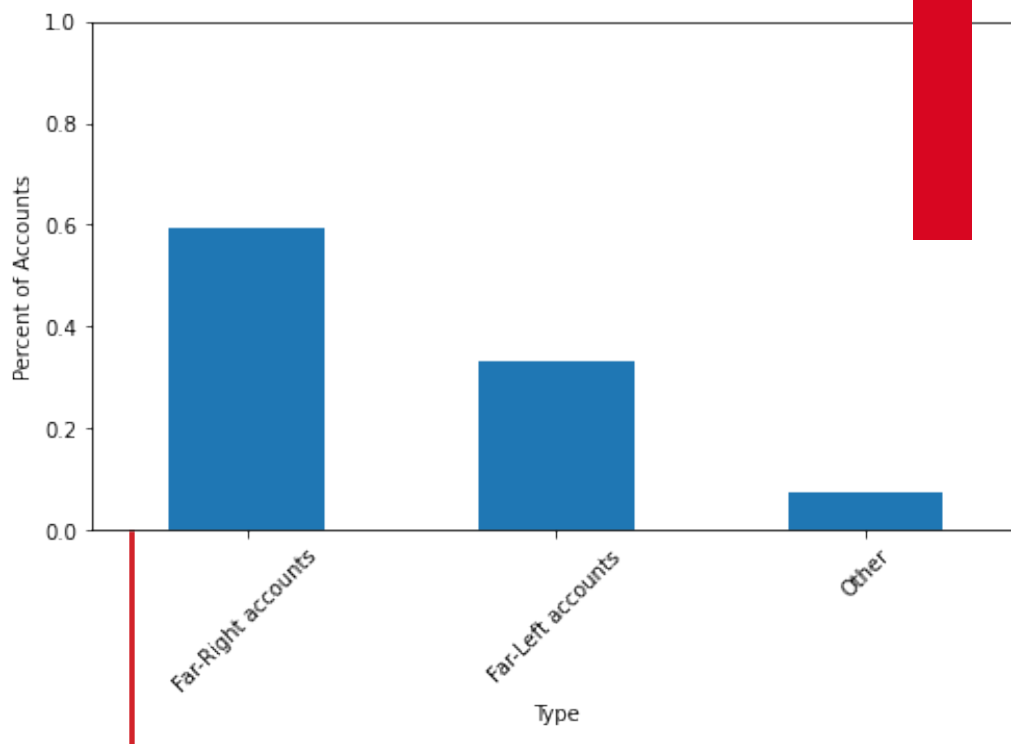


Figure 1. The political orientation of the core Russian-aligned accounts in Canada

## 2) Far right and far left networks are among the most active online political communities.

One of our primary goals in this report was to measure the relative size and reach of the networks amplifying Russian influence narratives. The research builds on previous studies that document Russian narratives that target Canadians.<sup>43</sup> To assess the networks’ potential influence, we first identified the supportive ecosystem engaging with these information campaigns.

To be successful, foreign influence operations on social media require the cooperation of thousands or, in some cases, millions of social media users. This network leveraging highlights the distinction between disinformation and misinformation.<sup>44</sup> The organizations disseminating content do so with malicious intent (disinformation), but most users who engage with those narratives are unaware of the creators’ intention — in other words, their unwitting engagement involves misinformation. However, their participation is essential for the amplification of influence operations. It is for this reason that those creating influence campaigns select narratives that closely align with a community’s current views or ideology to maximize that community’s uptake. This selection process is one reason we chose to study the broader supportive ecosystem (e.g., 200,000 accounts) to observe how these narratives resonated within the larger ecosystems.

Although the ecosystem had at least 200,000 accounts on Twitter, two distinct networks emerged. Only when we reviewed accounts central to these two ecosystems did we realize that the two networks corresponded to far-right or far-left communities in Canada. We identified the central accounts by calculating a centrality metric across all accounts engaging with an initial set of expert-identified relevant accounts. This centrality metric, PageRank, is often used to identify influential web pages on the Internet.<sup>45</sup> It has been used to study social networks, especially around conspiracy theories.<sup>46</sup> This centrality metric drops off quickly after the core ninety accounts. As we

43 Boucher et al., “Disinformation and Russian-Ukrainian War on Canadian Social Media.”

44 Hunt Allcott and Matthew Gentzkow, “Social Media and Fake News in the 2016 Election,” *Journal of Economic Perspectives* 31, no. 2 (2017): 211–36.

45 Yu Zhang, Zhaoqing Wang, and Chaolun Xia, “Identifying Key Users for Targeted Marketing by Mining Online Social Network,” *2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*, Perth, WA, Australia, 2010, 644–49, <doi:10.1109/waina.2010.137>.

46 Daniela Mahl, Jing Zeng, and Mike S. Schäfer, “From ‘Nasa Lies’ to ‘Reptilian Eyes’: Mapping Communication About Ten Conspiracy Theories, Their Communities, and Main Propagators on Twitter,” *Social Media and Society* 7, no. 2 (2021): <<https://doi.org/10.1177/20563051211017482>>.

reviewed the ecosystem's core accounts, our analysts determined that the users in Canada were among Canada's most prominent far-right and far-left voices.

To contextualize the potential influence of the pro-Russian ecosystem, the team identified two comparable sets of accounts. The first network mapped the Twitter ecosystem for Canada's 338 Members of Parliament who have Twitter accounts. This network served as a comparison of a politically oriented online community in Canada. For the second network, the team identified the most influential Twitter accounts in Canada to serve as a benchmark against the pro-Russian networks we'd identified. The data set was created by collecting Twitter data geolocated to Canada, as identified by Twitter's geolocation metadata and applying the same PageRank-based approach to identify the most influential accounts. These included accounts such as the CBC and Justin Trudeau. The three sets of accounts were then compared by examining, among other comparisons, the number of tweets they produced, the number of times they were retweeted, the number of accounts that followed each, and the number of accounts they followed.

In comparison to the 338 Members of Parliament, the Canadian Russian-aligned accounts had comparable followers, followed three times more accounts, produced twenty-seven times more tweets, and had three times more engagement (see Figure 2). However, this analysis does not account for the ultimate influence of those ideas on Canadians' views of Ukraine. Still, as a network, it is among Canada's most active political communities. Measuring the Russian-aligned accounts compared to the most influential accounts in Canada of any kind, they produced four and a half times more content (450%), followed almost twice as many accounts, but only had a quarter (27%) of the followers. The analysis showed that the Russian-aligned posts were engaged with more often when accounting for the size of their audience.

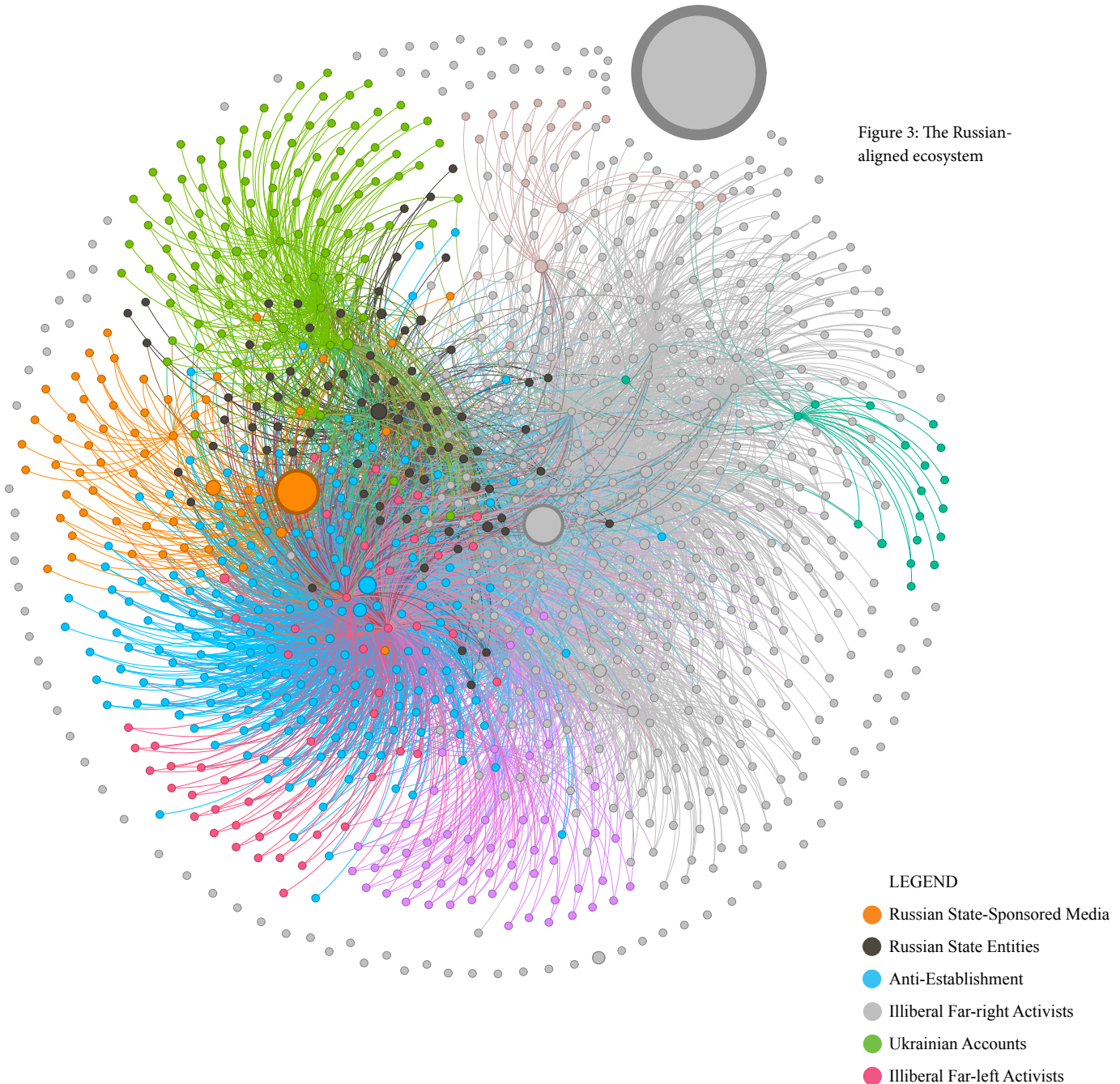
Figure 2. Comparing Canadian Russian-aligned accounts, Canadian MPs, and the most prominent Twitter accounts in Canada





### 3) Average Canadians enabled Russian influence operations.

The most active accounts — those driving much of the traffic — are a tiny percentage of the ecosystem (far less than 1 percent). Within the supportive ecosystem of 200,000 Twitter accounts, 83.4 percent of the audience have fewer than the average number of followers — fewer than 1,318 followers. By contrast, the 17 percent with more than that have approximately 6,477 followers on average, with a maximum of 800,175. One insight from this report, which is supported by other research, is how a small network of active pro-Putin accounts can co-opt and engage passive followers.<sup>47</sup> Without this tacit and usually unknowing support, such pro-Putin narratives would not be amplified in Canadian online spaces communities to the extent they are.



47 Starbird, Arif, and Wilson, “Disinformation as Collaborative Work.”

#### 4. Russian disinformation campaigns use content tailored to Canada.

Our findings confirmed previous research that Russian influence operations use Canadian-tailored content.<sup>48</sup> The most obvious examples include influence campaigns targeting specific Canadians. For example, one of the most consistent targets was Canadian Deputy Prime Minister Chrystia Freeland. The focus on Ms. Freeland is likely a result of her prominent role in the government, previous public support for Ukraine, and family ties to Ukraine. But it is also likely that Ms. Freeland is a target because of her potential candidacy as NATO's next Secretary-General.<sup>49</sup> Other examples include disinformation campaigns related to former Canadian General Trevor Kadier and other Canadians fighting in Ukraine. Beyond targeting specific individuals, many narratives blamed Canadian policies toward Ukraine for various global ills, including inflation, global food shortages, or the Russian motivations for initiating the war. Studying content with Canadian-related material helped distinguish the supportive ecosystem in Canada from accounts in the US. However, it was clear from the network mapping and qualitative assessment that significant sharing occurs between the US and Canadian ecosystems.

Our research confirmed other studies' findings that new influence narratives targeting Canada emerge every week.<sup>50</sup> These influence campaigns often produce variations of existing targets or themes but they also respond quickly to political and military events in Canada, Europe, Russia, and Ukraine. The sophistication and proliferation of these Canada-tailored narratives suggest a highly organized and well-funded effort to target Canadian support for Ukraine.

48 Boucher et al., "Disinformation and Russian-Ukrainian War on Canadian Social Media."

49 Murray Brewster and Alexander Panetta, "Chrystia Freeland Has a 'Legitimate Shot' at Top NATO Job, Expert Says," CBC, 9 September 2022; Steven Erlanger, "Who Will Be NATO's Next Chief? The Race Is On," *The New York Times*, 4 November 2022.

50 For example, see Madeline Roache, Sophia Tewa, Alex Cadier, et al., "Russia-Ukraine Disinformation Tracking Center: 358 Websites Spreading War Disinformation And the Top Myths They Publish," NewsGuard, 21 February 2023, <<https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center>> or the EUvsDisinfo site at <<https://euvsdisinfo.eu/>>.

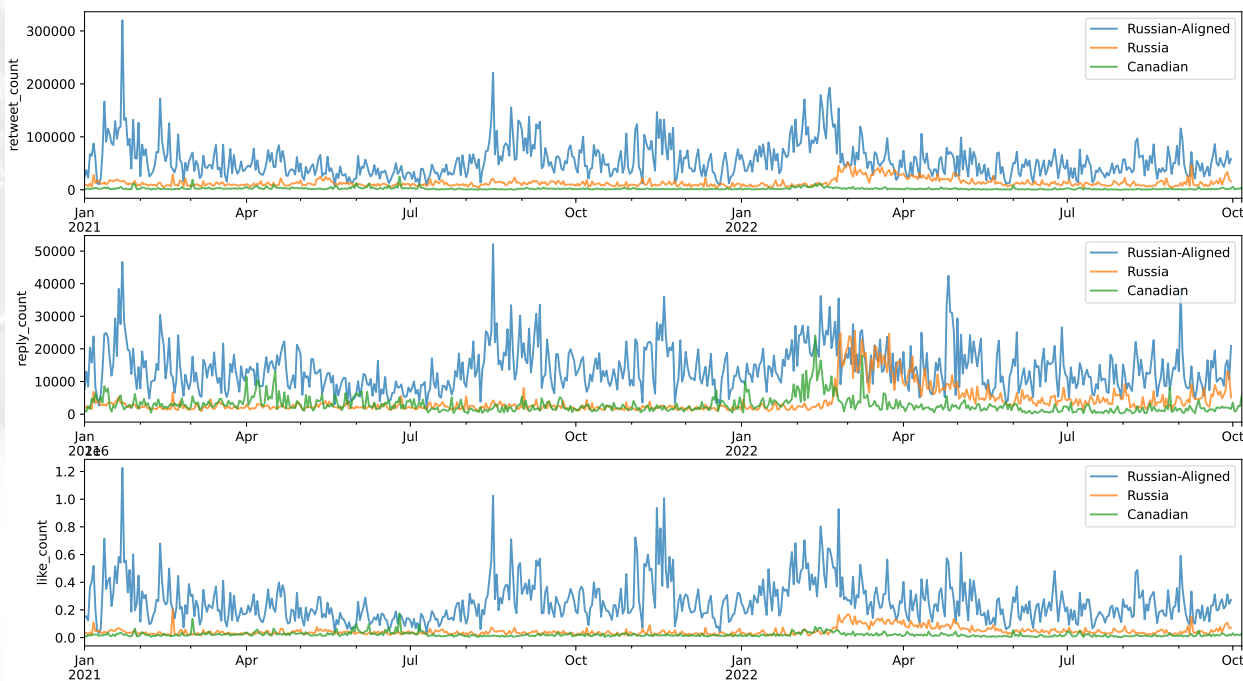


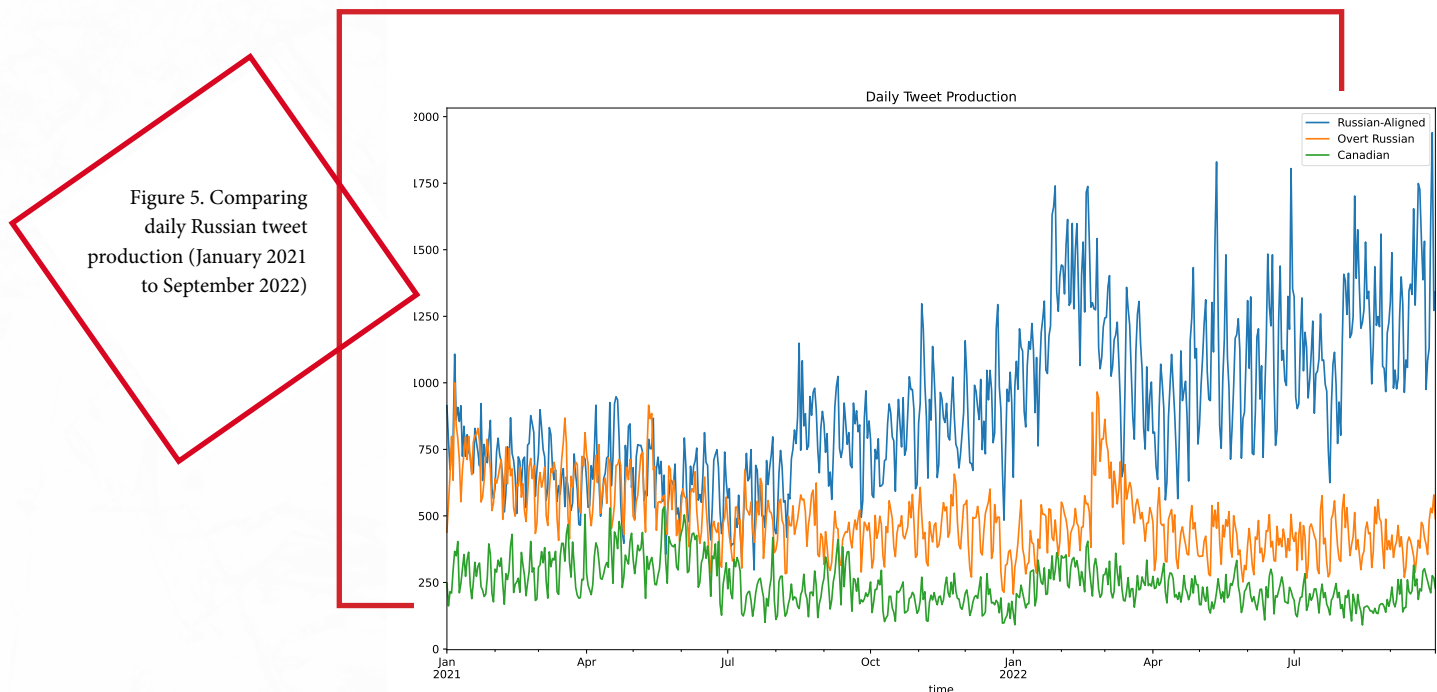
Figure 4. Daily tweet production by each set of accounts (January 2021 to October 2022)

The narratives pushed by accounts linked to Russian interests include the following narratives, many of which have been identified by previous research:

- “Canada’s foreign policy is controlled by Ukrainian Canadians.”
- “Canadian sanctions are responsible for inflation and rising energy costs.”
- “Canadian sanctions are responsible for growing global food shortages.”
- “If Canadians want to cooperate with Russia on climate and Arctic issues, then we must return to diplomacy.”
- “Ukraine is corrupt and doesn’t deserve our support.”
- “Russia is de-Nazifying Ukraine.”
- “NATO is responsible for the war.”
- “Western support for Ukraine should stop because it will cause nuclear Armageddon.”

### 5. Russian information operations spiked in the three months before the invasion.

The study examined tweets from Russian-aligned accounts for a full year before the invasion on 24 February 2022. This analysis allowed the researchers to establish baseline assessments of the ecosystem that would later be central to amplifying Russian government narratives. Figure 5 tracks the daily tweet production of three Twitter ecosystems described before: (a) online political community engaging with Canada’s 338 MPs, (b) twenty of Canada’s most influential Twitter accounts, and (c) a Russian aligned-network focused on Canadian content. Our analysis showed that the production of tweets in the Russian-aligned accounts quadrupled in the three months before the invasion, providing compelling evidence of a premeditated campaign to shape Canadians’ views before the invasion. The results also highlight a steady increase of approximately 8 percent per month in the tweet production of that network since 24 February 2022.



## Section 4

# RECOMMENDATIONS

## to Combat Russian Disinformation in Canada

**W**e've highlighted the prevalence and reach of the Russian government's efforts to undermine Canadian support for Ukraine. These efforts began months before the invasion and are increasing as the war continues. To better combat Russian influence operations in Canada, we recommend the following:

### **1) Strengthen government systems of oversight and information sharing.**

*a. Increase efforts to ensure elected officials at the federal and provincial levels are aware of the extent and strategies of Russian influence operations in Canada.* This would include regular briefings to elected representatives and government officials to help ensure they do not inadvertently amplify or normalize pro-Russian narratives. Additionally, provide targeted training on emerging security threats created by new information and communication technology.

*b. Establish an All-Party Parliamentary Committee for Defending Democracy* that would include members from each political party in Parliament, members of the Security and Intelligence Threats to Election (SITE) Task Force, and representatives from civil-society experts and the media. The members would receive regular reports about active foreign information operations and issue joint statements to counter and debunk them on a timely basis.

*c. Form a National Council For Democracy* that would monitor emerging threats and foreign influence narratives. The group would alert social media and government representatives to these threats and possible responses. It would also formulate a national whole-of-society strategy to foster long-term national resilience against malicious foreign information and influence operations. The initiative could be modelled on a similar effort in Taiwan, where civil society monitors and exposes foreign information manipulation and interference threats. Social media and government representatives are alerted to these threats and act accordingly. Social media platforms operating in Taiwan then dethrottle the identified narratives. When required, targeted government agencies can produce responses to directly address and often “pre-debunk” narratives within one hour of being alerted. The council would have representatives from some of the following constituencies:

- Canadian civil society experts
- Media representatives, editors, and publishers
- Social media platform representatives
- Government officials from responsible ministries, departments, and agencies.

*d. Ensure greater intergovernmental coordination and collaboration.* Several Canadian federal and provincial ministries, departments, and agencies have ongoing responsibilities and programs that monitor, analyze, or expose foreign information operations. They include, for example, the Global Affairs Rapid Reaction Mechanism,

Privy Council Office, Heritage Department, National Defence and Canadian Armed Forces, Communications Security Establishment (CSE), Canadian Security Intelligence Service (CSIS), and the RCMP. Establishing an overarching committee within the government could improve intergovernmental coordination and input from civil society actors and the media. This committee could be responsible for engagement within the National Council for Democracy (see recommendation 1c) and provide data to the All-Party Parliamentary Committee for Defending Democracy (see recommendation 1b).

## **2) Increase international coordination and collaboration.**

Many of Canada's allies have significant experience in defending against the threat of malicious foreign information operations and have done so effectively over the last decade. This includes the Baltic States, Finland, Sweden, and Taiwan. Many of these governments have adopted whole-of-society approaches to defending their societies, including robust early childhood education to provide cognitive resources that allow children to assess information through a critical lens. Malicious foreign information operations and narratives often target multiple nations in the community of global

democracies. The Canadian government should coordinate efforts to monitor and expose information operations targeting this community and collectively advocate for more robust self-regulation by social media companies.

## **3) Increase support to schools, civil society, and research organizations.**


*a. Support efforts by civil society and researchers to monitor, analyze, and expose foreign disinformation narratives.* Greater awareness of these narratives, the reasons foreign actors use tactical narratives, who they target, and the consequences of such narratives will lead to greater long-term resilience against them.

*b. Social and digital media literacy are essential skills for Canadian society.* It is especially crucial that children develop the necessary skills to inoculate them against information operations. The Canadian government should follow the example of Finland and the Baltic states by including digital media literacy and awareness in all school curricula from early childhood to high school. For instance, in Finland, at every grade level, digital media literacy is included in all classes, including science, math, and civics courses. Early and ongoing education and awareness will help ensure that



Exploded House in Borodyanka





students have the cognitive resources necessary to critically assess and consume information regardless of platform or source. This would require coordination among provinces, municipal authorities, and Canadian textbook publishers.

#### **4) Social media companies should provide researchers with greater access to data.**

Researchers' capacity to study foreign information campaigns in Canada is dramatically limited by the restrictions placed on academics studying most social media platforms. Governments should incentivize these platforms to provide access to researchers and civil society organizations. The quantitative research in this report is based on Twitter data because of its publicly available API. While we found evidence of Russian influence operations on other social media platforms (including Facebook, Instagram, and YouTube), we were limited in our ability to examine its scope. Social media companies serious about understanding the misuse and weaponization of their platforms by violent and extremist actors must equip researchers with the tools required to quantify the breadth and extent of the problem. With support from these platforms, researchers and civil society can help identify emerging threats.

#### **5) Stay ahead of Pro-Russian networks through real-time monitoring and learning.**

Current moderation efforts tend to be based on community standards and policies, often aiming to manage violations rather than preventing or minimizing them. Given that malicious networks typically find ways to circumvent rules and restrictions, social media companies can retain their edge by focusing on building — and sustaining — a continuous learning system that can monitor and adapt more quickly than nefarious actors can. This shift in moderation techniques involves reducing the reliance on reactive strategies that respond to single inappropriate activities and instead increasing the capacity to track foreign interventions and their enabling networks. Developing and maintaining

an actor-centred approach requires continuous input from relevant experts. By undertaking this transition, social media platforms and government agencies can enhance their ability to prevent and stem the spread of harmful content before it reaches large audiences.

All signs suggest that the war in Ukraine will continue for the foreseeable future. Ukraine's ability to fight will heavily depend on continued Western support. It is almost certain that efforts by the Russian government and its proxies to undermine support for Ukraine will only increase in the coming months. It is also likely that social media platforms will continue to be the main avenue for influence operations, disrupting authentic political debate in Canada.

Canadians should be able to discuss and debate the nature of support to Ukraine without malicious influence by foreign states. It is therefore crucial that the Canadian government, civil society, and social media platforms work together to reduce foreign influence operations. This should include additional resources for monitoring foreign interference. For instance, creating Russia and China teams within the Rapid Reaction Mechanism at Global Affairs is a welcome step toward achieving this. However, a whole-of-society approach is required, as is greater coordination and cooperation between relevant departments.

A crucial element of that approach involves better tools and methods to map the evolving ecosystems in Canada that are co-opted — willingly or not — by foreign influence operations to ensure their impact can be minimized. These tools include human-in-the-loop AI solutions that draw upon human analysis of the rapidly changing threat combined with the reach and pattern recognition of specialized AI algorithms. Together, they can contribute to timely and effective monitoring, exposing and countering foreign narratives injected or amplified in our information space, and will help build long-term public resilience against them.

## Centre for Artificial Intelligence, Data, and Conflict

CAIDAC's goal is to create a global, state-of-the-art platform to share human-in-the-loop AI tools, labels, models, and algorithms to capture social media's transformation of conflict, political violence, and war.

Its mission was born from our experience living in communities affected by violence. We watched as social media transformed conflict and also provided unprecedented documentation of events on the ground. And yet, the methods and tools available to researchers and humanitarians to study conflict have not undergone a similar revolution. CAIDAC's researchers are motivated by the real-world impact of our research on practice and policy. We strive to be a place of innovation: a hub for individuals with different skill sets and backgrounds to address consequential problems they could not attempt alone. We value humility, unusual perspectives, and a desire to change the world (for the better). CAIDAC was co-founded by Laura Courchesne, Brian McQuinn, Cody Buntain, Denilson Barbosa, and Matthew Taylor.

Brian McQuinn  
University of Regina

Marcus Kolga  
DisinfoWatch and The Macdonald-Laurier Institute

Cody Buntain  
University of Maryland College of Information Studies

Laura Courchesne  
Stanford University

