Leadership & Democracy Lab

Political Risk Assessment

# Cybersecurity: Social, Political, and Economic Risks

Prepared by the Leadership & Democracy Lab, University of Western Ontario

Published April 2023

**Generated By**
Mateo Larrazabal – *Student Director*
Opeyemi Dinah – *Team Leader*
Sarah Kabani – *Team Leader*
Faiq Farooq – *Research Analyst*
Julia Gille – *Research Analyst*
Jack Luck – *Research Analyst*

**Democracy Lab Faculty Director**
Dr. Cristine de Clercy
Martin Eidenberg
Dr. Peter Ferguson
Bruce Fyfe

**Graphic Design & Report Layout**
Ravinder Hans

Leadership and Democracy Lab
University of Western Ontario
1151 Richmond Street
London, Ontario, Canada, N6A 3K7

http://www.democracylab.uwo.ca/

# Table of Contents

# Executive Summary

Cyber interference with elections across the globe is rife, and Canadian elections are no exception. Whether through voter list tampering or foreign cyber-tampering with the democratic process, cyber interference in federal, provincial, and municipal Canadian elections is becoming a growing concern. In the elections between 2015 and 2021, Canada has faced several cyber security threats from state-sponsored cyber attackers. China, Russia, and Iran are a few countries believed to be responsible for most foreign interference and cyber threat activity against Canadian and global elections.[1]

Voting, as an essential right, needs to be better protected, and with a nation-wide critically low voter turnout at 62.6(%) in the most recent federal election, there are salient claims to be made for the Canadian government to take action to protect elections from interference, increase voter literacy, and in turn increase voter turnout. [2]

This report will outline several cross-sector risks associated with cyber interference in elections, while additionally seeking to provide methods of mitigation for the risks. Each section of this report will begin with a brief background, followed by an explanation of the risk, and finally, mitigations of each of the risks associated with given sectors' vulnerability to cyber-interference within Canadian elections.

This report is comprised of three sections:

1. **Social Risks**
   - Evaluating the risks associated with cyber interference on voter turnout and public opinion due to an increase in distrust in political institutions following cybersecurity attacks.

2. **Political Risks**
   - Analyzes three major risks associated with the electoral legitimacy of democratic processes in the face of cyber-security threats.

3. **Economic Risks**
   - Case study assessing the economic risks posed to firms, businesses, and organizations that have a stake in the Canadian cybersecurity industry when cyber-attacks on elections infrastructure take place.

Despite the use of paper ballots, there are many sections of cyber security related vulnerability within Canadian elections. Canadian federal elections are subject to cyber security interference on several fronts, some of which includes voter registration lists, democratic processes, political parties, and elections infrastructure. The pages that follow outline the several risks and mitigation proposal strategies that are argued to be the most compelling issues and solutions for election cybersecurity firms in Canada. The risks and mitigations can be translated into essential policies that will both lessen the risks associated with cyber security attacks and enact preventative measures.

Acronyms/ Abbreviations

The Communications Security Establishment (CSE)
Canadian Security Intelligence Service (CSIS)

# Introduction

The issue of cyberattacks have become a recurring, if not, permanent feature of foreign policy agendas.[3] While cyberattacks vary in the domains they are conducted within, one fact remains consistent and that is cyberattacks are increasing in their frequency, publicity, and impact. [4] A sub-set of cyberattacks include cyber-interferences in elections, which can take the form of:

- cyberattacks against election-related infrastructure aimed at breaching the confidentiality, integrity and availability of election technology and data;
- disinformation campaigns that attempt to undermine the credibility of the electoral administration and democratic institutions;
- cyberattacks against electoral stakeholders, parties, candidates, media and campaigns; and
- disinformation campaigns designed to shape the political debate.[5]

The issue of cyber-interference in elections gained significant attention after the 2016 US presidential elections in which an array of foreign actors attempted to delegitimize Hilary Clinton's electability and potential presidency. [6, 7] However, various countries across the globe have experienced cybersecurity threats to their electoral processes for years prior to this event.[8] Nevertheless, the onset of the COVID-19 pandemic has resulted in the increased digitalization of various electoral processes, to which the opportunity for cyber-interference significantly increases.[9] While Canada's federal elections have remained paper-based, this does not mitigate the risk of cyber attackers attempting to manipulate other election-related processes online.[10]

According to the most recent update from the Canadian Centre for Cyber Security, Canada has experienced only a fraction of targeted cyber activity compared to the rest of the globe.[11] While cyberattacks to Canada's elections infrastructure remain a plausible threat, the Government of Canada has instituted a variety of measures in attempts to offset these risks. For example, the Canada Elections Act was amended with the passing of the Elections Modernization Act in 2018, aimed with safeguarding the electoral process from cyber threats.[12] Additionally, the Canadian Government has launched several initiatives and agreements to enhance communication and information sharing between state and non-state actors regarding political concerns.[13]

The upholding of free and fair elections marks the cornerstone of democracies as this process is one of the most transformative ways citizens can determine the course of change in their societies. As such, it is imperative Canada remains in constant awareness of cybersecurity risks and routinely enhances its protection measures so that democracy is not undermined.

# Political Risk

Cyber threat actors are targeting democratic processes around the globe at unprecedented levels. According to the Canadian Center for Cybersecurity, it is extremely likely that Canadian voters face a form of foreign cyber interference either prior to, or during the next federal election.[14] Cyber threat actors customarily target a combination of voters, political parties, and election infrastructure.[15]

The political risk section will analyze three major risks associated with the electoral legitimacy of democratic processes in the face of cyber-security threats. These risks include the conduction of cyberespionage for the purposes of coercion and manipulation of political parties, the lack of regulation, standards or guidelines which align the country's cyber-security objectives, and the unauthorized access to elections software and management resulting in tampering of election results and stealing of voter information. To mitigate these risks, this section will address potential national security policy responses and government training to increase the resources needed to protect the Canadian democracy against legitimate cyber threats.

## Risk #1: Conducting cyber espionage for the purposes of coercion of political parties and gathering of private data

The Canadian Centre for Cyber Security (Cyber Centre) deems Canada's democratic processes remain a lower-priority target, and as such, is not likely to face the same risks as high-profile countries such as the United States, most notably facing a wave of cyber-threats and interference during the 2016 US presidential election.[16, 17] Nonetheless, the digital era has accelerated opportunities for threats on Canadian democratic processes and unprecedented rates. The Communications Security Establishment suggests that the federal voting process is not necessarily vulnerable due to the continued use of paper ballots, but rather turns its attention to efforts targeted toward voters and political parties and candidates.[18]

As political parties and politicians are aiming to persuade voters to support their campaigns, cyber-threat adversaries could acquire harmful information to sway voter opinions of candidates.[19] With the rise of digital operations in elections, more confidential documents are stored on mainframe and individual computers, leaving new opportunities for cyber espionage.[20] Cyber adversaries may use the private information of political staff for manipulation or coercion purposes. This occurred in the 2016 United States federal elections when both the Democrats and Republicans were subjected to cyberespionage threats by Russia, which ultimately led to the leakage of emails from public political staff within the Democratic party.[21] In December of 2022, then released Government documents confirmed that the Privy Council Office was made aware of alleged attempts of Chinese interference in the 2019 general election, which were found in the document as "an active foreign interference (FI) network" under the header "Canada-China".[22] Following the 2019 and 2021 elections, CSIS made public a document on "Foreign Interference and Hostile Activities of State Actors", which declared that

"CSIS actively investigated a number of threats across Canada related to the 2019 Federal Elections and provided classified briefings on its threats assessments and investigations to the Critical Election Incident Public Protocol Panel".[23]

While according to Canada's security agencies, the extent of the interference did not meet thresholds to raise concerns regarding the overall integrity of the elections, there is lack of public knowledge on what type of foreign interference was experienced, and how the final judgment was determined.[24] With the lack of transparency from the Canadian government, Canadians lack accessible resources to educate themselves on the severity of cyber-security threats, and feel secure that the government has the proper tools to adequately deal with potential threats. The issues raised do not help to inspire confidence for the strength of existing cyber-security for Canadian federal elections.

## Risk #2: Ill-functioning or unauthorized access to online elections software resulting in potential tampering of election results, prevention of voter registration, and stealing of voter information.

The *Cyber Threats to Canada's Democratic Process: July 2021 Update* put forth by the Canada's national cryptologic agency, the Communications Security Establishment, determined that the incorporation of technology and the transitioning of several parts of the democratic processes (municipal, provincial, and federal elections) online has "almost certainly increased the cyber threat surface of democratic processes.[25]

Political parties have access to parts of voter registries from election bodies. This includes personal information of millions of Canadian citizens, including registered voters and political donors.[26] In addition, the entirety of voting registry information is connected on the internet for the federal, provincial/territorial, and municipal level.[27] If the voter registration is occurring online, cyber threat adversaries could use several cyber tools to attack the process by making the website inaccessible, polluting the database with fake voters, or attempting to encrypt or erase data altogether.[28] While there is lower risk to the actual voting process within federal elections due to the use of paper ballots, results of the vote could be tampered with during the deliverance to a centralized location, which can be done by hand, phone or through the Internet. When done through the Internet, cyber capabilities could tamper with the results while in transmission.[29]

While paper votes can be recounted, the delay and uncertainty of results could cause mass mistrust within the federal election process and may lead to the contestation of election results.[30] In 2015, many rural Canadian voters with a history of voting found themselves suddenly unlisted on Election Canada's voter registration website. A spokeswoman with Elections Canada attributed the misinformation to the fact that certain cases within the system were not able to accommodate "rural numbers". This resulted in several rural voters becoming disengaged from participating in the upcoming federal election.[31] The

**FIGURE 4:** Target: Elections

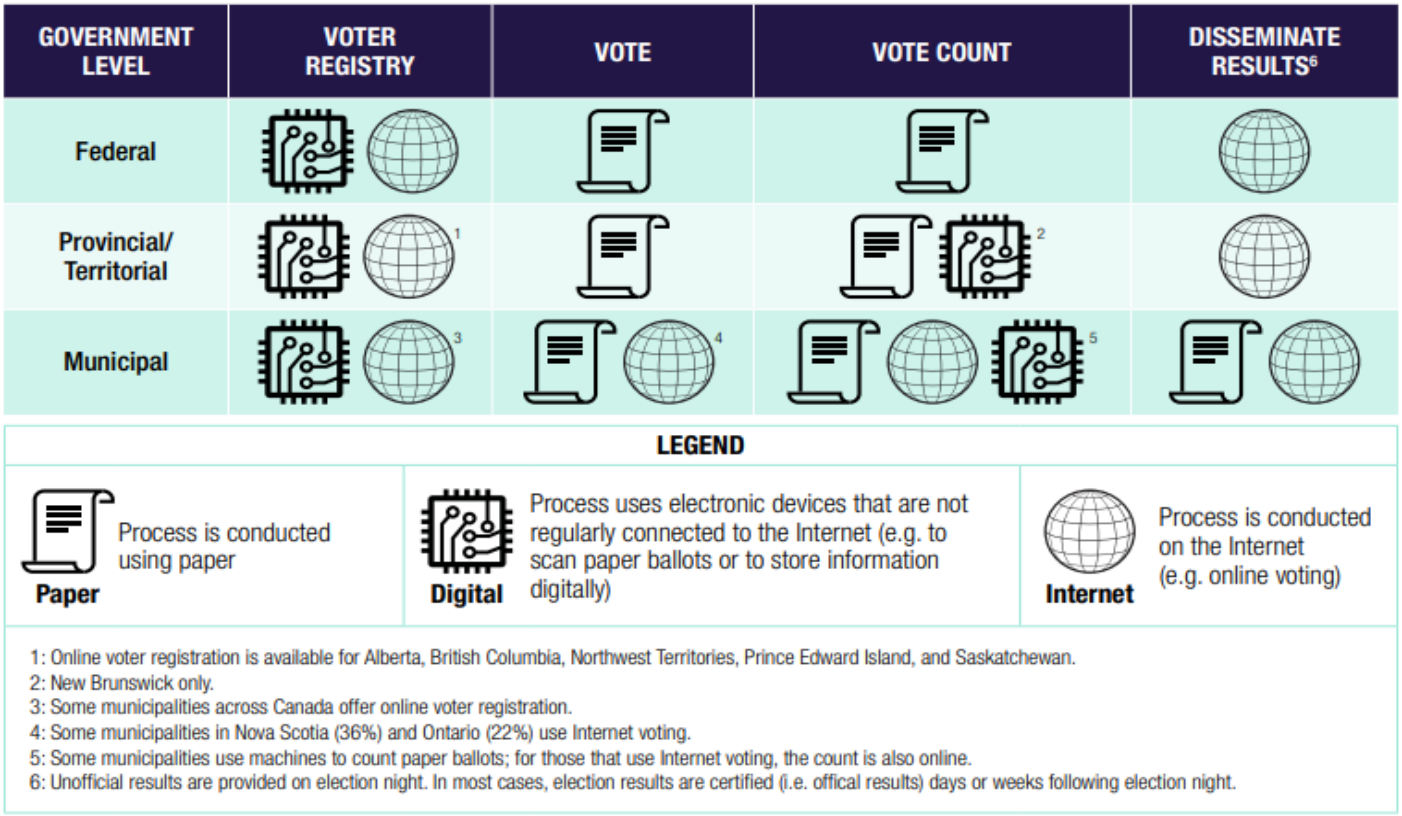


Figure 1

small-scale nature of this cyber-security risk due to the Elections Canada website glitch highlights the potential risks of incorporating more technology within the federal election processes. While the risk of the glitch having long-term effects on citizen trust in federal election cyber-security safety is low, it demonstrates why effective mitigations to potential cyber-security issues is pivotal.

## Mitigation #1: Training of election officials, political parties, and civil servants on how to detect and respond to potential cyber espionage and security risks.

Efforts across the federal government and governmental organizations are being made to build human capital resilience regarding the growing threat of cybersecurity. For example, Elections Canada has announced their work with government departments and agencies to not only remain vigilant regarding ongoing cybersecurity threats, but also implement the appropriate safeguards to prepare for potential threats.[32] However, this awareness and training is often not given to the civilians and political officials working across the country, limiting the organizations where people are able to identify credible threats.[33] The efforts to increase awareness should be extended to include political candidates, election officials, political parties and civil servants.

These efforts were made in Sweden, where as a part of the bolstering and awareness of influence activities, The Swedish Civil Contingencies Agency has given training to over 10,000 civil and public servants and the national, regional and local levels.[34] Introducing such training in the Canadian elections landscape would increase the quality of the elections infrastructure by heightening the overall understanding on how to detect and respond to potential cyberespionage and security risks.

## Mitigation #2: Implementation of Policy for Improved Interagency collaboration to enhance cyber security risk management.

There is a need for interagency collaboration to manage the complexity of cyber-security within the federal elections. Maintaining contact between

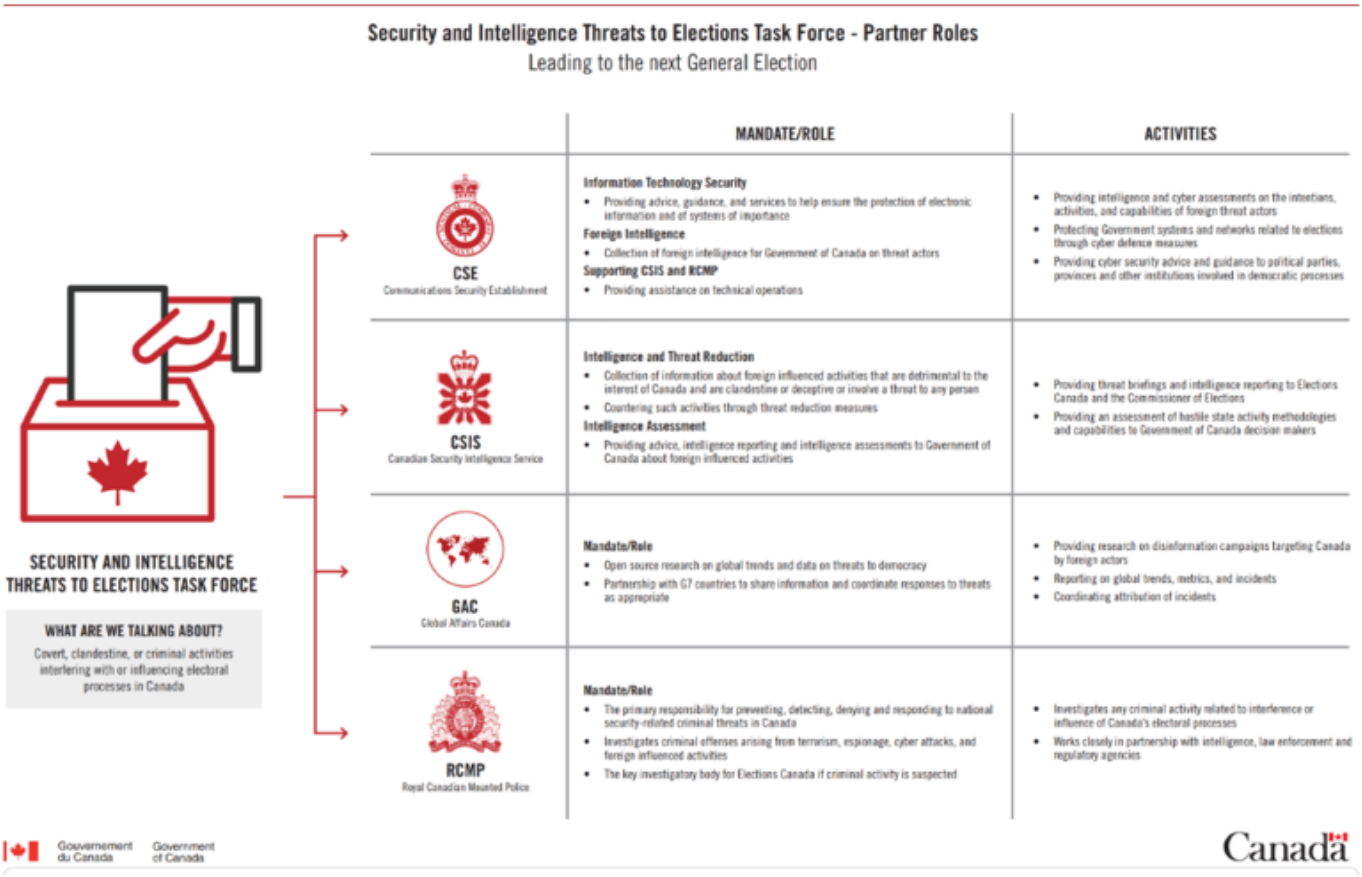


Figure 2 [35]

relevant actors and establishing internal, as well as public communication prior to the upcoming federal election would result in continued collaboration and sharing of valuable resources. In the lead up to the Canadian federal election in 2019, the Security and Intelligence Threats to Elections Task Force (SITE) was established to protect the Canadian election from foreign (cyber) interference.[36] However, the Government of Canada has not updated the SITE Partner roles, which include the mandates and activities of the Communication Security Establishment, Canadian Security Intelligence Service, Global Affairs Canada, and the Royal Canadian Mounted Police since November, 2021.[37] Election Canada should partner with the SITE actors to revisit the relevancy of their mandates in accordance with new cyber security threats. Additionally, The SITE actors should consider inviting non-government sectors such as print and broadcast media, political parties and candidates, academia, and private sector security contractors to provide their expertise and resources.[38]

Ultimately interagency collaboration would mitigate the effects of potential cyber-attacks on the electoral system, which could potentially cause damage to public confidence in the results and legitimacy of electoral authorities such as Elections Canada.[39]

# Governance Risk

Elections around the globe have been subject to digital interference, both domestic and foreign, and Canadian elections are no different. Compared to other countries in the international community, Canada qualifies as a very healthy democracy, regularly receiving high scores on worldwide assessments of civil liberties, political rights and freedoms, and stability in governance.[40] However, with the ever-changing political landscape in Canada, and the shift towards online democratic participation and engagement, cyber interference in Canadian election infrastructure poses a troubling threat to democracy, trust in institutions, and societal cohesion in Canada.

Persons or entities interfering in Canadian elections use a variety of methods to mislead the electorate to suppress or shift voter turnout, such as impersonations of electoral official or candidates through social media and traditional advertising channels. In addition, the spread of misinformation causes polarization in political discourse, shaping the attitudes and political preferences of citizens, which can lead to distrust in institutions and democracy. Considering the essential role that a politically motivated and informed electorate has in a healthy democracy, the governance risks associated with interference in election infrastructure pose serious threats to the stability of Canadian democracy. To mitigate these risks to governance and democratic stability, the Government of Canada and its various agencies and institutions should adopt measures including public education, digital literacy development, and increased government transparency, all of which will help counteract interference in electoral infrastructure and strengthen Canadian democracy.

## Risk #1: Effects on Voter Turnout & Behavior.

Interference in Canadian election infrastructure can take many forms, all of which have societal impacts on voters and social implications for electoral politics in Canada overall. As mentioned, electoral administrators, political parties, and their candidates are at risk of impersonation in the digital space, which could have negative consequences for voter turnout and behavior. This type of interference was evident in the 2011 Canadian federal election which saw fraudulent automated telephone calls, some reportedly from Elections Canada, directing voters to wrong polling stations or giving them the incorrect election date.[41] While 'robocall' scams such as these have been present in Canada for some time, the fact that malicious entities are targeting elections infrastructure could have particularly troubling repercussions for Canada's democratic processes.


Figure 3: Federal Election Polling Station; an essential part of Canadian democracy. Canada has maintained the paper ballot in federal elections, mitigating the effects of direct digital interference (Elections Canada, 2023)

In addition, those seeking to influence Canadian elections have deployed social media posts, advertisements, and phishing emails impersonating trusted public figures, such as government agencies, to manipulate Canadian voters.[42] For example, during the 2021 federal election a video circulated on Twitter showed Conservative Party Leader Erin O'Toole responding "yes" when asked whether he supports privatized healthcare in Canada. It was later discovered that this video edited and pieced together by an unknown source in order to mislead Canadian on social media, but not before it was widely circulated, reposted by prominent figures including Deputy Prime Minister Chrystia Freeland, and garnering national news attention.[43] Given the lack of accountability and fact checking that takes place on social media and online, these actions all have the potential to suppress voter turnout by sowing confusion within the electorate.


Figure 4: A screenshot of the tweet reposted by Deputy Prime Minister Chrystia Freeland during the 2021 federal election, a tweet which contained manipulated sound bites of then Conservative Leader Erin O'Toole (CTV News, 2021)

Most Canadians access news online through traditional media outlets, and increasingly through social media. Malicious entities have taken advantage of this easily accessible mode of information collection to spread disinformation and shape voter preferences.[44] The Canadian Broadcasting Corporation (CBC) conducted two separate studies, one in 2018 and another in 2019, which analyzed Twitter accounts and posts related to Canadian politics. In 2018 they found that Twitter accounts deleted after they were discovered to be connected to the Russian Internet Research Agency released over 8000 tweets related to Canadian public issues, and that content was also linked to Russian state media, extremist left and right-wing conspiracy sites, and propaganda disseminators in that country.[45] The 2019 study came up with similar conclusions, finding 21,600 public tweets directly targeting Canadians on 'hot-button' issues, such as pipelines and immigration, all of which were found to originate in Russia, Iran, and Venezuela.[46]

Each of these efforts seek to influence voter opinion and undermine social cohesion by inflaming existing divisions in Canadian political discourse. The United States is a notable example of a threatened democracy because of heightened political polarization, raising serious questions about the effects that these influence operations may be having on Canadian politics.

## Risk #2: Effects on Public Opinion of Government Institutions & Political Parties.

The CSE, Canada's signals intelligence agency, identified political parties as a weak point in Canadian election cyber security, citing that between 2015 and 2020 cyber threat activity was often directed at the major federal parties.[47] Political parties contain large amounts of personal information about their members and voters, which makes them a tempting target for cyber interference. Interference in political parties or the leaking of personal member and voter information would have widespread effects on the trust of Canadians in the electoral process.[48] Furthermore, the possibility of electoral interference and potential access to personal information may hinder Canadians' willingness to vote.[49]

Moreover, aforementioned fears about electoral intervention can have an impact on voter trust in the political system, leading to changes in attitude and

ideological polarization. This lack of confidence may lead to behavioral changes as well, including an unwillingness to access government services or participate in elections on the part of citizens.[50] For the first time in Canadian election history, Elections Canada monitored public online discussion during the 2019 federal election in an attempt to combat disinformation campaigns on social media and found that some Canadians had "profound doubts" about the integrity of Canada's electoral system. Among some of the comments were assertions that the voting system was 'rigged', claims that non-Canadian citizens might be voting in the election, and foreign entities were influencing the vote in Canada.[51] Trust in the electoral process is central to democratic stability and anything that may compromise this should be taken seriously.[52]

Finally, Elections Canada and those that facilitate and administer elections have databases that contain voter registration information, as well as information necessary to the functioning of elections in Canada. A cyber-attack or interference in the internal operations of these organizations could have a serious impact on the electoral process, possibly disrupting or derailing elections all together.[53] This is one of the most troubling outcomes that could arise from interference in elections infrastructure in Canada as it would represent a direct attack on Canadian elections, which leads one to question the democratic legitimacy of elections in Canada. The questions surrounding legitimacy of elections would surely be cause for alarm among voters, possibly dissuading some from casting their ballot at all. While there has not been any reported instances of this level of interference in Canadian elections, experts say that given the value of such information to foreign influencers, the risk for this occurring in Canada is quite high. However, it should be mentioned that there is very little research done to date on the effect of electoral interference in the Canadian context, therefore more work needs to be done on the effect that these influence operations have on voter turnout and public opinion in order to gain concrete data on its effects on democracy in Canada.

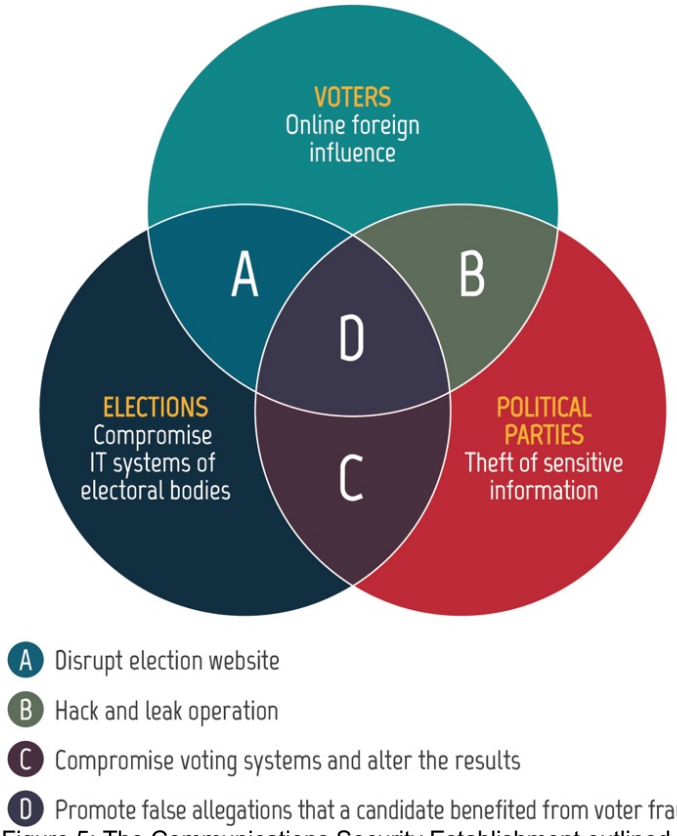

Figure 5: The Communications Security Establishment outlined three key targets for cyber interference in Canadian elections: voters, election infrastructure, and political parties (Communications Security Establishment, 2021)

## Mitigation #1: Public Education & Digital Literacy Development.

In order to combat the spread of disinformation, misinformation, and harmful rhetoric, as well as the aforementioned social effects that result from it, CSIS and the CSE recommend increased public education on how to identify and counteract cyber influencing in Canadian politics and elections.[54] It would be prudent for the Government of Canada to engage in public information campaigns warning individuals about the threats of cyber influencing on election infrastructure and steps private citizens can take to become aware of attempts to influence their political opinions and preferences. This would develop the digital literacy skills of Canadians and assist the government in their efforts to combat election interference.

A guide for best practices published by the Commonwealth Secretariat on cybersecurity for elections concurs with the CSIS and CSE recommendations, underscoring how voter education programmes, and in particular media and digital literacy training for youth, the next generation of

voters, are essential to combatting foreign influence operations on elections in Commonwealth countries.[55] By having an electorate equipped with the tools and techniques to identify influence operations and cyber interference in Canadian elections, voters are less likely to be misled by disinformation and be taken by attempts to polarize and divide the political community. However, it is recommended that the Government of Canada go one step further, and emulate steps taken by Sweden to combat digital election interference, by providing training to elections workers so they can identify and resist any attempts to influence their behavior, as individuals who facilitate elections are prime target for foreign influencers. It may also be effective for the government to coordinate with media outlets and regulating bodies to come up with a comprehensive plan to track sources of disinformation online, flag that content, and actively fact-check and correct such information.[56]

## Mitigation #2: Government Transparency.

In addition to public education, it is recommended that the Government of Canada be open and transparent with the Canadian public about the threats that elections infrastructure in the country face, the risks of political engagement in the digital space, and the efforts taken to combat these attempts at election interference in order to combat the social effects associated with said interference.[57] By informing citizens about government practices during elections, it reduces the risk of Canadians being misled which would impact voter turnout and behaviour.[58] Take, for example, the 2011 “robocall” scam; public advertisements detailing the election date and how Canadian voters can accurately locate the correct polling station for them to cast their ballot could have mitigated the effects of the misinformation spread by the scam calls.[59] By being transparent with the population about government practices and the threats to the electoral process, the Government of Canada can stabilize our democracy by regaining the trust of the general public that is being eroded by malicious entities conducting influence operations in Canada.

Furthermore, government transparency could go one step further into fact-checking and correcting inaccurate information being spread by bad actors attempting to interfere in Canadian elections in order to mitigate the effects of the interference and develop a more accurately informed electorate. Elections Canada already engages in this type of activity, which includes correcting false information and misleading online content about the electoral process in Canada.[60] By expanding this effort, attempts to interfere in Canadian elections by foreign and domestic actors could be further hampered, creating a more stable electoral system and democracy in Canada. The Government of Canada should create a non-political, independent agency tasked with raising public awareness about interference in Canadian elections and equip the government and the various federal political parties with the tools and best practices to counter foreign interference. These steps were successfully taken by the Government of France, who were able to effectively mitigate the effects of digital interference and the spread of misinformation in the 2017 presidential election that took place in that country, which could act as a template for the Canadian government to combat similar threats in federal elections. [61]

# Economic Risks

Canadian elections infrastructure will become increasingly targeted through cyber-interference soon, especially considering the increasing aggression and complexity of state-sponsored attacks upon such critical systems.[62] While no major cyber breach in Canadian elections systems has been recorded, state-sponsored attempts to influence elections have been reported quite recently. Although there is limited literature on the subject, an examination of similar cases shows that there are significant economic implications associated with cybersecurity risks to Canadian elections; given such an environment, mitigation strategies must be prescribed accordingly. While different electoral outcomes may result in varied economic implications, questions about the integrity of institutions would most certainly move markets - this is the risk that lies at the center of the assessment of Canada's elections security.

However, events like the January 8th attacks, have demonstrated the risks that the renewable energy industry must contend with. Power transitions, mass corruption, and political violence and polarization are key political risks to the renewables industry in Brazil, and the following sections will outline these risks and provide mitigating strategies.

## Risks:

State actors have been identified in the manipulation of the information ecosystem for their own benefit. Even the association with such misinformation campaigns in elections is enough to cause a financial impact. One can use the 2016 United States presidential election as a case study, especially considering the similarities between Canadian and American political and media culture. Cambridge Analytica was a data consulting firm that was alleged to have helped the spread of disinformation in 2016 using data pulled from Facebook – data used to specifically target information to users to sway the election in coordination with Russian interests.[63] The data mining and targeting techniques used by Cambridge Analytica are common in the online advertising world but have been increasingly used in influencing election outcomes. The firm was quoted as spreading propaganda primarily through "creating a web of [targeted] disinformation online so people started going down the rabbit hole of clicking on blogs, websites, etc. that make them think things are happening that may not be".[64] Facebook's association with the Cambridge Analytica situation was enough to severely affect financial performance. After the revelations came to light, its market capitalization was reduced by more than $100 billion with its stock price falling nearly 20%. Additionally, user growth fell significantly, with more than 3 million users leaving the platform.[65] The Cambridge Analytica case is a considerable example that a primary association with such a misinformation campaign can have deleterious effects on economic stakeholders.

In the last three years, more than 40 cases of private companies deploying disinformation on behalf of a political actor were identified. [66] Malicious actors can target free elections through the dissemination of 'fake news', particularly with the goal to influence voters - as was the case with recent elections in the United States. Such concerns about American elections led to (for a variety of reasons) widespread doubt about the integrity and results of the 2020 U.S. election – culminating in the United States Capitol being attacked. This incident, along with other threats to the integrity of American elections, can all be linked to the rise of targeted 'fake news' and its exploitation by both state and non-state actors. Not only do primary associations with issues regarding electoral instability affect economic stakeholders, but there are secondary, more widespread impacts as well. There are now very real concerns about the medium and long-term political stability of the U.S. business environment. The reduction in the legitimacy of American elections due to cyber threats is a direct threat to the inherent legitimacy of the administration in power – the argument can be made that this can lead to greater volatility in the operating environment for business with each election cycle.

It was recently revealed through uncovered CSIS documents that China was linked to various influence operations in the 2021 Canadian general

election. China was heavily involved in using disinformation campaigns (through a variety of mechanisms, including online) and employing proxy Chinese-Canadian organizations to impact the election.[67] A post-COVID world has seen large parts of elections infrastructure move online, including campaigning, information repositories, and voter registration.[68] Given the long-term effects of disinformation on American elections on the business environment, if faced with the same doubts in Canada, firms may reconsider the scale of their activities in domestic capital markets – especially considering that the threat of electoral uncertainty has now been realized. This is in line with r*eal options theory*, which dictates that investors are hesitant to invest capital when confronted with political uncertainty. Political uncertainty in Canada, say it be the result of compromised elections, may act as a significant tax on domestic investment.[69] It may prove more economically advantageous to a firm to participate in a domestic environment stable operating conditions - secure elections lends itself to such conditions. Political uncertainty also affects the average weighted cost of capital for economic stakeholders as well, distorting what should be a well-established relationship between investment and the cost of capital.[70] This can negatively affect equity returns for firms, in turn, leading to lower non-domestic investments made by affected stakeholders, particularly due to a heightened level of aggregate risk aversion in investment activity. [71]

Such political uncertainty would also mean that firms involved in Canadian capital markets would need a higher return on investment to justify extensive economic activity within the country, as risk premiums go up and the implicit put protection that comes with a stable government is reduced.[72] These tangible effects on economic conditions would mean that Canada needs to address the root causes of potential political instability, that is, the threats that cyber activity may have upon elections infrastructure. Stable and uncompromised elections with the perception of legitimate authority are the best way to ensure the health of Canadian capital markets. A domestic economy supported by a transparent and legitimate government yields stable economic growth, even so, Canadian economic stakeholders must be wary of very real risks and ready to face them.[73]

## Mitigation Strategies

As discussed, cyber interference in Canadian elections can pose risks to economic stakeholders due to heightened political uncertainty - such risks must be properly acknowledged and mitigated. Despite the lack of specific literature on what exactly the outlook may look like for economic stakeholders, firms can still take active measures toward ensuring their own stability. Such mitigation strategies must focus on reducing the effects that political volatility and lack of confidence in policy may have on economic activity.

As such, Canadian firms must develop contingency plans of any elections to be prepared for exposure to any potential risks that may arise. This requires the active monitoring of Canadian political and electoral developments (including risks to related infrastructure), to take proactive steps. Such an emphasis on proactiveness may be reflected by hiring additional in-house political analysts/consultants whose mandate is specifically to help navigate through electoral uncertainty. Staff with specialized knowledge in domestic policy and political relationships may be well suited to leverage such knowledge in times of uncertainty to protect the economic interests of Canadian firms. Additionally, companies can develop relationships with important stakeholders including government representatives, business associations, and local communities to better understand the political landscape and possibly sway legislation in favour of core strategic interests. At the center of this strategy of leveraging relationships would be organizing with other stakeholders that may have similar core strategic interests. It has been found that the average return to lobbying expenditures ranges from 137-152%.[74] If a firm's fiduciary duty is to ensure its financial success, it may be worth exploring an additional investment in developing beneficial relationships with key government officials to promote its own business interests. Economic stakeholders can also mitigate risk by diversifying operations and investments that are held, particularly through using financial instruments such as futures, options, and swaps to hedge against potential losses due to political risk. Doing so provides economic stakeholders with ways in Canadian markets to protect themselves against the risk of financial loss due to extraneous factors,

particularly political risk. Finally, it may prove particularly useful to use insurance products, namely political risk insurance, as a final stopgap measure against political instability.

Cyber interference in Canadian elections is a topic that remains to be explored in depth. Given the nature of current elections infrastructure, limited literature is available; that being said, a comparative and theoretical approach can still be taken when considering the economic risks that compromised elections pose. Canadian firms and economic stakeholders can consider what risks may arise going forward in the broader landscape of Canadian elections and create a contingency plan to mitigate potential losses based on the suggestions outlined.

# Figures

# Endnotes

[1] Canadian Centre for Cyber Security, “Cyber Threats to Canada's Democratic Process : July 2021 Update,” Canadian Centre for Cyber Security, Government of Canada / Gouvernement du Canada, July 16, 2021. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update.

[2] “Voter Turnout at Federal Elections and Referendums.” Elections Canada. Elections Canada. Accessed March 6, 2023. https://www.elections.ca/content.aspx?section=ele&dir=turn&document=index&lang=e.

[3] Jacqueline Van De Velde, “The Law of Cyber Interference in Elections” (paper, Yale University, 2016), 1. https://law.yale.edu/sites/default/files/area/center/global/document/van_de_velde_cyber_interference_in_elections_06.14.2017.pdf

[4] Van De Velde, “The Law of Cyber Interference in Elections”, 1.

[5] Sam van der Staak and Peter Wolf, “Cybersecurity in Elections: Models of Interagency Collaboration,” International Institute for Democracy and Electoral Assistance, 2019, https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

[6] Sam van der Staak and Peter Wolf, “Cybersecurity in Elections: Models of Interagency Collaboration”

[7] Jack A. Jarmon, *The New Era in U.S. National Security: Challenges of the Information Age,* 2nd ed. (United States: Rowman & Littlefield Publishers, 2019), 190.

[8] Sam van der Staak and Peter Wolf, “Cybersecurity in Elections: Models of Interagency Collaboration”

[9] “Cyber threats to Canada’s democratic process : July 2021 update,” Government of Canada, https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

[10] “Cyber threats to Canada’s democratic process : July 2021 update,” Government of Canada.

[11] “Cyber threats to Canada’s democratic process : July 2021 update,” Government of Canada

[12] “Government of Canada passes Elections Modernization Act,” Government of Canada, last modified December 18, 2018, https://www.canada.ca/en/democratic-institutions/news/2018/12/government-of-canada-passes-elections-modernization-act.html

[13] “Cyber threats to Canada’s democratic process : July 2021 update,” Government of Canada

[14] (Canadian Centre for Cyber Security 2021)

[15] Ibid.

[16] (Canadian Centre for Cyber Security 2021)

[17] (Young 2022, 31)

[18] Ibid. 42

[19] (Canadian Centre for Cyber Security 2021)

[20] (Hansen 2020, 259)

[21] (Office of the Director of National Intelligence, n.d.)

[22] (Boutilier 2022)

[23] (Rochon 2021)

[24] (Goldstein 2022)

[25] (Canadian Centre for Cyber Security 2021)

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] (CBC News 2015)

[32] (Elections Canada 2022)

[33] (MacLellan 2018)

[34] (Cederberg 2018)

[35] (Canadian Centre for Cyber Security. 2021)

[36] (Canadian Security Intelligence Service, 14)

[37] (Government of Canada 2021)

[38] (International Institute for Democracy and Electoral Assistance, 28)

[39] (Commonwealth Secretariat 2020, 91)

[40] Elisabeth Gidengil and Heather Bastedo, *Canadian Democracy from the Ground Up:*

*Perceptions and Performance,* (Vancouver, BC: University of British Columbia Press, 2014), 03.

[41] Elizabeth F. Judge and Michael Pal, “Election Cyber Security Challenges for Canada”, (Centre for International Governance, 2019), 17.

[42] Judge and Pal, “Election Cyber Security”, 18.

[43] Media Ecosystem Observatory, “Mis- and Disinformation During the 2021 Canadian Federal Election” (Montreal, QC: Media Ecosystem Observatory, March 2022), 19.

[44] Centre for International Governance Innovation, “Threats to Canada’s Democratic Process”, (Centre for International Governance Innovation, 2019), 5.

[45] Centre for International Governance Innovation, “Threats to Canada’s”*,* 5.

[46] Centre for International Governance Innovation, “Threats to Canada’s”, 6.

[47] Canada, Communications Security Establishment, *Cyber Threats to Canada’s Democratic*

*Process,* (Ottawa, ON: Communications Security Establishment, July 2021) https://cyber.gc.ca/sites/default/files/cyber/2021-07/2021-threat-to-democratic-process-3-web-e.pdf, 3.

[48] Judge and Pal, “Election Cyber Security”, 16.

[49] Jean-Nicolas Bordeleau, “Does Election Interference Rhetoric Influence Voters’ Behaviours and Attitudes? Empirical Evidence from an Experimental Survey Study,” BA thesis, (Royal Military College of Canada, Kingston ON, 2021), 60.

[50] Bordeleau, “Does Election Interference,” 4.

[51] Ashley Burke, “Social Media Users Voiced Fears About Election Manipulation During 2019 Campaign, says Elections Canada,” *CBC News,* January 30, 2020.

[52] Bordeleau, “Does Election Interference,” 63.

[53] Judge and Pal, “Election Cyber Security”*,* 17.

[54] Canada, Communications Security Establishment, *Cyber Threats to Canada’s,* 32.

[55] Commonwealth Secretariat, “Cyber Security for Elections: A Commonwealth Guide on Best Practice”, (London, UK: Commonwealth Secretariat, 2020), 85.

[56] Margaret L. Taylor, “Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe,” *Brookings Institute,* July 31, 2019.

[57] Canada, Communications Security Establishment, *Cyber Threats to Canada’s,* 32.

[58] Commonwealth Secretariat, “Cyber Security for Elections”, 121.

[59] Judge and Pal, “Election Cyber Security”, 17.

[60] Canada, Communications Security Establishment, *Cyber Threats to Canada’s,* 32.

[61] Taylor, “Combating Disinformation.”

[62] Canadian Centre for Cyber Security, “Cyber Threat Bulletin: The Ransomware Threat in 2021.” *Communications Security Establishment, Government of Canada,* 2021, https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021

[63] Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. “How Trump Consultants Exploited the Facebook Data of Millions.” *The New York Times,* March 17, 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[64] “Trump Campaign Mined Facebook User Data Using Israeli ‘Intelligence Gathering.’” *The Times of Israel,* March 20, 2018. https://www.timesofisrael.com/trump-campaign-mined-facebook-user-data-using-israeli-intelligence-gathering/.

[65] Neate, Rupert. “Https://Www.theguardian.com/Technology/2018/Jul/26/Facebook-Market-Cap-Falls-109bn-Dollars-after-Growth-Shock.” *The Guardian,* July 26, 2018. https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock.

[66] Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. “Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." *University of Oxford*, 2021. https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/

[67] Fife, Robert, and Steven Chase. “CSIS documents reveal Chinese strategy to influence Canada’s 2021 election.” *The Globe and Mail,* February 17, 2023. https://www.theglobeandmail.com/politics/article-china-influence-2021-federal-election-csis-documents/

[68] Canadian Centre for Cyber Security, “Cyber threats to Canada's democratic process : July 2021 update.” *Communications Security Establishment, Government of Canada*, July 2021, https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update.

[69] Rodrik, Dani. “Policy Uncertainty and Private Investment in Developing Countries.” *Journal of Development Economics* 36, no. 2, October 1991: 229–42. https://doi.org/10.3386/w2999.

[70] Drobetz, Wolfgang, Sadok El Ghoul, Omrane Guedhami, and Malte Janzen. “Policy Uncertainty, Investment, and the Cost of Capital.” *Journal of Financial Stability, Forthcoming*, October 5, 2017. https://doi.org/10.2139/ssrn.2980918.

[71] Brogaard, Jonathan, Lili Dai, Phong T. H. Ngo, and Bohui Zhang. “Global Political Uncertainty and Asset Prices.” *The Review of Financial Studies* 33, no. 4, August 6, 2019: 1737–80. https://doi.org/10.1093/rfs/hhz087.

[72] Pastor, Lubos, and Pietro Veronesi. “Political Uncertainty and Risk Premia.” *Journal of Financial Economics* 110, no. 3, December 2013: 520–45. https://doi.org/10.3386/w17464.

[73] Repuccia, Sarah. “Democracy Is Good for Business.” *Freedom House,* August 3, 2015. https://freedomhouse.org/article/democracy-good-business.

[74] Kang, Karam. “Policy Influence and Private Returns from Lobbying in the Energy Sector.” *The Review of Economic Studies* 83, no. 1, January 2016: 269–305. https://doi.org/10.1093/restud/rdv029.

# Bibliography


Bloomfield, Tyler. “Why Elections Canada still uses paper voter lists and hand counts ballots for federal elections.” CBC, 9 September 2021, https://www.cbc.ca/news/politics/ask-paper-voter-lists-hand-counting-ballots-election-1.6167809. Accessed 26 February 2023.

Bordeleau, Jean-Nicolas. “Does Election Interference Rhetoric Influence Voters’ Behaviours and Attitudes? Empirical Evidence from an Experimental Survey Study.” BA thesis. Royal Military College of Canada, Kingston ON, 2021.

Boutilier, Alex. 2022. “Chinese interference: What government documents tell us about election meddling - National | Globalnews.ca.” Global News. https://globalnews.ca/news/9354682/chinese-interference-what-government-documents-tell-us-about-election-meddling/.

Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. “Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." University of Oxford, 2021. https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/

Brogaard, Jonathan, Lili Dai, Phong T. H. Ngo, and Bohui Zhang. “Global Political Uncertainty and Asset Prices.” The Review of Financial Studies 33, no. 4, August 6, 2019: 1737–80. https://doi.org/10.1093/rfs/hhz087.

Burke, Ashley. “Social Media Users Voiced Fears About Election Manipulation During 2019 Campaign, says Elections Canada.” CBC News, January 30, 2020. Accessed through cbc.ca.

Canada. Canadian Security Intelligence Service. Foreign Interference: Threats to Canada’s Democratic Process. Ottawa, ON: Canadian Security Intelligence Service, July 2021. https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf.

Canadian Centre for Cyber Security. “Cyber Threats to Canada's Democratic Process : July 2021 Update.” Canadian Centre for Cyber Security. Government of Canada / Gouvernement du Canada, July 16, 2021. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update.

Canada. Communications Security Establishment. Cyber Threats to Canada’s Democratic Process. Ottawa, ON: Communications Security Establishment, July 2021. https://cyber.gc.ca/sites/default/files/cyber/2021-07/2021-threat-to-democratic-process-3-web-e.pdf.

Canadian Centre for Cyber Security, “Cyber Threat Bulletin: The Ransomware Threat in 2021.” Communications Security Establishment, Government of Canada, 2021, https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021

Canadian Centre for Cyber Security, “Cyber threats to Canada's democratic process : July 2021 update.” Communications Security Establishment, Government of Canada, July 2021, https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update.

Canadian Security Intelligence Service. n.d. “Foreign Interference Threats to Canada's democratic process.”

Canada.ca. Accessed January 15, 2023. https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf.

CBC News. 2015. “Elections Canada website glitches show some voters as unregistered.” CBC. https://www.cbc.ca/news/canada/nova-scotia/elections-canada-online-registration-problems-1.3240393.

Cederberg, Gabriel. 2018. “Catching Swedish Phish.” Belfer Center. https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf.

Centre for International Governance Innovation. “Threats to Canada’s Democratic Process.” Centre for International Governance Innovation, 2019. https://www.jstor.org/stable/pdf/resrep21106.7.pdf?refreqid=excelsior%3A2281ebf03d7a07e1185f6c0b87b4bee3&ab_segments=0%2FSYC-6744_basic_search%2Fcontrol&origin=&acceptTC=1.

Commonwealth Secretariat. “Cybersecurity for Elections: A Commonwealth Guide on Best Practice”. London, UK: Commonwealth Secretariat, 2020. file:///Users/jackluck/Downloads/Cybersecurity_for_Elections_PDF_0.pdf.

“Cyber threats to Canada’s democratic process: July 2021 update,” Government of Canada. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

Drobetz, Wolfgang, Sadok El Ghoul, Omrane Guedhami, and Malte Janzen. “Policy Uncertainty, Investment, and the Cost of Capital.” Journal of Financial Stability, Forthcoming, October 5, 2017. https://doi.org/10.2139/ssrn.2980918.

Elections Canada. 2022. Election Integrity and Security. https://www.elections.ca/content.aspx?section=vot&dir=int&document=index&lang=e.

Fife, Robert, and Steven Chase. “CSIS documents reveal Chinese strategy to influence Canada’s 2021 election.” The Globe and Mail, February 17, 2023. https://www.theglobeandmail.com/politics/article-china-influence-2021-federal-election-csis-documents/

Gidengil, Elisabeth and Heather Bastedo. Canadian Democracy from the Ground Up: Perceptions and Performance. Vancouver, BC: University of British Columbia Press, 2014.

Goldstein, Lorrie. 2022. “GOLDSTEIN: Yes, China interfered in 2019 and 2021 federal elections.” Toronto Sun. https://torontosun.com/opinion/columnists/goldstein-yes-china-interfered-in-2019-and-2021-federal-elections.

“Government of Canada passes Elections Modernization Act,” Government of Canada. Last modified December 18, 2018, https://www.canada.ca/en/democratic-institutions/news/2018/12/government-of-canada-passes-elections-modernization-act.html

Hansen, Laura P. 2020. “The Spy Who Never Has to Go Out Into the Cold: Cyber Espionage.” In Encyclopedia of Criminal Activities and the Deep Web, edited by Mehdi Khosrow-Pour D.B.A., 258-270. N.p.: IGI Global. 10.4018/978-1-5225-9715-5.ch017.

International Institute for Democracy and Electoral Assistance. n.d. “Cybersecurity in Elections | Models of Interagency Collaboration.” International IDEA. Accessed January 15, 2023.

https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf.

Jarmon, Jack A. The New Era in U.S. National Security: Challenges of the Information Age, 2nd ed. United States: Rowman & Littlefield Publishers, 2019

Judge, Elizabeth F. and Michael Pal. “Election Cyber Security Challenges for Canada.” Centre for International Governance, 2019. https://www.jstor.org/stable/pdf/resrep26129.5.pdf.

Kang, Karam. “Policy Influence and Private Returns from Lobbying in the Energy Sector.” The Review of Economic Studies 83, no. 1, January 2016: 269–305. https://doi.org/10.1093/restud/rdv029.

MacLellan, Stephanie. 2018. “Canada's Voting System Isn't Immune to Interference.” Centre for International Governance Innovation. https://www.cigionline.org/articles/canadas-voting-system-isnt-immune-interference/.

Media Ecosystem Observatory. “Mis- and Disinformation During the 2021 Canadian Federal Election.” Montreal, QC: Media Ecosystem Observatory, March 2022. https://www.mcgill.ca/maxbellschool/files/maxbellschool/meo_election_2021_report.pdf.

Neate, Rupert. “Https://Www.theguardian.com/Technology/2018/Jul/26/Facebook-Market-Cap-Falls-109bn-Dollars-after-Growth-Shock.” The Guardian, July 26, 2018. https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock.

Office of the Director of National Intelligence. n.d. “Assessing Russian Activities and Intentions in Recent US Elections.” Office of the Director of National Intelligence. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Pastor, Lubos, and Pietro Veronesi. “Political Uncertainty and Risk Premia.” Journal of Financial Economics 110, no. 3, December 2013: 520–45. https://doi.org/10.3386/w17464.

Practice. N.p.: Commonwealth Secretariat.

Repuccia, Sarah. “Democracy Is Good for Business.” Freedom House, August 3, 2015. https://freedomhouse.org/article/democracy-good-business.

Rochon, Dominic. 2021. Foreign Interference and Hostile Activities of State Actors. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/08-en.aspx.

Rodrik, Dani. “Policy Uncertainty and Private Investment in Developing Countries.” Journal of Development Economics 36, no. 2, October 1991: 229–42. https://doi.org/10.3386/w2999.

Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. “How Trump Consultants Exploited the Facebook Data of Millions.” The New York Times, March 17, 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Staak, Sam van der and Peter Wolf. , “Cybersecurity in Elections: Models of Interagency Collaboration,” International Institute for Democracy and Electoral Assistance, 2019,

https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

Taylor, Margaret L. “Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe.” Brookings Institute, July 31, 2019. Accessed through brookings.edu.

“Trudeau Defends Liberal Campaign Video Flagged by Twitter as 'Manipulated Media'.” CTVNews, August 23, 2021. https://www.ctvnews.ca/politics/federal-election-2021/trudeau-defends-liberal-campaign-video-flagged-by-twitter-as-manipulated-media-1.5557657?cache=gszlebujvvuylyge.

Van De Velde, Jacqueline. “The Law of Cyber Interference in Elections.” Paper, Yale University, 2016. https://law.yale.edu/sites/default/files/area/center/global/document/van_de_velde_cyber_interference_in_elections_06.14.2017.pdf

“Voter Turnout at Federal Elections and Referendums.” Elections Canada. Elections Canada. Accessed March 6, 2023. https://www.elections.ca/content.aspx?section=ele&dir=turn&document=index&lang=e.

Young, Lisa. 2022. Cyber-Threats to Canadian Democracy. Edited by Holly A. Garnett and Michael Pal. N.p.: McGill-Queen's University Press. Scholars Portal Books.

“Trump Campaign Mined Facebook User Data Using Israeli ‘Intelligence Gathering.’” The Times of Israel, March 20, 2018. https://www.timesofisrael.com/trump-campaign-mined-facebook-user-data-using-israeli-intelligence-gathering/.