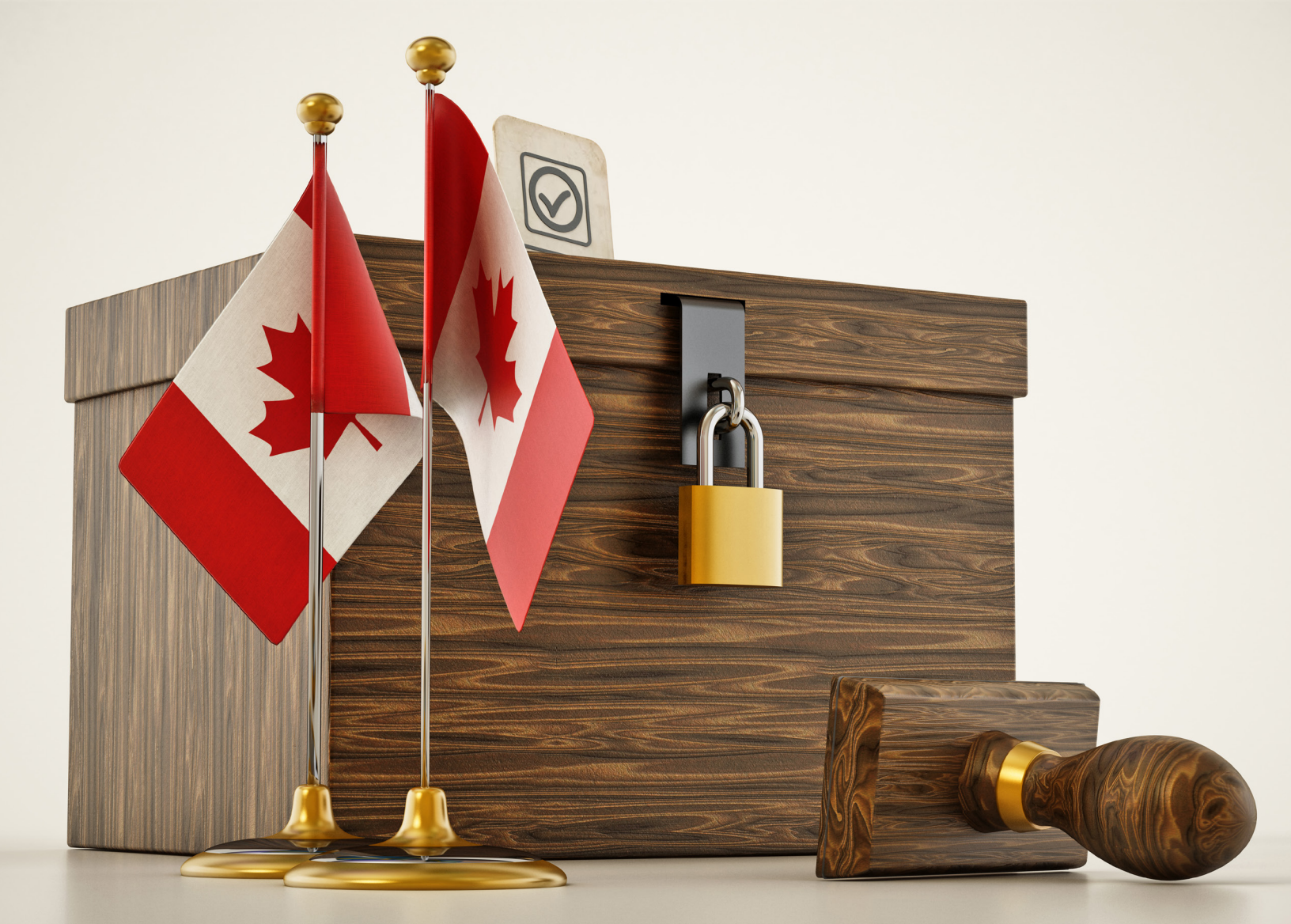
Centre for International Governance Innovation

Alliance of Democracies

Election Risk Monitor

Canada



Election Risk Monitor

Canada

Centre for International Governance Innovation

Alliance of Democracies

CIGI Masthead

Executive

President Rohinton P. Medhora
Deputy Director, International Intellectual Property Law and Innovation Bassem Awad
Chief Financial Officer and Director of Operations Shelley Boettger
Director of the Global Economy Program Robert Fay
Director of the International Law Research Program Oonagh Fitzgerald
Director of the Global Security & Politics Program Fen Osler Hampson
Director of Human Resources Laura Kacur
Deputy Director, International Environmental Law Silvia Maciunas
Deputy Director, International Economic Law Hugo Perezcano Díaz
Managing Director and General Counsel Aaron Shull
Director of Communications and Digital Media Spencer Tripp

Publications

Publisher Carol Bonnett
Senior Publications Editor Jennifer Goyder
Senior Publications Editor Nicole Langlois
Publications Editor Susan Bubak
Publications Editor Patricia Holmes
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz
Graphic Designer Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

@cigionline

Printed in Canada on paper containing 100% post-consumer fibre and certified by the Forest Stewardship Council® and the Sustainable Forestry Initiative.

Centre for International Governance Innovation and CIGI are registered trademarks.

Centre for International Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Members of the Transatlantic Commission on Election Integrity

Felipe Calderon
President of Mexico (2006–2012)

Michael Chertoff
United States Secretary of Homeland Security (2005–2009), Co-Chair

Eileen Donahoe
Executive Director, Global Digital Policy Incubator, Stanford Center on Democracy, Development and the Rule of Law

Toomas Hendrik Ilves
President of Estonia (2006–2016)

Natalie Jaresko
Finance Minister of Ukraine (2014–2016)

Tanit Koch
Editor-in-Chief of *BILD* newspaper (2016–2018)

Jeanne Meserve
Anchor and correspondent at ABC news and CNN (1984–2011), Senior Fellow at the George Washington University Center for Cyber and Homeland Security (2011–2017)

Victor Pinchuk
Ukrainian businessman and philanthropist, founder of the Victor Pinchuk Foundation

Anders Fogh Rasmussen
NATO Secretary General (2009–2014), Founder, Alliance of Democracies, Co-Chair

Allan Rock
Canadian Ambassador to the United Nations (2003–2006), President Emeritus of University of Ottawa

Marietje Schaake
Member of the European Parliament, Vice-President of the European Parliament delegation to the United States

Joanna Shields
UK Minister for Internet Safety and Security and Under-Secretary of State (2015–2017), Member of the UK House of Lords

TCEI Secretariat

Olaf Boehnke
Jana Kobzova
Harry Nedelcu
Jonas Parello-Plesner
Fabrice Pothier
Alexander Vershbow

Table of Contents

Acronyms and Abbreviations

CBC	Canadian Broadcasting Corporation
CEO	chief electoral officer
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
G7	Group of Seven
MP	member of Parliament
NATO	North Atlantic Treaty Organization
NDP	New Democratic Party
RCMP	Royal Canadian Mounted Police
SITE	Security and Intelligence Threats to Elections
TCEI	Transatlantic Commission on Election Integrity

Introduction

The Transatlantic Commission on Election Integrity (TCEI) is an initiative of the Alliance of Democracies Foundation with the aim of preventing election interference by advocating for increased transparency and fighting the use of disinformation in campaigns. In pursuing its objectives, the TCEI is systematically assessing the adequacy of laws, policies and practices in democratic states in order to evaluate the electoral resilience of those states and their ability to preserve the integrity of their elections. The TCEI met in Ottawa on April 29, 2019, to consider Canada's performance in this regard.

The special report that follows was prepared as a foundation for that assessment. It describes the legal and administrative regime that governs federal elections in Canada. It refers to threats that have been identified and to new laws, policies and investments intended to anticipate and respond to them. It documents strategies that have been adopted by the federal government and explains how Canada is contributing to international efforts (through the Group of Seven [G7]) to manage those threats. Finally, the report discusses policy choices that Canada is facing as it decides how best to deal with unresolved issues arising from the exploitation of social media platforms by malicious actors with an interest in influencing Canadian elections.

Canada's 2019 Election

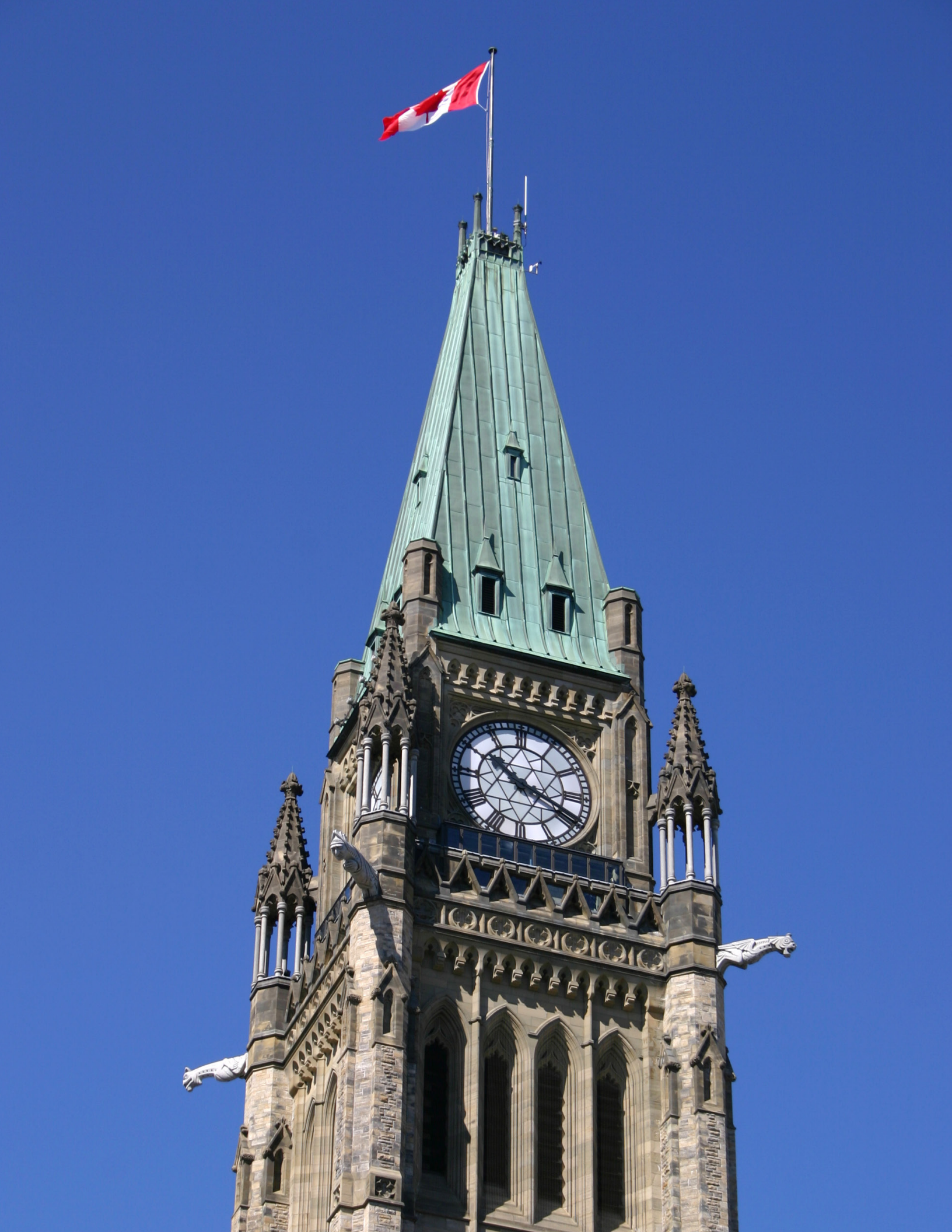
Canadians will cast their ballots in the next federal election on or before October 21, 2019. In the wake of a growing trend of foreign interference worldwide, the right to a free and fair election — a fundamental condition of democracy — is under threat, as Canada's national cryptologic agency, the Communications Security Establishment (CSE), has reported (2017, 5; see also CSE 2019, 5). As well, there is growing evidence that in recent years foreign interference has influenced other elections, in the United States, the United Kingdom, France and Germany (Bradshaw 2018, 4).

In fact, Canada's democratic process has been targeted before, by low-sophistication cyber activity during the last federal election, in 2015 (CSE 2017, 33). The media reported that "hacktivist" groups had leaked high-level federal documents taken from secure government computers (ibid.; Humphreys 2015). Prime Minister Justin Trudeau has stated that there was "not much direct interference" by Russia in that election, but he refused to provide further details, citing legislation exempting the government from disclosing information for "reasons of international affairs" (cited in Bryden 2018).

While the 2015 federal election was not a major target, Minister of Democratic Institutions Karina Gould has said that it would be "naive" to assume that Canada is not a target for cyber attacks (*The House* 2019a). Both Minister Gould and Minister of Foreign Affairs Chrystia Freeland have emphasized that Canada must be ready to identify and counter such attacks.

A member of the G7, the North Atlantic Treaty Organization (NATO) and the Five Eyes intelligence alliance, Canada is an influential member of the international community whose policy choices can affect foreign interests (CSE 2019, 9). For example, in recent months Canada has imposed sanctions on Russia under its new Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law); criticized Saudi Arabia's human rights records; and arrested Chinese Huawei executive Meng Wanzhou for extradition to the United States (Orol 2019; Momani 2019). Adversaries may seek to influence Canada's democratic process to further their own interests, to make a show of force, to damage Canada's reputation or to delegitimize democracy (CSE 2017, 13; 2019, 9). Regarding the fall 2019 federal election, Minister of National Defence Harjit Sajjan anticipates Russia will target Canadian voters through cyber attacks and fake news (MacDonald and Doucette 2018), and former Clerk of the Privy Council Michael Wernick has warned of the risk of foreign interference.[1]

1 House of Commons, Standing Committee on Justice and Human Rights, *Evidence*, 42nd Parl, 1st Sess, No 132 (21 February 2019) at 1215 (Michael Wernick) (Chair: Anthony Housefather).



Part One: The Electoral System in Canada

Canada's federal electoral system is a single-member plurality or "first-past-the-post" system (Elections Canada 2015). In this system, an elector votes for a candidate from a particular party to represent the elector's riding by becoming its member of Parliament (MP); electors do not vote directly for the prime minister. The leader of the party that elects the greatest number of MPs becomes the prime minister.

There is no limit to the number of candidates that can run for election in an electoral district, but a candidate can only run in one riding, and each party can only endorse one candidate in a given electoral district (ibid.). The candidate's name, along with his or her party affiliation (or the designation "independent," if the candidate has no party affiliation) will appear on the ballot. The first electoral districts were established by the Constitution Act, 1867, and their boundaries are periodically adjusted by an independent commission based on population changes after every 10-year census (ibid., 8); as of 2019, there are 338 districts in total.

Each electoral district represents a corresponding seat in the House of Commons. The candidate with the highest number of votes in each electoral district wins a seat in the House of Commons and represents that electoral district as its MP. An absolute majority of 50 percent is not required to be elected (ibid., 9). After a general election, by convention, the leader of the party with the largest number of elected representatives will normally form the government, and the party with the second-largest number of elected representatives will normally form the official opposition. The maximum duration of the House of Commons is five years, but elections are traditionally held every four years (Lithwick and Spano 2015, 4).

Prime Minister Justin Trudeau campaigned in the 2015 federal election on changing the electoral system from first-past-the-post to another form of voting, such as proportional representation (Liberal Party of Canada 2019). After a parliamentary review of various electoral systems, and following numerous town halls and surveys of Canadian citizens, no clear consensus emerged on what system should be adopted (von Scheel 2018). In 2017, Trudeau cancelled the electoral reform agenda, believing it would be "harmful to Canada" to move forward on a campaign promise for the sake of change (ibid.). Whether electoral reform will be a platform issue in 2019 will depend on Canadian voters' and party support to reopen the issue (ibid.).

The Office of the Chief Electoral Officer of Canada, known as Elections Canada, is an independent, non-partisan agency that reports directly to Parliament. The chief electoral officer (CEO) is responsible for administering federal general elections, by-elections and referendums. The CEO is an officer of Parliament, appointed by a resolution of the House of Commons for a 10-year term. This procedure allows all represented parties to participate in the CEO's election (Elections Canada 2015, 15).

Elections Canada, under the CEO's direction, is responsible for preparing, administering and reporting on federal elections and administering election expense provisions (Lithwick and Spano 2015, 3). The Commissioner of Canada Elections (the "Commissioner") is responsible for ensuring compliance with Canada's electoral legislation and is appointed for a seven-year term by the CEO (Elections Canada 2015, 15).[2]

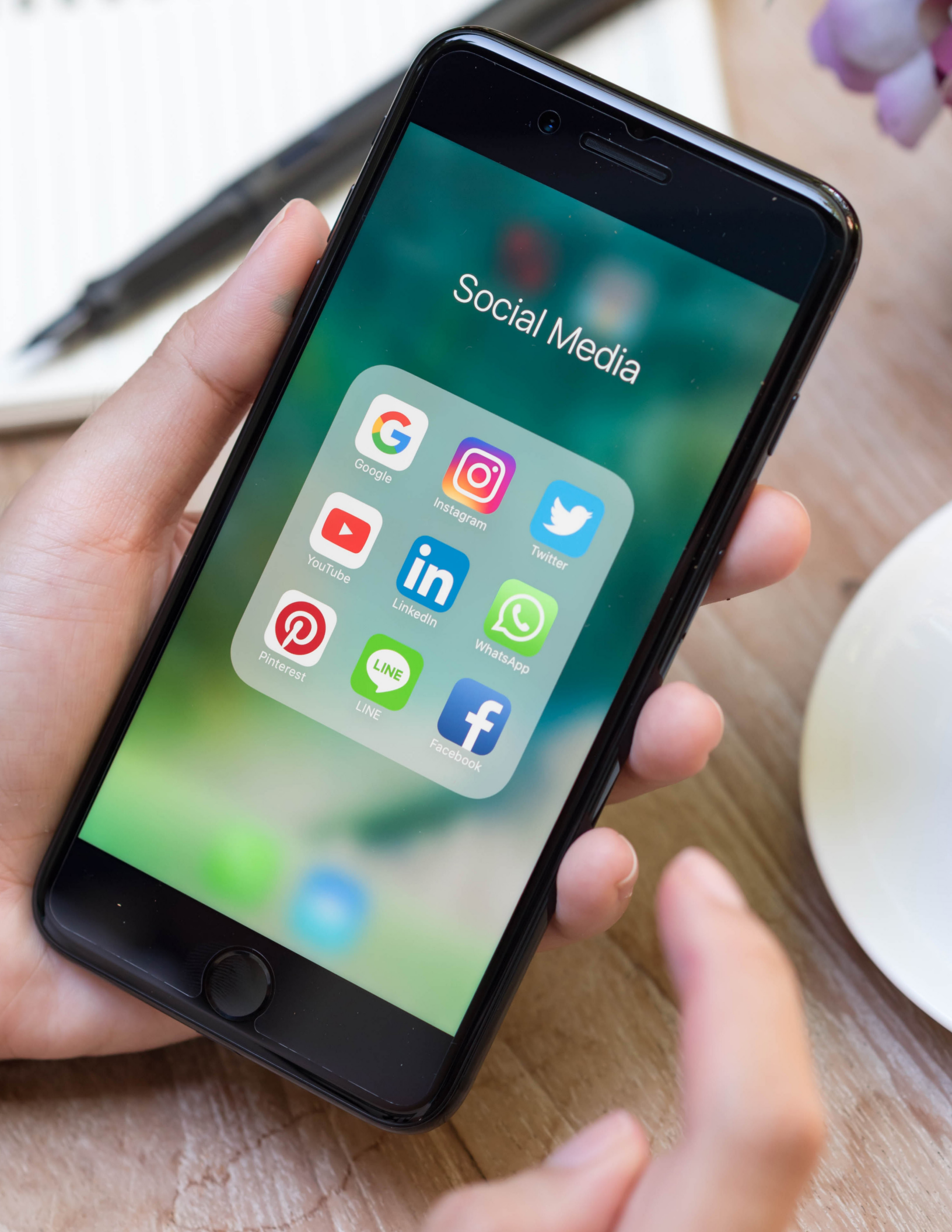
The Canada Elections Act[3] governs federal electoral matters regarding the election of MPs to the House of Commons. In December 2018, the Government of Canada passed the Elections Modernization Act (Bill C-76),[4] which makes significant and extensive changes to the Canada Elections Act. The revised legislation limits the election period to a maximum of 50 days following the issue of the writ of election, the formal order instructing each electoral district to hold an election on a set polling date (Marleau and Montpetit 2000, chap. 4).[5] Other key changes in Bill C-76 aimed at protecting the election process from foreign interference are set out in Part Three of this report.

2 *An Act to Amend the Canada Elections Act and other Acts and to make certain consequential amendments*, SC 2018, c 31, s 351(1) [*EMA*], amending *Canada Elections Act*, SC 2000, c 9, s 509(1) [*CEA*].

3 *CEA*, *supra* note 2.

4 *EMA*, *supra* note 2.

5 *EMA*, *supra* note 2, s 47, amending *CEA*, s 57(1.2)(c).


Social Media
Google
Instagram
Twitter
YouTube
LinkedIn
WhatsApp
Pinterest
LINE
LINE
Facebook

Part Two: Threats to Canada's Democratic Process

The biggest threat of foreign interference in Canada's upcoming federal election is through cyber activities aimed at key aspects of the democratic process. In the past few years, disinformation campaigns propagated online surrounding politicians and policy issues have been used to discredit leaders, undermine trust and sow discord among Canadians. Foreign influence exerted through other non-cyber means, such as third-party funding or direct interference, may also play a limited disruptive role.

Cyber Threats Targeting the Democratic Process

The CSE identified three areas that cyber activity may target: elections; political parties and politicians; and voters (CSE 2019, 13). Foreign adversaries have invested in cyber capabilities to pursue their strategic objectives, using cyber tools as an inexpensive way to influence domestic processes while maintaining plausible deniability (ibid., 10).

Elections

The election itself can be targeted by cyber capabilities that steal voter information, suppress voter turnout or tamper with the election agency's website (ibid., 19). In Canada, the paper-based ballot system has a lower threat level because the physical ballots are immune to cyber attacks; therefore, political parties, politicians and, in particular, voters are more vulnerable to cyber threats than is the ballot box itself (ibid., 17). However, aspects of the election process carried out electronically, including the storing of national voter registries and the electronic dissemination of election results, are vulnerable to attack (MacLellan 2018).

Politicians and Political Parties

Cyber attacks may target politicians and political parties to coerce, manipulate and publicly discredit individuals (CSE 2019, 18). Adversaries may use private information about a candidate or the candidate's staff to gain control over that individual (ibid.). Party and voter lists stored digitally can be obtained and the information sold or used to manipulate voter turnout, such as by sending voters to the wrong polling station (ibid., 18-19; Kolga 2019, 39). Party information, including emails, can be hacked and leaked to the public to damage the party or the candidate's reputation (Kolga 2019, 39). Over time, these threats could have a "chilling effect," in that the potential good of running for public office becomes outweighed by the risks of running to a candidate's privacy and personal life (CSE 2019, 11).

Voters

Most Canadians get their news and information online, from traditional media outlets and through social media accounts; they also participate in political discussions through online platforms (CSE 2017, 20; 2019, 9, 18). Actors with cyber capabilities can target these media to spread disinformation in the attempt to shape voters' opinions and undermine social cohesion (ibid., 5; Kolga 2019, 37). Online information can be manipulated to influence voter behaviour; this process of manipulation weakens trust in the democratic process and in the accuracy of the information people receive (CSE 2019, 11, 13, 18; MacLellan 2018). Further, disinformation can create confusion and divert attention away from campaign issues (MacLellan 2018).

Foreign Influence through Disinformation Campaigns

The most pervasive concern in the 2019 Canadian federal election will likely be disinformation campaigns that undermine social cohesion by amplifying extremist narratives and discrediting leaders (*The House* 2019b; Kolga 2019, 12).

Evidence suggests that Canada's adversaries use troll accounts to polarize debate in Canada on contentious policy issues (Bradshaw 2018, 7). A 2018 study by the Canadian Broadcasting Corporation (CBC) of Twitter accounts that were deleted after they were discovered to be connected to the Russian-based Internet Research Agency found that 8,000 of the three million tweets were related to Canadian issues, such as the Fort McMurray wildfire, the Quebec City mosque shooting, increased border crossings by asylum seekers and the Keystone XL pipeline (Rocha 2018; see also CSE 2018b, 15). A closer look at these Twitter accounts revealed that the majority of

the shared content was linked to Russian state media and extremist left and right conspiracy sites, demonstrating the strategic objective of "driving wedges between people" (Kolga 2019, 12).

In 2019, the CBC released another report about 9.6 million tweets from deleted accounts that were linked to suspected foreign influence campaigns originating in Russia, Iran and Venezuela. Of these, 21,600 tweets directly targeted Canadians on "hot-button" issues such as pipelines and immigration policies (Rocha and Yates 2019). In most cases, the tweet was copied from a legitimate account and amplified by a troll network to intensify coverage of extremist views on contentious issues (ibid.). Further, Russian state media channels that promote anti-democratic views are available in Canada (Kolga 2019, 20-21).

Recent disinformation campaigns targeting Canadian foreign policy and politicians highlight how fake news can be used to manipulate public opinion. The Canadian Armed Forces in Latvia have been targeted by local Russian-controlled media to turn public opinion against the NATO mission in the country (ibid., 15); examples of disinformation include stories that reported Canadian soldiers being housed in luxury accommodations at taxpayer expense and suggested that the former colonel and convicted serial killer Russell Williams still commanded Canada's air base there (Blackwell 2017).

The 2017 media frenzy reporting that Foreign Affairs Minister Chrystia Freeland's grandfather was involved in the Nazi regime occupying Poland was largely identified as a Russian disinformation campaign (Kolga 2019, 16-17).

In 2018, fake news stories involving New Democratic Party (NDP) leader Jagmeet Singh emerged ahead of his by-election. An ad claiming Singh was linked to Sikh militants and wanted for terrorism in 15 countries was shared more than 5,700 times before it was removed (Tunney 2019).

Another ad depicted Singh reportedly showing off a $5.5 million mansion, which runs counter to the NDP's affordable housing policy (ibid.). The ads were quickly identified as fake, but their source remains unclear (Harris 2019); the NDP has asked the Commissioner to investigate the ads (Tunney 2019).

Non-cyber Threats through Indirect and Direct Interference

While cyber threats are the most prominent concern for Canada's democratic process, foreign influence can also be exerted through other indirect and direct mechanisms. Third-party funding and covert action by foreign actors on Canadian soil could affect the election, although the extent of these threats may be limited.

Third-party funding from foreign sources to political advocacy groups in Canada was a major concern in the 2015 federal election. Canada Decides, a corporation set up by three Conservative candidates who lost in their ridings, filed a complaint with Elections Canada regarding foreign interference. Canada Decides alleged that foreign money was funnelled to Canadian advocacy groups, bypassing spending limits and thus influencing the election outcome (*National Post* 2017; Oliver 2017). In total, 114 third parties were registered in the 2015 election and spent $6 million; many of these third parties were funded through US-based companies (*National Post* 2017; Oliver 2017). The complaint focused on Leadnow, an organization substantially funded and launched by an American organization,[6] and alleged that foreign money helped fund its large "Vote Together" campaign to successfully defeat Conservative candidates in over 20 ridings (*National Post* 2017).

The previous legislation did not prohibit third parties from using foreign funds for campaign activities, did not regulate foreign funds received before the writ period and only capped third-party spending related to disseminating election advertising (Oliver 2017). Foreign contributions to third parties were therefore legal, if undesirable.

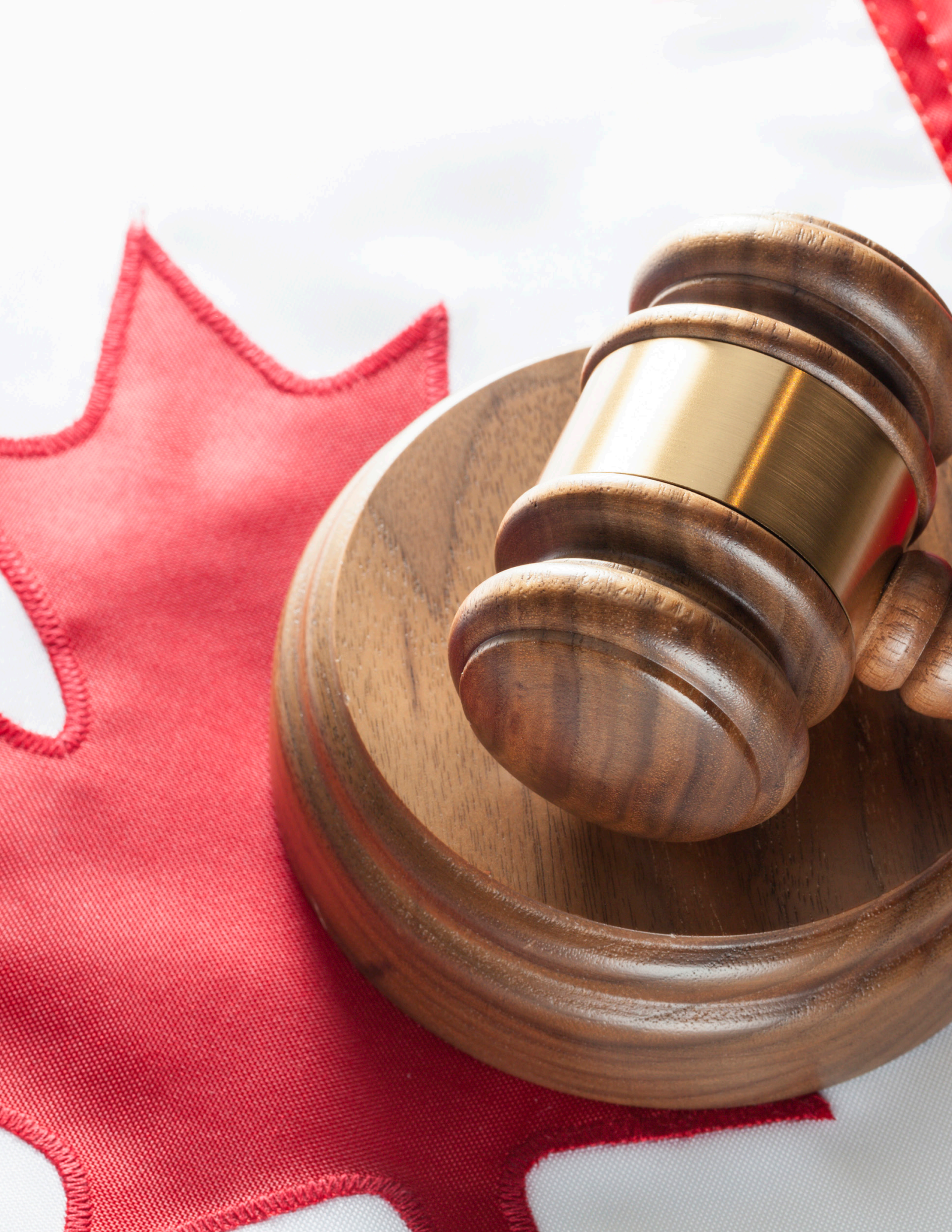
In 2017, the report of the Standing Senate Committee on Legal and Constitutional Affairs (2017, 4), *Controlling Foreign Influence in Canadian Elections*, recognized the legislation did not sufficiently protect elections from foreign interference by allowing foreign parties to make unlimited and unregulated contributions to third parties if outside an election period and not used for election advertising. The report recommended, *inter alia*, legislative changes to

6 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Evidence*, 42nd Parl, 1st Sess, No 120 (16 October 2018) at 1130 (Vivian Krause) (Vice-Chair Nathaniel Erskine-Smith).

ensure foreign funding does not play a role, direct or indirect, in Canadian elections (ibid., 1).

The new legislation, as detailed in Part Three of this report, now imposes strict conditions on third parties and prohibits foreign contributions. Therefore, foreign influence through third-party funding is unlikely to be a major concern in the 2019 federal election.

In early 2018, Canada expelled four Russian diplomats and denied applications for three additional diplomatic staff. Foreign Affairs Minister Freeland stated the four diplomats were "intelligence officers or individuals who have used their diplomatic status to undermine Canada's security or *interfere in our democracy*" (Global Affairs Canada 2018; see also Kolga 2019, 28; Gollom 2018). National Defence Minister Sajjan declined to answer whether and how the diplomats were involved in the 2015 elections (*Power & Politics* 2018). It is unclear the extent to which covert action is a concern for the upcoming election.



Part Three: Protective Measures Canada Is Taking

Canada is proactively taking protective measures ahead of the 2019 federal election to safeguard its democratic process from foreign interference. As discussed above, the government overhauled Canada's election legislation to strengthen existing protections and include new provisions aimed at preventing foreign influence. An interdepartmental plan to defend Canada's election against threats has been unveiled, integrating cyber security strategies and implementing public information campaigns.

Legislative Improvements

The Elections Modernization Act (Bill C-76) was introduced by the minister of democratic institutions on April 30, 2018. It received royal assent on December 13, 2018, and will enter into force on June 13, 2019. The Act strengthens Canada's resilience against foreign interference and cyber threats to its elections through provisions that prohibit the use of foreign funds, clarify offences related to false statements and require online platforms to publish a registry of online advertising. Other provisions include expanding the CEO's education mandate, requiring political parties to publish their policies to protect personal information and strengthening the Commissioner's investigative powers.

Use of Foreign Funds

Bill C-76 prohibits third parties from using funds from a foreign entity for partisan advertising and activities.[7] Foreign entities are defined to include individuals who are non-citizens or permanent residents; corporations outside Canada; trade unions outside Canada; a foreign political party; or a foreign government or agent of one.[8] It also prohibits foreign third parties from spending on partisan advertising and activities during the pre-election and election periods.[9] Previously, the Canada Elections Act permitted foreign third parties to spend up to $500 for advertising in an election.[10] The Act adds a new offence: third parties are now prohibited from using foreign contributions.[11]

In June 2018, Conservative MP Blaine Calkins introduced Bill C-406, a private member's bill, to address foreign contributions. This bill would amend the Canada Elections Act to prohibit third parties from using foreign contributions for election advertising purposes. However, its main objective has been substantially included in Bill C-76, and provisions that would extraterritorially legislate foreign entities would be difficult to enforce.[12]

Publishing False Statements

The provision governing false statements was significantly amended to clarify when and to whom or what the prohibition applies. The Elections Modernization Act prohibits a person or entity from making or publishing a false statement during the election period with the intention of affecting the election results.[13] It expands the individuals protected from candidates and prospective candidates to include leaders of public parties or public figures associated with political parties. The kinds of statements that are prohibited are limited to those falsely stating that a protected political person has committed an offence or is being charged or investigated for an offence, and false statements about a protected political person's citizenship, place of birth, education, professional qualifications or membership in a group or association.[14] The Act clarifies that the prohibition applies regardless of where the false statement is published or made[15] and makes it an offence for a person or an entity to publish a false statement or to impersonate a politician.[16]

Online Platforms

The Elections Modernization Act requires large online platforms that sell advertising space, directly or indirectly, to publish a registry of the person or group's advertising; this requirement applies to partisan advertising published during the pre-election period and election advertising published

7 *EMA*, *supra* note 2, s 223, amending *CEA*, s 349.02.

8 *Ibid*, amending *CEA*, s 349.01(1).

9 *Ibid*, s 223, 225, amending *CEA*, s 349.4(1)), s 351.1(1).

10 *CEA*, *supra* note 2, s 351.1.

11 *EMA*, *supra* note 2, s 336, amending *CEA* s 495.21(1)(a).

12 *House of Commons Debates*, 42nd Parl, 1st Sess, No 384 (21 February 2019) at 1750 (Arif Virani), 1755 (Hélène Laverdière).

13 *EMA*, *supra* note 2, s 61, replacing *CEA*, s 91(1).

14 *Ibid*.

15 *Ibid*, replacing *CEA* s 91(2).

16 *Ibid*, s 327, amending *CEA*, s 486(3).

during the election period.[17] The registry must include a copy of the advertisement and the name of the person who authorized the message,[18] and the person or group requesting the advertisement to be published must provide this information.[19] This information is to be published and made available to the public for a period of two years after publishing a partisan message, or two years after the end of the election period for an election message, and kept by the platform for five years.[20] The Act makes it an offence for online platforms to fail to publish the registry or maintain the necessary information for the required time, whether knowingly or not.[21]

Canada is one of the first countries to require major online platforms to maintain a publicly accessible registry of partisan and election advertising (Democratic Institutions 2019b). This is an important first step in increasing ad transparency, but the information available is extremely limited; the registry has been criticized for not going far enough to permit a user to determine why he or she was targeted (Hirsh 2018).

Other Provisions

The Elections Modernization Act expands the CEO's public education and information programs to the public at large, rather than just to students at the primary and secondary levels.[22] The CEO may use any media or other appropriate means and may establish programs to disseminate information outside Canada.[23] Public information campaigns are a key element of the Government of Canada's plan to safeguard the 2019 federal election, and this change reflects the reasoning that education should not be restricted because the risks posed by disinformation are not restricted to a single demographic.

The Act also requires political parties to publish their policies for protecting personal information on their websites.[24] This provision is an important step in the right direction, in particular as political parties are not subject to data privacy protections under the Personal Information Protection and Electronic Documents Act, which only applies to commercial activities, or the Privacy Act, which only applies to federal public sector activities (Canadian Bar Association 2018, 1). However, more could be done to limit the use of personal data in line with global norms, such as mandatory disclosure requirements when data privacy is breached (ibid., 2–5). With the increasing use of microtargeting in campaigns, greater legislative protections are desirable (see, for example, United Kingdom 2019, chap. 5).

Finally, the Elections Modernization Act adds additional offences related to protecting the election from foreign interference and expands the Commissioner's powers. The Act prohibits foreign persons or entities from unduly influencing an elector.[25] It also protects against the unauthorized use of a computer by prohibiting persons or entities from fraudulently, and with the intention of affecting election results, engaging in certain activities, such as altering or destroying data.[26] The Commissioner is permitted to apply for a court order to compel testimony,[27] to pursue administrative enforcement (i.e., monetary penalties)[28] and to initiate prosecutions if there are reasonable grounds to believe an offence has been committed.[29] These changes indicate the government's intent to give the Commissioner stronger powers to investigate and enforce the Act (Welch 2019).

Canada's Plan to Safeguard the 2019 Federal Election

On January 30, 2019, Minister of Democratic Institutions Gould, Minister of National Defence Sajjan and Minister of Public Safety and Emergency Preparedness Ralph Goodale announced the federal government's plan to defend Canada's elections and democratic institutions against threats. The plan focuses on four pillars: enhancing citizen preparedness; improving organizational readiness; combatting foreign interference; and expecting social media platforms to act.

17 *Ibid*, s 208.1, amending *CEA*, s 325.1 [limited to major online platforms that meet threshold criteria regarding the number of times the site was visited or used per month].

18 *Ibid*, amending *CEA*, s 325.1(3).

19 *Ibid*, amending *CEA*, s 325.2.

20 *Ibid*, amending *CEA*, s 325.1(4)-(5).

21 *Ibid*, s 333(1), replacing *CEA*, s 495(1)(b), s 495(4)(a).

22 *EMA*, *supra* note 2, s 14, replacing *CEA*, s 18.

23 *Ibid*.

24 *Ibid*, s 254, amending *CEA*, s 385(2)(k).

25 *EMA*, *supra* note 2, s 190, amending *CEA*, s 282.4.

26 *Ibid*, s 323, replacing *CEA*, s 482(1).

27 *Ibid*, s 357, amending *CEA*, s 510.01.

28 *Ibid*, s 350, amending *CEA*, s 508.

29 *Ibid*, s 360, replacing *CEA*, s 511.

Enhancing Citizen Preparedness

This pillar focuses on cultivating "an engaged and informed public" as the best defence against cyber threats. Three main activities will be carried out under this pillar to inform the public of identified threats, to educate the public on how to detect threats and to increase awareness to protect against threats (Democratic Institutions 2019e).

First, the Critical Election Incident Public Protocol (the "Protocol") will set out a process to inform Canadians of a serious threat to the integrity of the 2019 federal election. The Protocol will be implemented by a five-member "Panel" of senior public servants:

- the clerk of the Privy Council;
- the national security and intelligence adviser;
- the deputy minister of justice and deputy attorney general;
- the deputy minister of public safety; and
- the deputy minister of Global Affairs Canada.

The Protocol's mandate is limited to threats that occur within the writ period and do not fall within the scope of administering the election, which is within Elections Canada's responsibility. The Panel will only intervene when a high threshold is met that threatens the integrity of the election. If the threshold is met, all party leaders will be informed at the same time (*Power & Politics* 2019) and a press conference will be subsequently held to notify Canadians of the attack and how to protect themselves; the Panel will not address attribution or include classified information. The Panel's decision to notify Canadians cannot be vetoed by the prime minister (Democratic Institutions 2019f).

It is unclear what will meet this high threshold; Minister Gould has stated that the determination will be made after a contextual analysis, but she recently pointed to international examples, such as the Macron leaks, to illustrate events that could constitute such a threat.[30] An unnamed official said such incidents may include national-scale attacks such as "hacked or leaked party emails, viral deep-fake videos, or calculated disinformation campaigns" (Pinkerton 2019).

The Panel was modelled after actions taken by other countries, including France, the United States and the United Kingdom (*The House* 2019a; *Power & Politics* 2019). Minister Gould consulted with political parties to develop the Protocol and process, although it is unclear the extent to which their contributions were included.

Some have criticized the Protocol for not including the CEO or the Commissioner in the Panel.[31] Critics point out that the CEO is responsible for elections and so should be involved in election-related concerns; further, the CEO is appointed by Parliament, not by the government like the other Panel members, so the CEO's involvement could reduce any partisan concerns (*The House* 2019b; *Power & Politics* 2019). Minister Gould explained their exclusion by referring to the CEO's and the Commissioner's mandates, which are focused on, respectively, administering the election and ensuring compliance with the Elections Act, while foreign interference, as an attack on Canada, is a matter of national security that goes beyond elections (*The House* 2019a). There have also been reports that Elections Canada did not want to join the Panel for fear of compromising its independence.

Second, the Digital Citizen Initiative will support programming aimed at digital, civic and media literacy to inform and engage the public. The Government of Canada announced $7.5 million in funding for this initiative over two years to the Department of Canadian Heritage, starting in 2018-2019 (Department of Finance 2019, 180). The initiative will help Canadians to critically assess online reporting; to recognize how and when malicious actors exploit online platforms; and to learn how to reduce their own susceptibility to online manipulation (Canadian Heritage 2019).

These activities will reportedly engage youth and adults, but it is unclear how they will be carried out. Reaching older adults should be included, if not prioritized, as disinformation is often shared by this demographic (Momani 2019). The 2019 federal budget also proposed $19.4 million over four years to launch a Digital Democracy Project to research and develop guiding principles on online disinformation (Department of Finance 2019, 180), but as yet no further details have been released.

Third, existing public awareness campaigns will be leveraged and updated. The Get Cyber Safe national campaign on internet security and protective

30 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Evidence*, 42nd Parl, 1st Sess, No 138 (26 February 2019) at 1545 (Hon Karina Gould) (Chair: Bob Zimmer).

31 See e.g. *ibid* at 1555 (Hon Peter Kent).

strategies will be updated to include stronger linkages to cyber threats aimed at Canada's democratic process. The CSE published the *Cyber Threats to Canada's Democratic Process* report in 2017 and recently released an updated version (CSE 2019). This report, the first of its kind, alerts Canadians to potential cyber threats, with the updated version made available ahead of the 2019 federal election (Democratic Institutions 2019g).

Improving Organizational Readiness

This pillar focuses on improving the Government of Canada's ability to anticipate, identify and respond to emerging threats to our democratic process. This is carried out by providing advice and by sensitizing decision makers to threats, as well as through conducting security exercises to plan and respond to cyber attacks and disinformation campaigns (Democratic Institutions 2019d).

Political parties are a key area of concern. CEO Stéphane Perrault has expressed his concern about parties' abilities to protect themselves from cyber threats, noting, "They don't have access to the resources we have access to" (von Scheel and Tunney 2019; Bryden 2019). The CSE is providing technical advice and guidance to political parties (von Scheel and Tunney 2019). The leader of each major party and three of their staff will have security clearance to receive classified threat briefings to "promote situational awareness and help them strengthen internal security practices and behaviours" (*Power & Politics* 2019). The parties have already been receiving threat briefings in the lead-up to the election (von Scheel and Tunney 2019). Improving political parties' awareness of how to identify threats and protect against them will be critical, in particular given the vulnerabilities inherent in large-scale campaigns involving many people with limited resources. Elections Canada has also rebuilt its technology infrastructure with sophisticated security enhancements, following the CSE's advice (Bryden 2019).

Combatting Foreign Interference

This pillar focuses on engaging Canada's security and intelligence organizations as the front-line responders to foreign interference in the democratic process. The Government of Canada is creating a new Security and Intelligence Threats to Elections (SITE) Task Force and an investigative team led by the Royal Canadian Mounted Police (RCMP), as well as leveraging recent commitments, including the G7 Rapid Response Mechanism and the Canadian Centre for Cyber Security (the "Cyber Centre") (Democratic Institutions 2019a).

The SITE Task Force brings together the Canadian Security Intelligence Service (CSIS), the RCMP, the CSE and Global Affairs Canada to identify and counter activities that interfere with or influence Canadian elections. The task force will develop its awareness of threats and prepare the government to assess and respond to them (ibid.).

By gathering intelligence through a coordinated effort, it will be easier to respond to potential and new threats even in the final days or hours before the election.[32] A Foreign Actor Interference Investigative Team will be formed within the RCMP to investigate and disrupt foreign interference in Canada's election (Democratic Institutions 2019a). The CSE, CSIS and Elections Canada are conducting simulations to identify potential areas of vulnerability (Pinkerton 2019).

Canada is the international lead on the G7 Rapid Response Mechanism, announced at the Charlevoix Summit in June 2018. The mechanism is intended to coordinate, identify and respond to evolving threats to democracy. Canada is playing a coordination and leadership role through the Coordination Unit housed within Global Affairs Canada, which will act as a focal point for all G7 partners. The Coordination Unit will prepare threat analyses, share information and identify opportunities for joint international responses (Democratic Institutions 2019a; 2019c). The 2019 federal budget announced $2.1 million in funding over three years to support the mechanism (Department of Finance 2019, 180).

Through this leadership position, Canada is demonstrating its commitment to defending democracy from foreign interference and sharing best practices. With the rising global trend in cyber threats against democratic institutions, a coordinated, multinational response is an important step in the right direction.

The Cyber Centre is a key element of Canada's strategy to protect against cyber threats. The Government of Canada's National Cyber Security Strategy, first released in 2010, was updated in 2018 to reflect technological innovations and address gaps in the current cyber security environment (Public Safety Canada 2018). The updated strategy established the Cyber Centre to consolidate the

32 *Ibid* at 1700 (Dan Rogers).

cyber security functions and specialized expertise of approximately 750 employees from the CSE, Public Safety Canada and Shared Services Canada (CSE 2018a). It will enable fast, coordinated and focused government responses to cyber threats; allow timely and effective information flow between the government and private sector partners; and enhance public awareness and education about cyber security (Public Safety and Emergency Preparedness Canada 2018). The Cyber Centre, housed in the CSE, began its initial operations on October 1, 2018. The new facility is anticipated to open in the summer of 2019 and to be fully operational by spring 2020.

Canada's financial contributions to cyber security demonstrate its commitment to improving its capabilities and infrastructure. The 2018 federal budget announced $507.7 million in funding over five years and $108.8 million per year thereafter to fund the National Cyber Security Strategy, representing the largest single investment the Canadian government has ever made in cyber security; this commitment includes $155.2 million over five years and $44.5 million per year ongoing to establish the Cyber Centre (CSE 2018b, 11; Department of Finance 2018, 203). The 2019 federal budget announced additional funding of up to $4.2 million over three years to provide cyber security advice and guidance to political parties and election administrators (Department of Finance 2019).

Expecting Social Media Platforms to Act

This pillar focuses on engaging with social media platforms to encourage them to implement measures that increase transparency and prevent disinformation from spreading. The Government of Canada is engaging with social media platforms and expects them to take concrete steps to safeguard elections in Canada and to implement tools used in other countries (Democratic Institutions 2019b).

The Government of Canada recognizes the important role that social media platforms play in the democratic process. Minister Gould's ongoing dialogue with companies such as Facebook, Twitter and Microsoft is essential to combat the spread of disinformation on their platforms (Thompson 2019; Pinkerton 2019). It is not clear if discussions have been initiated with other major companies, such as YouTube, whose platforms could be harnessed to spread fake news, deep-fake videos and other forms of disinformation (Bradshaw 2018, 10).

Social media companies are taking steps, removing fake content and fake users and responding to legislative requirements to increase ad transparency. For example, Twitter published data on fake news and accounts it removed as part of its transparency campaign to combat election interference (Rocha and Yates 2019). Facebook launched its Canadian Election Integrity Initiative in 2017 in direct response to the CSE's report, *Cyber Threats to Canada's Democratic Process*, and released its *Cyber Hygiene Guide* aimed at politicians and political parties to advance account security (Facebook n.d.).

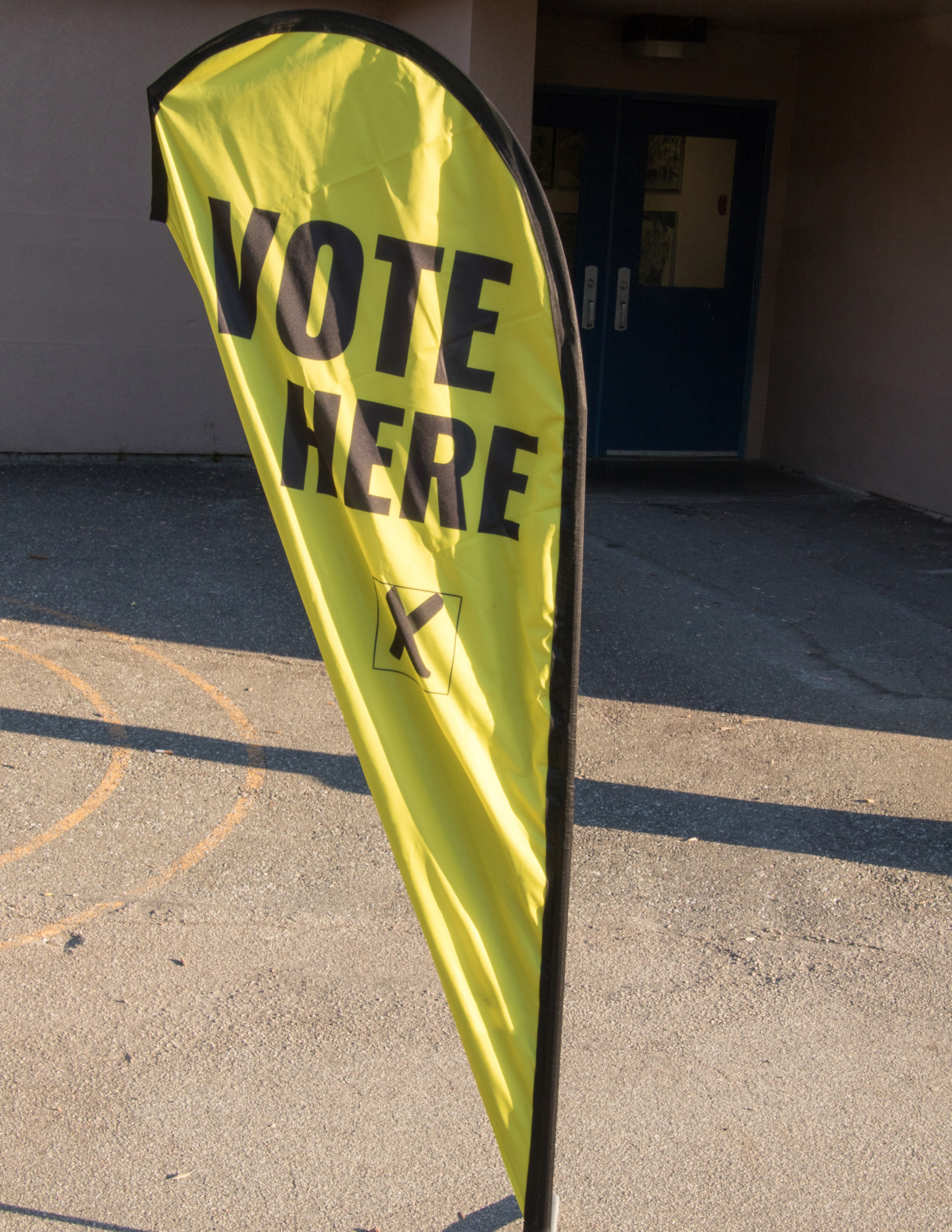
Despite these steps in the right direction, more can be done to require social media platforms to actively prevent the spread of disinformation. Political campaigning, after all, has evolved from paper brochures to social media posts, from broad messaging to targeted political ads. Social media and new technology have changed the potential scale, scope and precision of disinformation's distribution and consumption (Bradshaw 2018, 4). The revised legislation does require ad transparency, but there is little concrete action required of social media companies.

The Government of Canada has been criticized for simply "expecting" social media platforms to take concrete steps, without taking a firmer approach mandating legislative action to prevent disinformation.[33] Minister Gould has justified her approach by emphasizing that the government's role is not to police speech but to ensure Canadians have the tools and resources to make informed decisions, and that it is in the social media platforms' best interest to ensure Canadians can trust them (*The House* 2019a).

Recent comments suggest the Government of Canada may be considering whether to change its "nudge" approach and adopt a more directive policy by regulating social media. On February 26, 2019, Minister Gould appeared before the House of Commons' Standing Committee on Access to Information, Privacy and Ethics for a briefing on the SITE Task Force. Responding to a committee member's question about imposing a duty on platforms to quickly remove manifestly illegal content, Minister Gould stated: "I think we are moving in a direction where we need to *require* social media companies to act."[34]

33 See e.g. *ibid* at 1640 (Bob Zimmer).

34 *Ibid* at 1625 (Hon Karina Gould) [emphasis added].


VOTE
HERE

Part Four: Conclusion and Observations

It is evident from the foregoing that Canada is taking active measures ahead of the 2019 federal election to safeguard its democratic process from foreign interference. The Government of Canada has strengthened federal electoral legislation, developed an interdepartmental plan and invested in both cyber security infrastructure and public awareness campaigns.

Furthermore, Canada is taking a global leadership role as the lead for the G7 Rapid Response Mechanism, developing its capacity to assess threats and share best practices. Canada is, alongside the European Union, "leading the way in terms of protecting our democracy from foreign cyber-threats."[35]

Despite these positive and commendable steps, Canada's approach could be strengthened in two key areas to increase Canadians' trust in the democratic process and protect against vulnerabilities to foreign interference:

- First, the Panel could include the CEO or Commissioner, to fortify the confidence of Canadians in the process that decides whether the public should be informed of a threat during an election campaign.
- Second, more robust mechanisms should be implemented to require social media platforms to take steps to identify and remove disinformation.

As to the first of these points, the Protocol and the Panel are innovative mechanisms to determine when a threat impairs a free and fair election and to notify the public of that threat. However, the Panel's composition has generated concern, especially for not including the CEO or the Commissioner. The inclusion of one of these individuals could have the positive effect of deepening Canadians' confidence in the process.

This is particularly so given that Michael Wernick, until recently the clerk of the Privy Council (one of the five posts designated as Panel members), recently announced his resignation following suggestions that he had acted in a partisan manner in the recent SNC-Lavalin controversy (Platt 2019). Minister Gould is asking Canadians to "have confidence in both the message and the messenger" (*Power & Politics* 2019). Concerns about partisanship may diminish the public's trust that decisions to disclose threats will be made impartially. Canadians are being asked to trust the Panel's message if a threat is disclosed (*The House* 2019a), but they must also be able to trust in the Panel's silence when its members decide that a public announcement is not warranted.

Further, while these threats may be a national security concern, they are also inherently an election concern. There are strong arguments that the Panel should include representation by individuals mandated to administer, or to enforce, Canada's federal electoral legislation, which prohibits foreign interference in the electoral process.

As to the prospect of regulating social media, Canada has identified social media platforms as an integral component to safeguarding elections. But, instead of requiring concrete action, the government has merely expressed expectations. There is a strong argument that legislation should be introduced to regulate social media companies, requiring them to identify disinformation and respond in a timely manner.

There is some international precedent in this regard, with other countries taking a more robust approach to addressing the spread of fake news and disinformation. In January 2018, for example, Germany introduced new legislation, the Network Enforcement Act (NetzDG), requiring social media companies to remove fake news and hate speech from their platforms within 24 hours or face stiff fines (United Kingdom 2019, 12-13; *The House* 2019b). In France, legislation passed in November 2018 permits judges to order the removal of online materials, during an election campaign, that constitute disinformation.[36] The European Union's Code of Practice on Disinformation is also relevant in this regard (European Commission 2018).

35 *Ibid* at 1610 (Hon Karina Gould).

36 See www.gouvernement.fr/en/combating-the-manipulation-of-information; see also United Kingdom (2019, 13).

In Canada, even if disinformation is discovered, there is no guarantee that platforms will quickly remove it. For example, Facebook was alerted by a member of the House of Commons' Standing Committee on Access to Information, Privacy and Ethics about a false story regarding the Canadian military in Latvia but only removed the post a month later after it was prompted again to remove it.[37] Outside of the regulatory context, Europe openly monitors and publishes findings on pro-Kremlin disinformation on the "EU vs Disinfo" website, as part of the European Union's European External Action Service East Stratcom Task Force (EU vs Disinfo 2018; *The House* 2019b). A similar mechanism could be initiated in Canada to identify and alert citizens to smaller-scale disinformation that would not reach the Protocol's high threshold. A recent Canadian survey found that 70 percent of respondents were worried fake news could affect the 2019 election and that 57 percent admitted to believing fake news in the past (Thompson 2019). Increased regulation and transparency, complemented by digital literacy programs, could help Canadians to make informed decisions and trust the platforms they use to view content and engage in political debate.

The Government of Canada has made concerted efforts to invest in cyber security infrastructure and training to protect its systems from foreign influence. However, foreign interference through disinformation campaigns are aimed at civilians, deepening social divides and undermining the public's trust in its democratic institutions. As Canada prepares for the upcoming 2019 federal election, enhancing Canadians' trust in the election process and protecting against interference in democratic dialogue is clearly among the government's top priorities.

During its meeting in Ottawa on April 29, 2019, the TCEI engaged both senior government officials and Minister Gould about the regulation of social media platforms, exploring and discussing options and sharing best practices from other jurisdictions.

From the discussion, there emerged several observations that merit further consideration:

- Disinformation efforts are not new. During the Cold War, for example, both sides engaged in elaborate campaigns to persuade the other's population of a preferred version of reality. Attempts to "spin" or slant the facts have been a constant in the way governments deal with both current and historical events, seeking to influence how those events are perceived and understood.
- Indeed, some cable news television networks and radio talk shows today engage in concerted efforts to promote a certain perspective by presenting an interpretation of the news, or by focusing on some news events and not others.
- Regulating in order to limit social media content to what is "true" is a perilous task. To begin with, government is not an appropriate arbiter of what is true. It is a hallmark of the totalitarian state that government acts as a gatekeeper to determine what information will be published. Adopting such an approach in a democracy risks making things worse, rather than better.
- The very concept of "truth" can be elusive and difficult to determine:
  - If a true story is exaggerated or taken out of context, is it no longer true?
  - When someone posts on social media an *interpretation* of a true story, is that post false? Is it opinion rather than fact? How can one tell the difference?
  - For these and other reasons, regulating content on social media is fraught with difficulty, especially when government proposes to do the job.

That having been said, legislation from other countries provides models of how government can establish compulsory codes of behaviour for social media, by dictating standards that must be respected and imposing obligations on the platforms, which include monitoring content and removing offensive posts.

TCEI discussed in Ottawa some specific kinds of disinformation and manipulation that may potentially be controlled through government regulation. For example:

- Malign actors' exploitation of the public's trust by impersonating a figure known to the public as a credible person or authority and dishonestly putting words into that person's

37 *Ibid* at 1700 (Hon Peter Kent).

mouth; these so-called "sock puppets" are cleverly constructed and designed to deceive.

- Russians' or other interfering states' amplification of a false or malicious social media post by contriving to record a large number of "likes" or "re-tweets," leaving the untrue impression that the original post has broad popular support and thereby distorting the online conversation.

- The design and use of algorithms by social media proprietors such that when the user reads an entry posted by an extreme or "fringe" source the user is automatically driven to other similar posts, creating the false impression for the user that the extreme view is broadly shared and supported.

Members of the TCEI expressed the view that these forms of abuse and misconduct are examples of the kind of abuses capable of being regulated, by requiring the social media platforms themselves to monitor and eradicate them.

Commission members also expressed concern about "computational propaganda," by which data compiled and sold by social media is then used (as in the case of Cambridge Analytica) to target specific audiences with tailored messages. By imposing safeguards and limitations on the data that can be amassed and how the platforms can deal with it, such abuses may be controlled.

TCEI members also identified civil litigation as a potential tool in the effort by government and others to motivate social media platforms to respect their obligations to their users and to society at large. Class actions, individual lawsuits or litigation brought against them by government have the potential to modify the behaviour of the platforms, by exposing them to the risk that courts may award significant monetary damages.

Finally, TCEI members made a number of concluding observations.

First, coordination is key in defending against malign interference in a democracy's election. That means a "whole of government" approach is required in each country. (The Canadian model of the SITE Task Force provides a good example of interdepartmental coordination in government.)

However, coordination also means close cooperation between and among countries.

The vulnerabilities in question are common to all democracies. The only sensible approach is to go beyond mere information sharing among countries to developing common techniques employed by all and constantly upgrading them to take account of the increasing technological sophistication of the malign actors. This international collaboration is especially important for smaller countries (like Canada) who can benefit from the significant capacity of larger states.

Second, while international opinion surveys conducted by CIGI-Ipsos (2018) show that the public generally mistrusts social media, the platforms remain influential. Despite its misgivings, the public continues to use social media in increasing numbers. And, importantly, it is in those jurisdictions with the greatest regulation of social media (in Germany, with its NetzDG law, for example) that public trust in the platforms is greatest. It is apparent there is a public appetite for such regulation.

Third, the time has come for democracies under attack to call out their aggressors by name. There seems little need and no advantage to remain discreetly silent if an intelligence service has reliable information about which foreign country is the source of the interference. Calling out the attackers through public identification is one important way by which they can be held to account. Doing so would also assist the democratic state in efforts to persuade its citizens that the threats are real, and that they must be alert to falsity and distortions coming from abroad.

Finally, the Commission emphasized the importance of imposing major sanctions against social media companies that fail to meet standards established by democratic governments. Where it is determined that the platforms have allowed themselves to be used by a malign foreign actor or have permitted abuses they could have caught or controlled, they should face very stiff penalties. Where fines are imposed, they should be high enough to capture the attention even of those cash-rich corporations. Governments should also fashion innovative, non-monetary penalties that will entail business consequences of sufficient gravity that they will constitute a real deterrence and effective denunciation of the misconduct. Another option in designing effective penalties for the social media companies is to require their chief executive officers and members of senior management to certify in writing, signed personally

by each, that the companies have complied with all applicable regulations. If the penalties for falsely certifying included fines and possibly jail terms for those executives, they would no doubt take great care before certifying the truth of the declaration.

Acknowledgment

This report was submitted to TCEI by Allan Rock, TCEI member. The research and writing of Ashley Geerts, supported by Ariel Wheway, were essential to the preparation of this report. Both are J.D. candidates at the Faculty of Law, University of Ottawa. Allan Rock expresses his sincere appreciation for their excellent work.

Works Cited

Blackwell, Tom. 2017. "Russian fake-news campaigns against Canadian troops in Latvia includes propaganda about litter, luxury apartments." *National Post*, November 17. https://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments.

Bradshaw, Samantha. 2018. "Securing Canadian Election: Disinformation, Computational Propaganda, Targeted Advertising and What to Expect in 2019." *Canadian International Council* 66 (3).

Bryden, Joan. 2018. "Ottawa refusing to respond to question about Russian meddling in 2015 federal election." *The Globe and Mail*, November 22. www.theglobeandmail.com/canada/article-ottawa-refusing-to-respond-to-question-about-russian-meddling-in-201/.

———. 2019. "Chief electoral officer worries parties are a weak link in elections cybersecurity." *The Globe and Mail*, February 4. www.theglobeandmail.com/canada/article-chief-electoral-officer-worries-political-parties-are-a-weak-link-in/.

Canadian Bar Association. 2018. "Bill C-76: *Elections Modernization Act*." Ottawa, ON: Canadian Bar Association Privacy and Access Law Section.

Canadian Heritage. 2019. "Online Disinformation." Government of Canada website, February 5. www.canada.ca/en/canadian-heritage/services/online-disinformation.html.

CIGI-Ipsos. 2018. "2018 CIGI-Ipsos Global Survey on Internet Security and Trust." www.cigionline.org/internet-survey-2018.

CSE. 2017. *Cyber Threats to Canada's Democratic Process*. Ottawa, ON: Communications Security Establishment. https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-e.pdf.

———. 2018a. "Canadian Centre for Cyber Security." Government of Canada website, October 16. www.cse-cst.gc.ca/en/backgrounder-fiche-information.

———. 2018b. *Canadian Centre for Cyber Security National Cyber Threat Assessment 2018*. Ottawa, ON: Communications Security Establishment.

———. 2019. *2019 Update: Cyber Threats to Canada's Democratic Process*. Ottawa, ON: Communications Security Establishment. https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

Democratic Institutions. 2019a. "Combatting Foreign Interference." Government of Canada website, January 30. www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.html.

———. 2019b. "Expecting Social Media Platforms to Act." Government of Canada website, January 30. www.canada.ca/en/democratic-institutions/news/2019/01/encouraging-social-media-platforms-to-act.html.

———. 2019c. "G7 Rapid Response Mechanism." Government of Canada website, January 30. www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html.

———. 2019d. "Improving Organizational Readiness." Government of Canada website, January 30. www.canada.ca/en/democratic-institutions/news/2019/01/improving-organizational-readiness.html.

———. 2019e. "Enhancing Citizen Preparedness." Government of Canada website, February 5. www.canada.ca/en/democratic-institutions/news/2019/01/enhancing-citizen-preparedness.html.

———. 2019f. "Critical Election Incident Protocol." Government of Canada website, March 15. www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html.

———. 2019g. "The Government of Canada's Plan to Safeguard Canada's 2019 Election." Speech by the Hon. Harjit S. Sajjan. Government of Canada website, March 21. www.canada.ca/en/democratic-institutions/news/2019/03/speech-thegovernment-of-canadas-plan-to-safeguard-canadas-2019-election.html.

Department of Finance. 2018. *Equality and Growth: A Strong Middle Class [Budget 2018]*. Tabled in the House of Commons by the Hon. William Francis Morneau, PC, MP, Minister of Finance, February 27. Ottawa, ON: Department of Finance Canada. www.budget.gc.ca/2018/docs/plan/budget-2018-en.pdf.

———. 2019. *Investing in the Middle Class: Budget 2019*. Tabled in the House of Commons by the Hon. William Francis Morneau, PC, MP, Minister of Finance, March 19. Cat. No. F1-23/3E-PDF. Ottawa, ON: Department of Finance Canada. www.budget.gc.ca/2019/docs/plan/budget-2019-en.pdf.

Elections Canada. 2015. *The Electoral System of Canada. 4th ed*. Catalogue No SE1-5/1-2012E-PDF. Ottawa, ON: Elections Canada. www.elections.ca/res/ces/esoc_e.pdf.

EU vs Disinfo. 2018. "About." https://euvsdisinfo.eu/about/.

European Commission. 2018. "Digital Single Market — News — Code of Practice on Disinformation." European Commission website, September 26. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

Facebook. n.d. "Canadian Election Integrity Initiative." http://facebookcanadianelectionintegrityinitiative.com/.

Global Affairs Canada. 2018. "Canada expels Russian diplomats in solidarity with United Kingdom." Statement by the Hon. Chrystia Freeland, Minister of Foreign Affairs. Government of Canada website, March 26. www.canada.ca/en/global-affairs/news/2018/03/canada-expels-russian-diplomats-in-solidarity-with-united-kingdom.html.

Gollom, Mark. 2018. "Russian diplomats interfered in Canada's democracy, Ottawa says. Did they meddle in our election?" CBC News, March 31. www.cbc.ca/news/politics/russia-diplomats-expelled-canada-election-1.4599210.

Harris, Michael. 2019. "Since companies like Taboola and Facebook can't seem to control face news, the question is who can?" *The Hill Times*, February 11. www.hilltimes.com/2019/02/11/187738/187738.

Hirsh, Jesse. 2018. "Canadian Elections Can't Side-step Social Media Influence." Opinion, November 20. Waterloo, ON: CIGI. www.cigionline.org/articles/canadian-elections-cant-side-step-social-media-influence.

Humphreys, Adrian. 2015. "Anonymous leaks another high-level federal document as part of vendetta against government." *National Post*, September 26. https://nationalpost.com/news/canada/anonymous-leaks-another-high-level-federal-document-as-part-of-vendetta-against-government.

Kolga, Marcus. 2019. *Stemming the Virus: Understanding and responding to the threat of Russian disinformation*. Ottawa, ON: Macdonald-Laurier Institute. https://macdonaldlaurier.ca/files/pdf/20181211_MLI_Russian_Disinformation%20PAPER_FWeb.pdf.

Liberal Party of Canada. 2019. "Electoral Reform." www.liberal.ca/realchange/electoral-reform/.

Lithwick, Dara and Sebastian Spano. 2015. *The Canadian Electoral System*. Background paper, rev. October 22. Publication No. 2013-81-E. Ottawa, ON: Library of Parliament. https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201381E.

MacDonald, Michael and Keith Doucette. 2018. "Canadian federal election will be target for Russian interference, Sajjan says." CTV News, November 18. www.ctvnews.ca/politics/canadian-federal-election-will-be-target-for-russian-interference-sajjan-says-1.4182147.

MacLellan, Stephanie. 2018. "Canada's Voting System Isn't Immune to Interference." Opinion, November 5. Waterloo, ON: CIGI. www.cigionline.org/articles/canadas-voting-system-isnt-immune-interference.

Marleau, Robert and Camille Montpetit, eds. 2000. *House of Commons Procedure and Practice*. Online ed. Montreal, QC: Chenelière/McGraw-Hill. www.ourcommons.ca/MarleauMontpetit/DocumentViewer.aspx?DocId=1001&Sec=Ch001&Seq=0&Language=E.

Momani, Bessma. 2019. "Electoral integrity in Canada's 2019 federal election." Canada and the World podcast series, Episode 30. Open Canada, March 1. www.opencanada.org/features/canada-and-the-world-ep-30-electoral-integrity-in-canadas-2019-federal-election/.

National Post. 2017. "Millions in foreign funds spent in 2015 federal election to defeat Harper government, report alleges." *National Post*, May 23. https://nationalpost.com/news/politics/millions-in-foreign-funds-spent-in-2015-federal-election-to-defeat-harper-government-report-alleges.

Oliver, Joe. 2017. "Canada's elections are already being infiltrated by foreign interests and, shockingly, it's all legal." *Financial Post*, May 16. https://business.financialpost.com/opinion/joe-oliver-canadas-elections-are-already-being-infiltrated-by-foreign-interests-and-shockingly-its-all-legal.

Orol, Ronald. 2019. "Fake News Threatens Canada's Federal Election." Opinion, March 13. Waterloo, ON: CIGI. www.cigionline.org/articles/fake-news-threatens-canadas-federal-election.

Pinkerton, Charlie. 2019. "Government releases blueprint for protecting election from interference." *iPolitics*, January 30. https://ipolitics.ca/2019/01/30/government-releases-blueprint-for-protecting-election-from-interference/.

Platt, Brian. 2019. "Privy Council Clerk Michael Wernick resigns after controversy over SNC-Lavalin testimony." *National Post*, March 18. https://nationalpost.com/news/politics/privy-council-clerk-michael-wernick-resigns-after-controversy-over-snc-lavalin-testimony.

Power & Politics. 2018. "Did Russia Interfere in Canada's Last Election?" Interview of Harjit Sajjan. Video, 7:49 min. CBC Radio, March 26. www.cbc.ca/news/politics/did-russia-interfere-in-canada-s-last-election-1.4594243.

———. 2019. "It's important that this is above partisanship." Interview of Karina Gould. Video, 10:14 min. *Power & Politics*, January 30. www.cbc.ca/news/politics/powerandpolitics/it-s-important-that-this-is-above-partisanship-karina-gould-1.4999690.

Public Safety and Emergency Preparedness Canada. 2018. "UPDATE — New Cyber Security Strategy bolsters cyber safety, innovation and prosperity." Cision, July 13. www.newswire.ca/news-releases/update---new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity-688155151.html.

Public Safety Canada. 2018. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Cat. No. PS4-239/2018E. Ottawa, ON: Public Safety Canada. http://publications.gc.ca/site/eng/9.856424/publication.html.

Rocha, Roberto. 2018. "Data sheds light on how Russian Twitter trolls targeted Canadians." CBC News, August 3. www.cbc.ca/news/canada/russian-twitter-trolls-canada-targeted-1.4772397.

Rocha, Roberto and Jeff Yates. 2019. "Twitter trolls stoked debates about immigrants and pipelines in Canada, data show." CBC News, February 12. www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

Standing Senate Committee on Legal and Constitutional Affairs. 2017. *Controlling Foreign Influence in Canadian Elections: Report of the Standing Senate Committee on Legal and Constitutional Affairs*. June. Ottawa, ON: Senate of Canada. https://sencanada.ca/content/sen/committee/421/LCJC/reports/Election_Report_FINAL_e.pdf.

The House. 2019a. "Democracy in Danger (Interview — Minister Karina Gould)." Audio recording, 10:40 min. CBC Radio, January 31. www.cbc.ca/radio/thehouse/the-house-democracy-in-danger-and-battleground-b-c-1.4999337.

———. 2019b. "Democracy in Danger (Interview — Disinformation expert Marcus Kolga)." Audio recording, 7:00 min. CBC Radio, January 31. www.cbc.ca/radio/thehouse/the-house-democracy-in-danger-and-battleground-b-c-1.4999337.

Thompson, Elizabeth. 2019. "Minister tasked with safeguarding election calls on committee to look at regulating Facebook, Twitter." CBC News, February 19. www.cbc.ca/news/politics/gould-facebook-twitter-election-1.5024900.

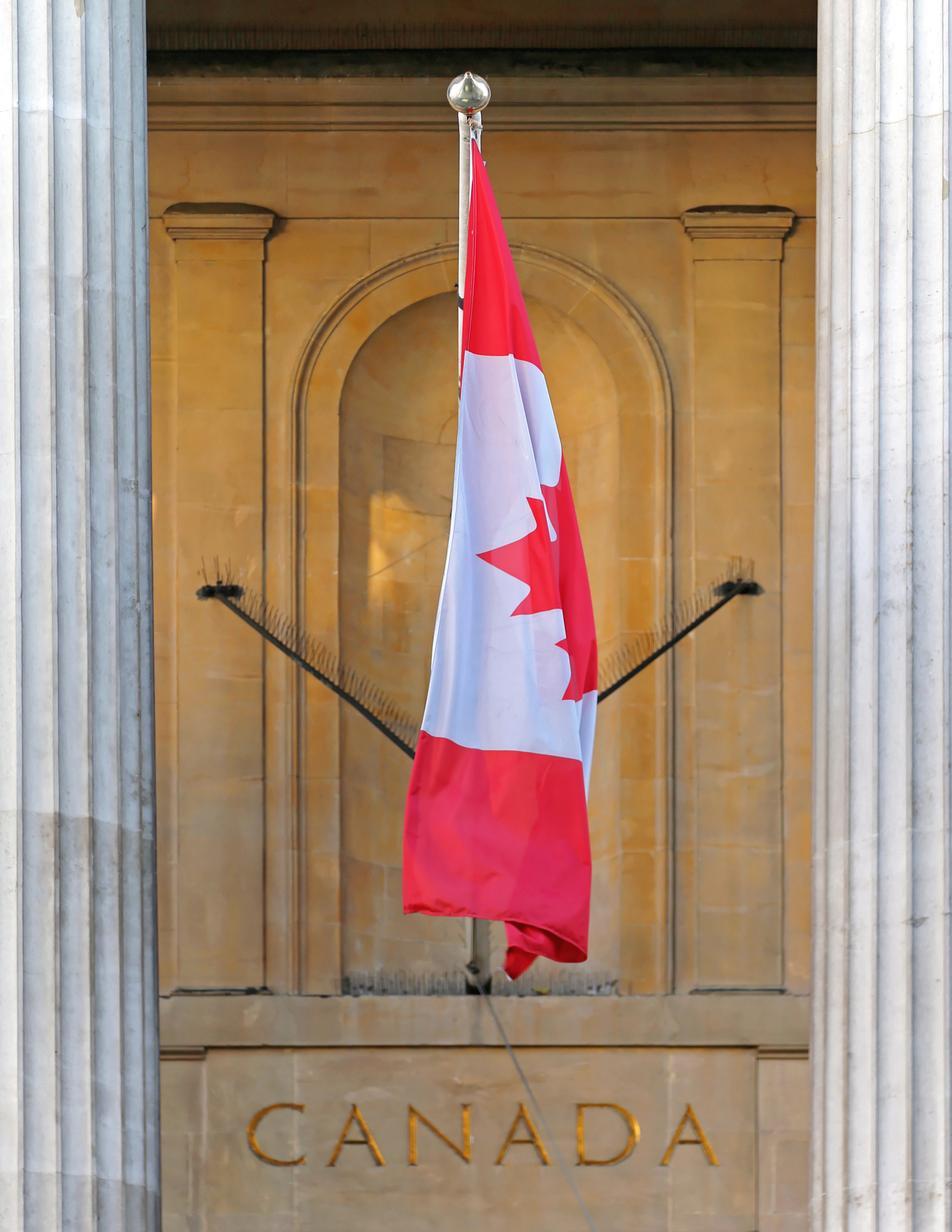
Tunney, Catharine. 2019. “NDP asks elections watchdog to investigate ‘slanderous’ ads targeting Singh.” CBC News, February 6. www.cbc.ca/news/politics/ndp-elections-canada-singh-1.5007989.

United Kingdom. 2019. House of Commons: Digital, Culture, Media and Sports Committee. *Disinformation and ‘fake news’: Final Report*. HC 1791, February 18. London, UK: House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

von Scheel, Elise. 2018. “A year later, Trudeau will only revisit electoral reform if pushed by other parties — something MPs don’t buy.” CBC News, February 1. www.cbc.ca/news/politics/trudeau-electoral-reform-january-2018-1.4511902.

von Scheel, Elise and Catharine Tunney. 2019. “Cyber security expert briefs parties on protecting themselves during election campaign.” CBC News, February 8. www.cbc.ca/news/politics/canada-security-cyber-threat-1.5010372.

Welch, Matthew. 2019. “Canada’s Federal Electoral Law Will Now Apply More Widely Than Ever, Including to Businesses and Advocacy Groups. Are You Ready?” Fasken Martineau DuMoulin LLP Political Law Bulletin, February 25. www.fasken.com/en/knowledge/2019/02/canadas-federal-election-law-will-now-apply-more-widely-than-ever.


CANADA

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and have received support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan doté d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques internationales, et le droit international. Nous comptons sur la collaboration de nombreux partenaires stratégiques et avons reçu le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

About the Alliance of Democracies Foundation

The Alliance of Democracies Foundation is a non-profit organization founded in 2017 by Anders Fogh Rasmussen, the former NATO Secretary General and former Prime Minister of Denmark. The Foundation is dedicated to the advancement of democracy and free markets across the globe and runs three programs: the Copenhagen Democracy Summit, the Expeditionary Economics program, and the Campaign for Democracy.

About the Transatlantic Commission on Election Integrity

As part of the Alliance of Democracies, the Transatlantic Commission on Election Integrity is a transatlantic, bi-partisan group of political, tech, business and media leaders that seeks to foster a more collective approach to preventing the next wave of foreign election interference. The Commission's work raises awareness of the risks, develops new technology tools, and identifies weaknesses and remedies in the policy response across Europe and the USA, including front-line states such as Ukraine.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline