Executive Summary

The manipulation of public opinion over social media platforms is a critical concern of the 21st century. Around the world, state and non-state actors are leveraging social media to spread disinformation to voters at key moments during public life. While the cyber element of elections security has traditionally focused on securing ballot boxes or voter registration rolls, governments are increasingly concerned about the impact of harmful information on democratic outcomes. As a result, this policy brief explores the challenges pertaining to social media manipulation as they relate to Canada’s upcoming federal election. By exploring some of the global trends of social media manipulation, the policy brief also discusses domestic and foreign threats to Canada’s democracy, and provides some practical and concrete steps for industry, government and Canadian citizens to enhance both the integrity and security of the information ecosystem in Canada.
About the Authors

Samantha Bradshaw is a Senior Fellow at the Canadian International Council and a Researcher on the Computational Propaganda Project at Oxford University. She is also a D.Phil. candidate at the Oxford Internet Institute and her dissertation examines government use of social media for coordinated digital disinformation campaigns. Samantha’s work has been featured by numerous media outlets, including the Globe and Mail, Washington Post, Bloomberg, and the Financial Times. She holds an MA in global governance from the Balsillie School of International Affairs, and a joint honors BA in political science and legal studies from the University of Waterloo.
Introduction

Cybersecurity concerns around elections have traditionally been focused on the physical security of ballot boxes and voter registration cards. But following a series of highly contentious elections in the United States and Europe involving strategic data leaks, widespread disinformation campaigns, and allegations of Russian interference, securing elections has also become about securing the integrity of information and the digital ecosystem that supports it. Increasingly, state and non-state actors are leveraging social media technology to spread fake news, generate false consensus and target propaganda to voters at key moments during political life. These actions not only serve to manipulate the outcome of elections, but also undermine trust in our political leaders, democratic institutions, and liberal international world order. As Canada begins preparing for its 2019 federal election, the softer and more subtle effects of social media manipulation are raising a number of pressing concerns for policymakers.

In Canada, digital infrastructure and information are an increasingly vital component supporting elections. Today, most Canadian citizens use the Internet and social media on a daily basis, with nearly 90% of all Canadian households connected to the Internet. Facebook and YouTube are the dominant social media platforms with 75% of the online population connected to them. Because of its ubiquity and importance in everyday life, social media is increasingly a place where Canadians find news and information that is relevant to politics, and engage in democratic discussion and deliberation. And it’s also where political parties identify new voter constituencies, target political messages and advertisements, and communicate and coordinate with their support base.

Given the importance of the Internet for elections and politics alongside widespread concerns surrounding foreign interference, the federal government recently invested 7.1 million dollars over five years to improve various aspects of Canada’s election security. Elections Canada also plans to reallocate 14 million dollars in 2018-2019 to protect the electoral system from cyber-related threats. In particular, 3 million dollars will be used to hire staff to work full-time on issues related to election interference at the federal level in 2019. These expenditures demonstrate that the security and integrity of the information ecosystem in the run-up to the 2019 election is a key priority for the Canadian government.

This policy brief explores the challenges pertaining to social media manipulation as they relate to Canada’s upcoming federal election. The first section provides context around the global trends in social media manipulation. It reminds readers that election security is not just about foreign interference, but also about how domestic actors in democracies are leveraging technological affordances to pave the way for populist movements and polarization, which challenge Canada’s traditionally diverse and pluralist political environment. The second section briefly outlines some of the policy responses to fake news, disinformation and social media manipulation. Focusing on government responses and private self-regulation, this section explores contemporary policy debates about free speech and democracy. The final section of this policy brief provides some practical and concrete steps Canadian industry, government and citizenry can take to enhance the security and integrity of the information ecosystem in Canada.

4 Ibid
Election Interference in the 21st Century: Old Problems, New Technology

Although Russia’s meddling in elections have dominated media headlines, election interference is not a new phenomenon limited to a few bad actors. For quite some time, adversaries have used communication technologies to spread disinformation and interfere with citizens’ abilities to make sound political decisions at key moments in public life. So-called “fake news” is as old as news itself and has long been used to influence the way individuals think and feel about politics. The telephone also opened new opportunities to reach individuals on a wider scale using automated robocalls that deliver pre-recorded messages to individuals. However, what is new about election interference in the 21st century is social media and the ways in which networking technology changes the scope, scale, and precision at which propaganda can be distributed and consumed. In addition to creating a larger vector for disseminating bad information, the vast amounts of data produced about users on social media has meant that propaganda can also be personalized much more than in the past. And reaching individuals with tailored messaging is relatively cheap to do, as online advertising has become the business model that social media is built upon.

The shifts that have occurred in communication technologies over the past few decades have truly revolutionized society. But what was once praised as a powerful tool that could topple authoritarian regimes, is now being used to undermine democracy. High-profile influence operations and the waves of populist movements have underscored new challenges that social media is increasingly posing for politics. And state actors are exploiting this technology to shape electoral outcomes. Traditionally, authoritarian states have used digital communication infrastructure as a tool of social control, to censor information and shape public attitudes within their own borders. But recently, social media technologies have been leveraged by foreign actors to meddle internationally. In 2016 and 2017, there has been a growing stream of evidence of foreign influence campaigns taking place during the Brexit Referendum, as well as the elections in the United States, France, the United Kingdom, and Germany.

The most prolific example of foreign meddling via social media occurred during the 2016 US election when Russian operatives used traditional hacking techniques in combination with data leaks and disinformation campaigns to create and amplify divisions between voters, with the ultimate goal of undermining American democracy. Following the outcome of the election, the three major social media platforms in the United States—Google, Facebook, and Twitter—shut down multiple fake accounts operated by Russians and handed over propaganda that was targeted to voters.

The actions came after the Senate began an investigation into Russian interference in the US election, which also led to the indictment of members of the infamous Internet Research Agency [IRA].

---

6 Ibid
The IRA—colloquially referred to as Russia’s troll factory—is a Russian organization that uses the Internet and social media technology to advance Russia’s domestic and foreign policy agenda. As early as 2014, the IRA had begun a long-term influence campaign that had the strategic goal of sowing discord in the US political system. Russian operatives posed as American citizens and created multiple groups, pages and posts around various political issues. Divisive messages from both sides of the political spectrum were spread and amplified through these fake personas and pages while derogatory messages were shared about a number of candidates. And members of the IRA posed as fake grassroots organizations to stage political rallies inside the US.

The IRA’s influence operations were also combined with traditional hacking campaigns. In addition to more blunt attempts at attacking US electoral infrastructure,\(^1\) operatives spent months social engineering their way into the emails of prominent members of the Democratic National Committee (DNC), using spear phishing techniques to steal passwords and account credentials. Troves of emails were dumped on WikiLeaks containing the DNC’s interactions with Hilary Clinton and Bernie Sanders, as well as personal information such as phone numbers, addresses, and social security numbers of various members of the party.

The IRA made multiple expenditures to carry out these activities. As an organization, it employs multiple people, from content creators to technical and administrative staff, who receive salaries and benefits for their work. The IRA also spent large sums of money on equipment and buying political advertisements on Facebook to target voters. There is also a growing amount of evidence that the IRA was involved in spreading messages during Brexit, elections across Europe, and is actively spreading propaganda in many Baltic countries,\(^2\) such as the broader hybrid war taking place in Ukraine.\(^3\)

Spending on social media manipulation is not a unique phenomenon, but is actually big business. Every year, millions of dollars are spent by governments around the world to develop tools and capacities to manipulate social media for use both at home and abroad.\(^4\) Sometimes governments develop the capacity in-house, where as other times strategic communications firms are hired to spread disinformation, suppress voter turnout, or generate “astroturf” or fake grass-roots movements around a particular issue or candidate.\(^5\)

There are a number of strategies being used around the world to manipulate public opinion and hack democracy. In addition to targeting advertisements to users, other strategies involve creating “political bots”, or pieces of code designed to mimic human behavior online. These bots can spread propaganda and generate a false sense of popularity or momentum around a particular issue or idea by algorithmically inflating the number of likes, shares, or retweets of a story or hashtag. State-sponsored cyber troops are also used to troll, harass and prey upon political dissidents, journalists, and civil society advocates. And as we have seen during the elections in the United States in 2016, sometimes it’s not even about altering a citizen’s political identity or affiliation, but rather creating multiple competing narratives to distort truth, confuse voters, and discourage political participation. Table 1 summaries some of the basic strategies of election interference via the Internet and social media.

---


\(^5\) Ibid.
Table 1: Election Interference through Social Media Technology: Tools and Techniques

<table>
<thead>
<tr>
<th>Traditional Cyber</th>
<th>Computational Propaganda</th>
<th>Communication Strategies</th>
<th>Messaging and Valence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Espionage</td>
<td>Political Bots</td>
<td>Creating Disinformation, Conspiracy Theories</td>
<td>Trolling and harassment</td>
</tr>
<tr>
<td>Hacking Voter Systems</td>
<td>Search Engine Optimization</td>
<td>Fake groups, pages and personas</td>
<td>Pro-government posts</td>
</tr>
<tr>
<td>Spear Phishing</td>
<td>Big Data Analytics &amp; Advertising</td>
<td>Astroturf movements</td>
<td>Distraction, multiple competing narratives</td>
</tr>
<tr>
<td>Data Leaks</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In June 2017, the Canadian Security Establishment (CSE) published a report on cyber threats to Canada’s democratic system. The report noted that in 2017 alone, 13 out of 17 democratic countries holding elections had their democratic processes targeted by foreign adversaries. Prime Minister Trudeau has stated that election meddling on social media is a “new reality in elections”. Indeed, there has already been mounting evidence of known Russian troll accounts spreading disinformation and sowing discord around Canadian policy issues, from the Keystone Pipeline to asylum seekers and refugees. The accounts posted polarizing messages, supporting both sides of the debate in order to further divide Canadians on contentious policy issues. Given the growing evidence of foreign interference already taking place on social media, Canada’s security community is rightly concerned that the 2019 federal elections could be a target. As a result of global trends in disinformation, as well as these early warning signs, the federal government has made a number of investments to hire more staff and improve the cyber security of political party candidates in the lead-up to the 2019 vote.

But it is not just foreign adversaries who might seek to undermine the Canadian electoral process. Around the world, there are also a number of threats to democracy coming from within: groups on the fringe of the political spectrum are successfully leveraging alternative media systems to spread falsehoods, conspiracy theories and hate speech that fuel cynicism and polarization between friends, families and voters. And political parties are increasingly deploying data-driven targeting in ways that mask transparency around political campaigning. Several political parties in democracies around the world have also hired firms such as Cambridge Analytica to help shape the outcome of elections through data-driven campaigns that can nudge public opinion and suppress voter turnout. Even in Canada, in 2016 the Liberal Party considered hiring the data analyst who blew the whistle on Cambridge Analytica.

While foreign interference in the 2019 elections will most likely take place, the overlooked threats to election security come from within. In Ontario, there is already emerging evidence of political bots being used to shape the popularity of the recently elected Premier, Doug Ford, the leader of the Ontario Progressive Conservative Party. And a number of Facebook pages and groups have been created to share junk news, polarizing messages and derogatory content that mimics the messaging strategy of other populist movements around the world. At the same time, there are no privacy laws at the federal level that protect Canadian voter’s data privacy, which creates a ripe environment for political parties to harvest data for micro-targeted political advertisements with limited transparency, accountability, or oversight.

The confluence of big data analytics, foreign meddling in electoral processes, targeted political advertising, and a lack of transparency around the ways in which social media companies collect data and personalize newsfeeds is the context in which policymakers need to address the question of elections security. As traditional democratic practices are disrupted by social media

technology, there is an increasingly blurry line between news and entertainment, paid advertising and free media, and domestic actors and foreign adversaries. A strong democracy requires high-quality news, a pluralistic climate of opinion and the ability to negotiate public consensus. But powerful political actors—both foreign and domestic—are increasingly leveraging social media to manufacture consensus, manipulate public opinion, and subvert democratic processes.

Government Responses and Industry Self-Regulation to Social Media Manipulation

Given the current challenges at the intersection of social media and democracy, there is growing momentum for both industry and government to restore the health of our digital ecosystem. Despite the common belief that the Internet is unregulated, uncontrolled, and that data can move freely from one person to another, government and industry actors play a significant role in controlling online information. In democracies, child pornography, hate speech, and language that incites violence are a few examples of harmful content that is blocked and policed. The current question policymakers are struggling with is whether disinformation and fake news qualify as harmful content that needs to be regulated.

Following a series of highly contentious elections in 2016 and 2017 in democracies around the world, there is a renewed interest in the free speech debate and growing momentum for legislative reform. In many countries, there are several new proposals to address disinformation, which are quickly translating into regulatory interventions and new mechanisms of private self-regulation.

In the United States, following the testimonies of Google, Twitter and Facebook in the US Senate about the extent of Russian interference in the 2016 elections, legislators proposed the Honest Ads Act which seeks to hold online platforms accountable to standards of transparency that exist for political campaigning on other forms of communication technology, such as radio and television. In January 2017, the United Kingdom launched a parliamentary committee to investigate the issue of fake news during the Brexit Referendum. British policymakers are now exploring ways to regulate social media platforms as media or utility companies. In June 2017, the German Parliament passed a law to fine social media companies up to 50 million Euros if they do not remove fake news and hate speech from their platforms within 24 hours. The enforcement of this law has already led to criticisms around censorship, as many pundits have demonstrated the chilling effect this law has had on free speech in the digital environment in Germany. In December 2017, Irish lawmakers proposed to criminalize the use of automated bots to spread misinformation. And in July 2018, France passed a new law to combat fake news. These are only a few examples. Since 2016, more than 30 countries have proposed new laws designed to tackle the threats—both real and perceived—of fake news.

Facing widespread criticism, platforms are also taking a more proactive role in combatting disinformation. Facebook has created a system to display related (fact-checked) articles next to disputed (fake news) stories. Twitter has stopped placing advertisements from Russian-based media such as RT and Sputnik. Google

---


has removed YouTube videos linked to disinformation campaigns and Russian propaganda. It is also updating its auto-complete function to prevent promoting fake news, and has expanded Google News fact checking to countries such as Brazil, Mexico and Argentina.\(^{31}\)

And all platforms have taken steps to limit the amount of fake or bot accounts that spread junk content on their platforms. However, there are larger questions surrounding the self-regulatory role platforms should take, and whether government intervention is needed to adequately address these challenges. Platforms have always been considered themselves to be “neutral” conduits of information, unlike the mass media who play a more direct “gate-keeping” role by broadcasting one-way messages to audiences. But academics and policy-makers have questioned the neutrality of these platforms, their role as information gatekeepers, and the sustainability of their business models which can cause significant harm not only to consumer privacy, but democracy more broadly. While many of these initiatives to combat some of the challenges we have seen are small steps in a positive direction, they do not address some of these larger, systemic issues that are at the core of the problem facing our digital public sphere.

In Canada specifically, there have been a number of initiatives announced by the government and by the platforms. The “Canadian Election Integrity Initiative”, launched by Facebook, is an initiative designed to pro-actively tackle fake news through digital literacy, and will provide politicians with a crisis line should their email accounts come under attack.\(^{32}\) Facebook also announced the rollout of new ad transparency features in Canada, so users can see where political advertisements are coming from and why they were targeted.\(^{33}\)

Although it seems like regulators and social media companies are taking big strides to combat these problems, is what they are doing enough? Or are these initiatives having a chilling effect on free speech? What can Canada learn from the policy proposals that are being debated and implemented around the world? And what are some other simple steps Canada could take to improve the security of its digital information ecosystem in preparation for the election in 2019?

### How Can Canada Better Protect Itself From Digital Threats to Democracy?

During the 2019 elections social media will be an important medium for campaigning. We can expect every political party to have a digital strategy. Thus, it is imperative that Canadians start debating the norms, rules and guidelines that will inform how political parties will use these platforms to reach voters. We can also expect elements of foreign interference. Indeed, fake accounts, trolls, and political bots will be leveraged to sow discord and polarize Canadian voters. These campaigns will take place on a variety of platforms, not just Facebook and Twitter. Instagram, WhatsApp, and YouTube are increasingly popular platforms that citizens—especially young ones—are using to formulate their political identities. Tracking campaigns that seek to exploit social media will have to look beyond Facebook and Twitter and scrutinize a wide array of social media platforms that Canadians are using to connect, express, and participate.

---


Although there is quite a bit of energy around regulating social media companies, solving these complex and inter-connected issues in a technological environment that is constantly innovating is a challenge. Through the Canadian Election Integrity Initiative and various expenditures on combatting foreign interference and disinformation on social media, Canada has taken a number of steps to improve the health of its digital ecosystem, such as increasing spending to address cyber-related threats. However, democracy needs a broad cybersecurity strategy, and these initiatives could be complemented by the suggestions below to help address some of the remaining gaps in policy that, in conclusion, both foreign and domestic actors could leverage to erode the integrity of our elections in 2019.

1) Strengthening Cyber Security

Best-Practices to Prevent Data Breaches

Investments in cybersecurity for elections should also focus on continuous cyber-hygiene training. When it comes to data leaks and more traditional cyber security breaches that occur alongside disinformation campaigns, humans are often the weakest link in security. Leaked data often comes from spear phishing attempts that have unwitting users enter a username and password, or surrender other sensitive information. Individuals who work on political campaigns or in sensitive positions should receive continuous training about best practices for data protection and security. These issues should not simply be left to IT departments to manage, but instead should become a part of the organizational culture as solving security requires cooperation and effort on everyone’s behalf.

2) Improving Data Protection Laws at the Federal Level

Canada needs data protection laws around how political parties use personal data for advertising. How political parties use personal data to tailor political advertisements can be a threat to democracy if there are little to no oversight mechanisms that ensure data is not being used to discriminate against voters and suppress political participation. Currently, no federal privacy legislation covers the activity of political parties with respect to voter data: the Personal Information Protection and Electronic Documents Act [PIPEDA] only applies to the commercial collection of personal data; in the Privacy Act, political parties are excluded in the definition of “government institutions”; and the Canadian Elections Act does not oversee data collection, analysis, use, or storage. In the past, the Liberal Party made a voluntary commitment to PIPEDA, and the New Democratic Party said it will honour the transparency aspect of the law. But beyond the privacy policies of the parties themselves, there are no legal or regulatory mechanisms in place to ensure that voter data is not being misused by politicians.

3) Making Commitments to Advertising Transparency

Political parties should commit to transparent political advertising by creating publicly accessible databases of advertisements that run on social media. In the past, political advertising took the form of localized print materials or television commercials that were distributed in specific ridings. or played on TV during specific hours, based on what campaign managers could generalize about these constituencies. As advertisements have the potential to become more individualized through social media data, political parties should create public records of their advertising campaigns that includes an archive of ads placed on social media. Political parties in other countries have already used social media to send highly targeted advertisements to voters with messages designed to suppress political participation. These so-called “dark ads” are not conducive to a healthy democracy as there is no public record of the messages that individuals see. By creating a digital, public archive of political advertisements, citizens could hold political parties accountable to their campaign platforms and protect against some of the more dangerous effects of micro-targeting voters. There are already civil society efforts to draw attention to these issues, such as pro-publica program to track political advertisements on
Facebook. But more could be done at the regulatory level to demand parties to archive these advertisements themselves.

4) Leveraging Bots to Improve Political Participation

Bots and other forms of automation could be leveraged to spread high-quality information relevant to voters, such as the location of polling stations or get out and vote reminders. While political bots have often been used to amplify fake news stories, these same techniques could be leveraged to improve democratic participation. Transparent bot accounts could be used to help draw attention to important information voters need to participate fully in a deliberative democracy. By automating information about voting day or the location of polling stations, technology could help increase voter turnout across the country.

5) Limiting Opportunities for Foreign Interference

Cooperation between government agencies and the private sector are vital to limiting opportunities for foreign interference. Using social media and other technology to meddle with the democratic processes of other countries is a hard—if not impossible—issue to address. This is because the low barriers to entry and ability to innovate quickly allow bad actors to find new holes and gaps to exploit. But governments and private companies have common goals when it comes to protecting the security and integrity of our information systems. Following the Snowden revelations, there has been a steady decline in public-private cooperation on security issues. But the Cambridge Analytica scandal has created a new willingness for Facebook, in particular, to work with government. In order to limit opportunities for foreign interference, there needs to be open dialogue between security institutions and social media platforms, so that private companies can identify risks earlier, and governments can develop a deeper knowledge and understanding of the technology. The goal isn’t to completely eradicate disinformation; instead there should be more cooperation between the public and private sector that will help increase the costs and limit the reach of social media manipulation.

Bibliography


About the CIC

The Canadian International Council (CIC) is Canada’s foreign relations council. It is an independent, non-partisan membership organization and think tank dedicated to advancing constructive dialogue on Canada’s place in the world and providing an incubator for innovative ideas on how to address the world’s most pressing problems.

The non-profit CIC integrates the voices of a diverse and multidisciplinary group of societal actors from academia, business, civil society, government and the media, and endeavours to inform and develop the capacity of the country’s next generation of foreign policy leaders.

One of Canada’s oldest and most respected think tanks, the CIC is not only dedicated to nurturing dialogue on Canadian foreign policy domestically, but also in projecting a Canadian perspective on the international stage. In our rapidly changing world, this effort to promote greater understanding and foster meaningful debate on critical challenges is more important than ever.