A Macdonald-Laurier Institute Publication

RUSSIA-PROOFING YOUR ELECTION

Global lessons for protecting Canadian democracy against foreign interference

Marcus Kolga, Jakub Janda, Nathalie Vogel

MLI

July 2019

True North in
Canadian public policy

SIR JOHN A. MACDONALD

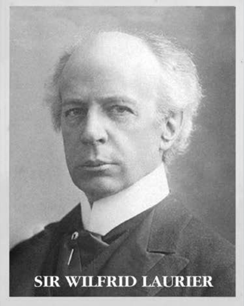

SIR WILFRID LAURIER

Table of contents

The authors of this document have worked independently and are solely responsible for the views presented here. The opinions are not necessarily those of the Macdonald-Laurier Institute, its Directors or Supporters.

Executive Summary

In the past decade, the Kremlin has spent significant resources to spread disinformation and disrupt the elections and decision-making processes of its perceived enemies, including in Europe and North America. Perhaps the most well-known attempt took place during the lead-up to the US presidential election in 2016. There have been a number of other occasions of suspected Russian electoral interference, including in the Netherlands' referendum on the EU-Ukraine trade deal in 2016, the UK's referendum on Brexit in 2016, and France's presidential election in 2017, among others.

For this reason, it seems prudent to expect an increase in Russian-directed and sponsored attacks in the near future, especially as the electorate in many countries in Europe and North America, including Canada and United States, are going to the polls over the next few years. Democracies around the world, including Canada's, will be in peril if countermeasures remain static. We must invest in countering Russian disinformation now to boost our immunity and resilience against it.

We must invest in countering Russian disinformation now to boost our immunity and resilience against it.

This report draws upon the experiences of other Western states that have faced active threats from Russian disinformation and the disruption of their democratic processes. Using the insights from these case studies – including Sweden, the three Baltic states, France, and Germany – the report outlines tools that Canada can use to protect its elections and the democratic processes that underpin them.

In the upcoming 2019 federal election, Canadians should expect that narratives that threaten to divide Canadians on both the right and left – such as those that promote anti-immigration, anti-globalism, and anti-pipeline – will intensify. The Kremlin is not the exclusive source of threat; Iran and China have also been identified as threats. Regardless of the regime, proxy groups that are organized to sow mischief and promote pro-regime positions represent a serious threat to our democratic processes.

Fortunately, Canadian authorities are well aware of the threat posed by Russian disinformation. The Canadian Security Establishment confirmed that the 2015 election was targeted by digital foreign interference. And Ottawa announced several major initiatives to counter foreign disinformation in January 2019. Many of these measures can be commended. Indeed, former Estonian President Toomas Hendrik Ilves, who is also a commissioner with the Transatlantic Commission for Election Integrity, has stated that Canada is in many ways leading the effort to address foreign disinformation. Yet, as he himself has acknowledged, when it comes to Canada's efforts, we are "still not doing enough," underscoring the depth of the challenge.

With that in mind, the report outlines a number of measures that Canadian authorities can take to protect ourselves from foreign interference. These include:

- Government should work with social media companies to adopt appropriate policies that will help to assure trust among users and the general public in the role of these increasingly important platforms.
- Domestic political parties need to develop and deploy robust security protocols to protect supporter data.
- CRTC policies and regulations should be updated to hold foreign cable news licence holders accountable for propaganda and false news that are broadcast by channels to which they hold licences.
- Canada should communicate to potential adversaries that major attacks against our strategic assets, including our media and our democratic processes, could trigger a commensurate response under NATO's Article 5.
- Canada should join and actively participate in NATO's Centers of Excellence (COE), especially those in the Baltic states.
- The federal government should fully implement Bill C-59, giving Canadian security agencies the means to actively defend against digital interference by having the capability to strike back against attackers.

Ultimately, a well informed and educated public, media, and government will provide the most resilient form of defence against foreign malign influence and disinformation campaigns. The public should be given the necessary tools to enhance their ability to consume media with a critical eye, to check facts, and question the platforms that promote and amplify foreign disinformation and false narratives that are aimed at manipulating our views and undermining the stability of our democracy and society.

Sommaire

Depuis dix ans, le Kremlin déploie des efforts considérables pour répandre de la désinformation et perturber le déroulement des élections et les processus décisionnels de ses ennemis présumés, notamment en Europe et en Amérique du Nord. Les opérations qui ont sans doute attiré le plus d'attention se sont déroulées peu avant l'élection présidentielle américaine, en 2016. Il y a aussi eu certains autres cas présumés d'ingérence électorale russe, notamment lors du référendum néerlandais sur l'accord commercial entre l'UE et l'Ukraine en 2016, du référendum britannique sur le Brexit en 2016 et de l'élection présidentielle française en 2017.

> *Nous devons investir dès maintenant pour faire obstacle plus efficacement aux tentatives de désinformation russes.*

Il semble donc prudent de s'attendre à une augmentation prochaine des attaques dirigées et commanditées par la Russie, d'autant plus que l'électorat de nombreux pays européens et nordaméricains, y compris du Canada et des États-Unis, se rendra aux urnes au cours des prochaines années. Les démocraties du monde entier, y compris la nôtre, pourraient être mises à mal si les contre-mesures n'évoluent pas. Nous devons investir dès maintenant pour faire obstacle plus efficacement aux tentatives de désinformation russes.

Ce rapport s'appuie sur les expériences d'autres États occidentaux qui ont eu à conjurer des menaces réelles de désinformation et de manipulation des processus démocratiques orchestrées par la Russie. Tirant parti de ces leçons apprises – par exemple, en Suède, dans les trois États baltes, en France et en Allemagne –, le rapport décrit les outils à la disposition du Canada pour protéger ses élections et les processus démocratiques qui les sous-tendent.

Lors de la prochaine élection fédérale en 2019, les Canadiens doivent s'attendre à l'aggravation des discours diviseurs, tant au sein de la droite que de la gauche – notamment de la part des militants anti-immigration, anti-mondialisation et anti-pipelines. Or, le Kremlin n'est pas la seule source de menace identifiée; l'Iran et la Chine le sont également. Quel que soit le régime, les groupes mandataires constitués en vue de commettre des méfaits et de promouvoir des positions favorables au régime posent une menace sérieuse pour nos processus démocratiques.

Heureusement, le Canada est bien conscient de la menace posée par la Russie. Le Centre de la sécurité des télécommunications du Canada a conclu que l'élection de 2015 avait été ciblée par des interférences numériques étrangères. Et, en janvier 2019, Ottawa a annoncé plusieurs initiatives importantes pour lutter contre la désinformation. Bon nombre de ces mesures méritent d'être saluées. D'ailleurs, l'ancien président estonien, Toomas Hendrik Ilves, membre de la Commission transatlantique pour l'intégrité des élections, a déclaré que le Canada traçait la voie à suivre sur plusieurs fronts. Il a pourtant aussi lui-même reconnu que malgré les efforts déployés, le Canada « n'en fait toujours pas assez », soulignant ainsi l'ampleur des difficultés.

C'est dans ce contexte que ce rapport présente un certain nombre de mesures à l'intention des autorités canadiennes en matière de protection contre l'ingérence étrangère. Elles comprennent les suivantes :

- Le gouvernement doit collaborer avec les entreprises de médias sociaux pour adopter des politiques visant à renforcer la confiance des utilisateurs et du grand public à l'égard de ces plates-formes de plus en plus populaires.
- Les partis politiques nationaux doivent mettre au point et déployer des protocoles de sécurité robustes pour protéger les données de leurs sympathisants.
- Les politiques et les règlements du CRTC doivent être actualisés de manière à ce que les détenteurs étrangers de licences de distribution par câble puissent être tenus responsables de la diffusion de matériel de propagande et de fausses nouvelles sur leurs chaînes de nouvelles.
- Le Canada doit signaler à ses adversaires potentiels que les attaques majeures contre ses actifs stratégiques, y compris ses médias et ses processus démocratiques, pourraient déclencher une réaction en accord avec le libellé de l'article 5 de l'OTAN.
- Le Canada doit adhérer et participer activement aux Centres d'excellence de l'OTAN, tout particulièrement à ceux des États baltes.
- Le gouvernement fédéral doit mettre pleinement en œuvre le Projet de loi C-59 afin de permettre aux agences de sécurité canadiennes de déployer la capacité nécessaire pour neutraliser les attaques et contrer la désinformation.

Ultimement, un public, des médias et des gouvernants bien informés et éduqués constitueront la ligne de défense la plus solide contre les campagnes de désinformation et d'influence étrangères. Le public doit disposer des outils appropriés pour pouvoir consommer des contenus multimédias en faisant preuve de discernement, pour vérifier les faits et pour remettre en question la désinformation étrangère et les idées fausses relayées et amplifiées par ces plates-formes en vue de manipuler nos points de vue et de déstabiliser notre démocratie et notre société.

Introduction

> *Foreign interference is a relatively low-cost affair in terms of human or financial resources needed. Yet it brings the almost guaranteed advantage of undermining confidence in our legitimate institutions, something non-democratic regimes like Russia relish in. Worryingly, Western governments are still fighting the last war: They're stuck in the blunt 2016 lexis of "fake news," while current trends indicate that Russia and similar adversaries are sharpening their toolkit.*
>
> – **Anders Fogh Rasmussen,** former Secretary General of NATO, and
> **Michael Chertoff,** former US Secretary of Homeland Security

The Russian government has successfully weaponized disinformation as a tool to advance its foreign policy objectives and destabilize its adversaries. The effectiveness of its operations has ensured that it will continue developing and improving these tactics, which will only become more efficient thanks to developments in artificial intelligence (AI) and other technological advances. Democracies around the world, including Canada's, will be put in peril if countermeasures remain static. We must invest in countering Russian disinformation now in order to boost our immunity and resilience against it.

Referring to the May 2019 European elections, Mark Galeotti, a Senior Associate Fellow at the Royal United Services Institute, warned that the Kremlin would focus on "exploiting the campaigns and outcomes to maximise internal dissent and to make them as acrimonious as possible." The same can also be said of the Canadian federal election later in the year. Such exploitation would entail using disinformation and propaganda designed to polarize the public's views. As Galeotti goes on to note, such tactics would likely be supported by covert intelligence activities, which "could range from hacking and leaking real or doctored materials, to providing relatively small amounts of what the Russians call *chernaya kassa*, or 'black account' moneys, to useful individuals, campaigns and media outlets (in an age when a passionate partisan with a website or a Twitter feed can be considered such an 'outlet')" (Galeotti 2019).

The cost of engaging in information warfare is remarkably low, while its destructive yield is extremely high. Groups who profit from disinformation through advertising revenue, including those who help fund propaganda and conspiracy theory websites by placing ads on them, must be held to account and be regulated so they do become accountable if they are unable or unwilling to do so voluntarily. Politicians, policy-makers, academics, and former diplomats who speak on behalf of malign foreign regimes must face a cost for allowing themselves to be used as proxies or "useful idiots" in western media and society. This includes identifying them and their foreign interests so that the public can put their views and analysis into the proper, and critical, context.

It's clear that the world's autocrats and dictators view media and information as strategic, which is why they control and censor it domestically and use it against us when it suits them. Like their adversaries, democracies need to view information and media as a strategic asset – one that alongside our elections and democratic processes is an important part of our national critical infrastructure. Any attempt to attack our information and media should therefore be treated as a cyber attack.

Disinformation represents the greatest threat to our democratic society that we face today. Any solution must be non-partisan since foreign disinformation is driven by an ideology aimed at the subversion and destruction of western democracy. Maximizing public trust in any response should be a priority and any potential solution must involve the ongoing, constant input and participation of all major political parties and their leaders. Governments and state authorities will need to be involved, but we also need to ensure that norms of free expression and media are protected. As such, concerns about government overreach with regards to censorship must be taken seriously and measures taken to ensure that counter measures are transparent.

This report draws upon the experiences of other Western states that have faced active threats posed by Russian disinformation and the disruption of their democratic processes and societies. Using the insights generated from these case studies – including Sweden, the Baltic states, France, and Germany – the report outlines possible tools that we in Canada can use to protect our elections and the democratic processes that underpin them. It concludes with a list of recommendations that are based on the lessons learned by those jurisdictions and the measures they've taken to secure their own democracies. Canada should apply those recommendations to this country to protect our upcoming federal election against foreign interference.

Case Studies from Europe

In the past decade, Russia has spent significant resources to spread disinformation and disrupt the elections and decision-making processes of its perceived enemies, including in Europe and North America. Perhaps most well-known are the "active measures" it took in the lead-up to the US presidential election in 2016, the success of which has only emboldened the Kremlin. There have been a number of other occasions where Russia was suspected of interfering in elections and key referendums, including the Netherlands' referendum on the EU-Ukraine trade deal in 2016, the UK's referendum on Brexit in 2016, and France's presidential election in 2017, among others. For this reason, it seems prudent to expect an increase in Russian-directed and sponsored attacks in the near future, especially as the electorate in many countries in Europe and North America, including Canada and United States, are going to the polls over the next few years.

This section will explore how other countries have approached dealing with Kremlin disinformation and the threat of election interference. In so doing, we will determine what the best practices are for dealing with such interference. Our goal is to inform Canada about how best to respond to this threat so it can Russia-proof its elections. We have selected a diverse range of European countries for our analysis. They include large and geopolitically important European countries like France and Germany, which have been targeted by Russia partly for that reason; all three Baltic states, which have had a long history in dealing with foreign interference from Russia; and the non-NATO country Sweden, which has become a close NATO partner and, for that reason, has also emerged as a possible target of Russian interference.

Sweden

Sweden's recent shift towards greater cooperation with NATO, its public contemplation about joining the alliance, and its influence on important issues in the Baltic Sea region, have all increased the likelihood of it being targeted by Kremlin disinformation and influence operations. In 2016, according to the head of Sweden's main foreign intelligence agency, Russia was the most frequent cyber attacker against the Nordic state (SVT Nyheter 2016). A 2018 US Senate Foreign Relations Committee Report identifies Sweden, among the other Nordic countries, as "a favorite target of the Kremlin's propaganda machine" (US Senate, Committee on Foreign Relations 2018).

Given that its parliamentary elections were held in the fall of 2018, Sweden was able to assess Russian interference in various Western elections and referendums prior to preparing for its own election. Swedish government officials used the opportunity to meet their Western counterparts and other specialists and applied what they learned to adapt the country's defences and adequately tailor its policy measures. Sweden's security institutions (The Local 2016) and political leadership (The Local 2017a) have also publicly warned about Russian interference.

The main government driver and coordinator of the country's response is the Swedish Civil Contingencies Agency (MSB), which is the national civil defence agency under the Ministry of Justice. One of its primary civil defence measures is to educate the public about being more critical of the news media. In advance of the 2018 election, MSB was tasked for the first time with educating election officials and preparing them for election meddling or influence operations targeting the election (Kremlin Watch 2019). MSB works with the National Board of Elections and all other applicable and stakeholding agencies to safeguard the elections.

Russian interference before the Swedish election

Russian proxy messengers, such as certain far-right media outlets like Alex Jones, have targeted Sweden due to its migration-related policies and so-called censorship (Colliver et al 2018). Of note, bot activities spiked in the days prior to the elections. A Swedish exit from the European Union ("Swexit") has also been a recurring narrative in right-fringe communication, despite the fact that EU support in Sweden is at an all-time high. The Swexit theme has been repeated and enhanced by alt-right and Russian English-language media. Moreover, the youth Nazi movement conducted a rather well-coordinated delegitimization campaign against the conservative party (Moderaterna).[1] The political logic is clear – by undermining the ruling Social Democrats and delegitimizing the moderate right, the far-right can only gain. And, given that the far-right have views that are aligned with Russia on a number of issues (from immigration to possible NATO membership), Russia's efforts now and in the future to cultivate such views may potentially bear fruit.

Yet, while reports indicate an increase in disinformation activities against Sweden (Dagens Nyheter 2017), the country still experienced relatively limited Russian interference activities in the lead-up to the 2018 election. This is partly due to Sweden's preparations in advance of the country going to polls. Sweden has a robust experience with civil crisis response and prior to the election it also established an election task force, which was composed of dozens of relevant public and private agencies and actors to safeguard its elections. Thousands of public officials were trained. It also published an extensive manual on countering influence operations. On the technical side, Sweden also used a paper ballot electoral system, which reduced the chances of a cyber attack that could delegitimize the election results.

An additional reason for the limited extent of Russian interference stems from Sweden's domestic situation. While Sweden is domestically vulnerable due to real internal grievances over migration-related issues, the country also has local conditions that make it harder for Russian intelligence to operate. For instance, Russia has limited capacity to communicate fluently in Swedish and the country is home to only a small Russian minority (fewer than 20,000).

Sweden's political culture also makes it harder for a strong pro-Kremlin political party to be cultivated. Simply put, Sweden does not have a political counterpart to the usual Kremlin proxies in other European states, such as the French National Front, Austrian Freedom Party, or Italian 5-Star Movement. So far, Russia's political allies are limited to a new micro-party (Alternative for Sweden[2]) and to individuals pushing the "neutral" agenda within the mainstream parties. The strongest anti-establishment party, Sweden Democrats, has not yet shown itself as a Kremlin proxy. It remains an open question whether Russian cultivation efforts will prove more successful in the future.

A final factor is timing. Three arguably more significant political events with the potential to have a larger impact were happening around the same time as Sweden's election – US midterms, elections in deeply vulnerable Bosnia and Herzegovina, and the vote in Latvia in early October. Given that the Kremlin's strategic deployment of resources is ultimately decided by a cost-benefit assessment, it is no surprise that it prioritized these other elections.[3]

Assessment

In Sweden, the Kremlin refrained from direct interference of the sort that took place in the 2016 US presidential elections or the 2016 Brexit campaign, both of which involved massive disinformation and political influence. Instead, it opted for a playbook similar to that used in the 2017 Bundestag elections in Germany, which entailed a disinformation campaign designed to help amplify migration-related narratives as opposed to the aggressive hack-and-leak tactics that Russia deployed against Hillary Clinton, for example. Russia's goal could be to cultivate the far-right in Sweden, which is already quite strong,[4] as the potential future blocker of Swedish accession to NATO. It is possible that the Kremlin, realizing that direct and aggressive interference in Sweden could backfire (and even undermine its strategic objective of keeping Sweden out of NATO), decided to pursue a less intrusive form of interference. Of course, if NATO membership had been a key campaign topic in Sweden's election, it is possible that we would have seen more aggressive Russian interference in the election.

The Baltic States: Latvia, Lithuania, and Estonia

Latvia, Lithuania, and Estonia have long suffered threats and fallout from Moscow's campaigns of information warfare and propaganda. After entering a pact with Adolf Hitler that facilitated the start of World War Two, which resulted in Europe splitting in half and Stalin's dominance over the Baltic states being guaranteed, the Soviets engineered a sham referendum for the three Baltic nations to join the Soviet Union – an act that would be replicated nearly 75 years later to provide justification for Russia's annexation of Crimea.

Throughout the half-century of Soviet occupation, the people of the occupied Baltic nations were subjected to an endless regime of propaganda that was designed to weaken their longing for independence by manipulating historical memory and everyday realities. Anyone who resisted Soviet state authority was labelled a traitor, a fascist, and an "enemy of the state."

The disintegration of the Soviet Union granted freedom and independence to tens of millions of people in Central and Eastern Europe, including in the three nations in the Baltics. Yet, for Vladimir Putin, it represented the greatest geopolitical disaster in history. Indeed, he has expressed his desire to reverse its collapse (Taylor 2018), which would include the reinstatement of Moscow's hegemony over the Baltic states.

Starting with the 2007 attacks against Estonia (see text box) and accelerating under Putin's reign, Russia has made several efforts to restore its regional dominance in the Baltics. Russia has done this by actively engaging in information warfare against these states to undermine their democracies, governments, media, and the alliances that underpin their security and independence, including membership in the European Union and NATO. After Russia's 2014 annexation of Crimea, Lithuanian President Dalia Grybauskaite warned that her country was in a state of war with regards to propaganda and information security (European Integration Studies Centre 2018).

> *Russia has made several efforts to restore its regional dominance in the Baltics.*

In addition to the Kremlin's aggressive information warfare against the Baltic nations and NATO, the Putin regime has also engaged in intelligence activities and military provocations, including large-scale military exercises near NATO borders (Standish 2017), incursions by Russian Air Force fighters and bombers, which have led to reactions by NATO Air Policing (Dearden 2017), and escalations of troop deployments in Russia's Western Military District and Arctic regions.

In the wake of Russian hybrid warfare operations against Crimea and ongoing offensives in Eastern Ukraine, the Baltic states have persistent concerns about similar operations that also use Russian minorities as a pretext. As frontline NATO countries defending against Russian information warfare, other allied and G7 nations can learn from the Baltic experience in information and cyber warfare and the strategies they have developed to defend themselves and NATO against such attacks.

Television

Kremlin disinformation narratives are commonly transmitted via Russian state television media, which is widely available in the Baltic states and viewed primarily by the significant ethnic Russian population in the region.

In 2005, the Baltic Media Alliance was registered in the UK and launched operations in the Baltic states. Its primary Russian-language television news channel is Pervõi Baltiiskii Kanal (PBK) (Król 2017). The channel has three separate editorial offices for each of the Baltic countries. In addition to rebroadcasting news produced by state media in Russia, the channels produce news about local issues, which allows producers to add a Kremlin spin. Notably, the Latvian government has fined PBK several times for showing fake Russian state news broadcasts (Sarlo 2017) and has suspended broadcasts of the Russian state channel, RTR Planeta, for allegedly inciting war.

RUSSIA’S FIRST CYBER OFFENSIVE: ESTONIA 2007

In 2007, Estonia became the first state to fall victim to a massive foreign state-sponsored cyber attack and disinformation campaign intended to destabilize the nation along ethnic lines. Harnessing massive global botnets, waves of distributed denial of service attacks (DDoS) bombarded the Estonian government, media, and business servers, knocking them offline. The Estonian government was forced to seal off its domestic Internet network from external connections, making it difficult to get information out of Estonia to the rest of the world.

The attacks were apparently triggered by the Estonian government’s decision in late April to relocate a Soviet war monument from the centre of the Estonian capital, Tallinn, to a nearby Soviet war memorial. Of note, the attacks spiked on May 9th, the Russian anniversary of the end of the Second World War.

According to former Estonian President Toomas Hendrik Ilves, the attacks intensified for some 24 hours and ended as quickly as they started. Ilves was told that “the money ran out” for sustaining an attack by international criminal hackers, which was likely paid for by someone or some state (Tamkin 2017).

Estonian analysts found early on that the “malicious traffic often contained clear indications of political motivation and a clear indication of Russian language background. For example, malformed queries directed at a government website included phrases like ‘ANSIP_PIDOR=FASCIST.’ (Mr. Ansip was the Estonian prime minister at the time)” (Ottis Undated). Estonia (and many observers) see this landmark digital attack as having been approved (and perhaps even sponsored) by the Russian government, though the Kremlin has been quick to deny such allegations (and refused to cooperate with Estonian authorities investigating the case) (Ruus 2008).

The attack did have the positive consequence of forcing NATO to start taking cyber and information warfare seriously. Before the attacks, allies were reluctant to take Estonian warnings about cyber security seriously. President Ilves told NATO officials that “‘cyber is an area NATO has to deal with.’ And they were like, ‘yeah, yeah, yeah, go away. We’re worried about real stuff.’ And then this happened” (Tamkin 2017). A year after the attack, the NATO Cooperative Cyber Defence Center of Excellence was established in Tallinn.

The attacks on Estonia’s cyber and information infrastructure were the first such politically motivated attacks in an ongoing string of similar offensives that became ever more sophisticated. They have also been combined with traditional kinetic warfare to create what is now called hybrid warfare. Indeed, just a year following the attacks against Estonia, Russian hackers attacked Georgia’s Internet infrastructure just as Russian forces invaded South Ossetia and Abkhazia. In 2014, Russia used similar tactics in Ukraine as its forces invaded and occupied Crimea.

Lithuania has also blocked PBK 2013 and done the same to other channels that are Russian state media or under indirect Kremlin control, including RTR Planeta, NTV Mir Lietuva, and TVCI (Denisenko 2018).

Estonia is countering Russian state television by funding the development of a Russian-language state media channel, ETV+. Latvia has helped support an independent Russian media platform, Medusa.io, which is staffed largely by Russian journalists who have been forced into exile. The long-term effectiveness of these alternate platforms and channels is yet unknown. Offering Russian speakers a fact- and truth-based alternative to Kremlin-controlled media is a critically important initiative that should be considered in other jurisdictions that feature large Russian speaking diaspora groups, including Canada.

Online platforms

The Kremlin employs a broad network of web platforms that advance regime objectives through directly owned websites and other platforms funded through a network of NGOs and Kremlin-aligned oligarchs. The most prominent pro-Kremlin platforms in the Baltic region are Sputnik, Baltnews, and Vesti. Sputnik is the official Russian state media platform, whereas Baltnews and Vesti have veiled and complicated ownership structures that obfuscate the identity of their actual owners (Roonemaa and Springe 2018; DFRLab 2018a).

> *Sputnik's open association with the Kremlin ensures that it is an instrument of state propaganda.*

Sputnik's open association with the Kremlin ensures that it is an instrument of state propaganda, which makes it easier for viewers to critically evaluate information published on the platform. Baltnews, which publishes more subtle headlines, seeks to acquire broader credibility by projecting a more independent and non-state-aligned position. However, a 2018 report exposed how the Baltnews group of websites "presented themselves as independent news outlets, but, in fact, editorial lines were dictated directly by Moscow" (Roonemaa and Springe 2018). The report also demonstrated that the websites were ultimately owned and funded by the Russian state news agency Rossiya Segodnya.

Vesti.lv, the Latvian-based Russian language portal, has published content that, according to an analysis by the Centre for Eastern European Policy Studies, suggests the portal "systematically spread[s] pro-Kremlin narratives in Latvia." For example, it has published stories about Canadian soldiers serving in Latvia that are intended to undermine local trust and support in the NATO mission (DFRLab 2018a; Brown 2017), some of which were republished from earlier Russian state media (Wasserman 2017). Ultimately, Russian government propaganda seeks to paint Canadian, UK, German, and other NATO troops serving in the Baltics as invaders in the Russian-speaking media (Teperik 2019). In addition, a report by Latvian investigative journalism portal RE:Baltica states that it is an open secret that the true owner of Vesti.lv is a "former member of the Russian duma and millionaire Eduard Yanakov" (Springe 2017).

The Baltic experience clearly demonstrates that the Russian government is aggressively using state-owned and state-aligned platforms to influence regional public opinion on important issues.

Elections

After Estonia's March 2019 parliamentary elections, the head of Estonia's Internal Security Service, Arnold Sinisalu, stated: "The Russian Federation has attempted to influence Estonian elections since its re-independence [in 1991]" (Vahtla 2019). Yet he also acknowledged that the "feared cyber-attacks did not occur in Estonia, and in reality, Russia didn't need them either. Influencing has taken place via the media, via social media networks, and via personal contacts – and constantly" (Vahtla 2019).

Estonia's reliance on digital governance, including e-voting, does make it an obvious target for direct cyber interference and hacking. In March 2019, for example, nearly 50 percent of all Estonians voted online instead of going to a traditional voting booth (Galano 2019). However, the country's reliance on digital technologies has also made its public more aware and its democracy more resistant and resilient to such interference. Estonian e-voting cyber security expert Liisa Past has pointed to Estonia's development of robust and secure systems in response to the 2007 cyber attacks, which have resulted in broad trust in the country's digital infrastructure (Past and Brown 2019a).

According to a joint annual assessment by Lithuania's intelligence agencies released in early 2019, "Russian intelligence will step up its activity during the 2019-2020 election cycle." Lithuanians went to the polls in May 2019 to find a successor for their staunchly anti-Kremlin president Dalia Grybauskaite. As the intelligence assessment went on to note, "Russia will seek to sway the course of the elections by information and cyber means" (Sytas 2019). The country will also hold parliamentary elections in 2020. Moreover, Lithuanian intelligence has observed Russian intelligence targeting Lithuania's energy sector, including hacking into the country's electrical control systems.

> *Lithuanian intelligence has observed Russian intelligence targeting Lithuania's energy sector.*

Latvia held parliamentary elections in October 2018. Fear of Russian interference was a prominent theme in the run-up to the election (DFRLab 2018b) – and for good reason. The country has a significant ethnic Russian minority, larger than the Russian minority population in either Estonia or Lithuania, which often relies on Russian state media and social media as its primary news source. In addition, a political party in Latvia largely caters to this minority. The likelihood that the Kremlin would seek to influence this ethnic minority could not be discounted. There had also been reports of increased cyber threat activity on the eve of the election, including a high number of threatened unique IP addresses and a massive DDoS attack on the popular Latvian news portal Delfi during a debate among the candidates for prime minister.

Yet Latvia also made some important preparations prior to the election. Latvia's CERT cyber-security group was ready to repel possible Russian interference efforts; the government worked with large social media companies like Twitter and Facebook to remove disinformation news; and ballots were scanned electronically and counted by hand (Eglitis 2018). The election did result in significant gains for pro-Russian and anti-establishment parties, but it is uncertain to what extent (if any) Russian interference had a hand in these gains.

Baltic counter measures

The Baltic states have adopted several countermeasures that other western nations should consider implementing. After its 2007 experience, Estonia was among the first in 2011 to formally adopt a long-term strategy to deal with disinformation by including "psychological defence" in its national defence strategy. This strategy states that "the purpose of psychological defence is to prevent panic, the spread of hostile influences and misinformation.... Psychological defence involves the development, safeguarding and protection of common values that are linked to the cohesion and security of society" (Estonia, Ministry of Defence 2011).

Either the Prime Minister's Office or the State Chancellery coordinates this large, whole-of-government initiative. Various ministries are tasked with "identifying hostile influences," "ensuring the continuation of public broadcasting services" (essentially defining national media as a strategic asset), and "notifying the population of the risks that may endanger society," among others. Other governments in the Baltics are also exploring a similar "total defence" concept of security, such as Latvia, which, in light of the broad nature of the hybrid warfare threat, is planning for a comprehensive defence strategy that would not be limited to military means.

SUPPORT FOR INDEPENDENT MEDIA

Governments in the Baltic region have also realized that strong, local, Russian-language media can compete with Russian state media, helping blunt the Kremlin's propaganda narratives in those countries. In Estonia, for instance, the government has responded to the threat of Russian state television news propaganda by creating ETV+, a Russian-language television news programming channel that offers an alternative to Russian state news. Latvia also supports the ongoing development of independent Russian media outlets, such as Meduza.io, which has become a hub for Russian-language journalists who have been forced into exile by the Russian government.

DETECTING, MONITORING, AND COUNTERING FALSE NARRATIVES AND TROLLS

Among NATO and EU nations, the Baltic states have had the most tactical experience defending against Russian government information warfare. Yet they have struggled to convince their allies about the threat. "Ten years ago there was no way to discuss these issues at all, because [EU] colleagues thought 'it is not our business, it's freedom of speech and that's it,' says Lithuanian Minister of Foreign Affairs, Linus Linkevicius, 'it took time to convince them that lies are not freedom of speech'" (Peel 2019).

Across the Baltics, civil society organizations and volunteers have taken it upon themselves to fight Kremlin disinformation and raise public awareness. A website supported by Estonia's civilian defence league, Propastop.org (Propastop Undated), posts regular news about ongoing Kremlin disinformation operations. The Lithuanian "elves" (in contrast to the Kremlin's Internet Research Agency "trolls") are a loose group of thousands of journalists, IT professionals, students, business people, and scientists who expose and combat false claims and narratives, debunk them, and identify and publicly expose Kremlin trolls and proxies (Peel 2019). Similar groups have also formed in Latvia. In Lithuania, a website similar to Estonia's propastop.org, called debunk.eu, fact checks and debunks disinformation. The EU-funded euvsdisinfo.eu website also analyses misleading and false narratives in real time and provides tools to improve the public's ability to detect disinformation when it's being published and shared.

Raising awareness of disinformation campaigns and narratives by alerting the public when they emerge is one way to build public resistance against them. These sites can act as early warning systems for local media, politicians, and governments to let them know of disinformation attacks.

Moreover, the Latvian and Lithuanian governments have adopted regulations that would allow them, much like the British government's Office of Communications (OFCOM), to levy fines against Russian state-run outlets that are reporting false information. The fines, while small, are publicized to fulfill the important task of raising warnings about the perils of trusting Russian state media sources (Fried and Polyakova 2018).

In Estonia, the Internal Security Service publishes an annual report that highlights Russian intelligence operations and disinformation campaigns. This includes details of attempts to discredit leading Estonian politicians, such as former President Toomas Hendrik Ilves, who was targeted for a smear by Russian state media. News "scripts" obtained from two Kremlin reporters, who were detained by Estonian authorities when they tried to enter the country without documentation, outlined how the reporters were to concoct a story about the former president's father's collaboration with the occupying Nazi forces during the Second World War (Estonian Internal Security Service 2018) – an effort that draws parallels to Russia's attempts to discredit Canadian Minister of Foreign Affairs Chrystia Freeland by directly promoting a story about her grandfather's work at a Krakow newspaper in Nazi-occupied Poland (Glavin 2017a).

The Latvian government also makes it a priority to expose disinformation. Citing disparaging stories published by pro-Kremlin media platforms about Canadian soldiers in his country, Foreign Minister Edgars Rinkevics says "everybody has a right to know this is fake information and who is behind spreading it" (Dorell 2018). The Latvian government has exposed other disinformation campaigns, including a webpage that was maliciously created to promote a fake independence movement in Eastern Latvia for a "People's Republic of Latgale" (similar to the Kremlin-organized separatist movement in Eastern Ukraine). This site was created by forces inside Russia and quickly shut down by the Latvian government, according to Latvian security police (Higgins 2015).

LITERACY, EDUCATION, AND CYBER HYGIENE

Media literacy, cyber hygiene, and awareness of disinformation campaigns are at the foundation of any program to counter foreign interference and information warfare. In the lead-up to Estonia's recent parliamentary elections, the Estonian government took efforts to educate local political parties and individual candidates about the threat of foreign disinformation and how to protect themselves and their data (Past and Brown 2019b). In Latvia, the Information Technology Security Incident Response Institution operating under the Minister of Defence educates state employees on cyber hygiene including identifying suspicious emails, phishing attempts, and other activities (Eglitis 2018). Lithuania's government, meanwhile, has prioritized media literacy as part of its "Lithuania 2030" national strategy, with a variety of educational projects meant to cultivate critical thinking and media literacy (Denisenko 2018).

If they are to protect their democratic systems, western nations should follow the lead of the Baltic states, taking tougher government approaches to disinformation that include greater support for civil society groups and other organizations that are committed to fighting it. Experts have been sounding warnings about this threat since the 2007 cyber attacks on Estonia, yet have been largely ignored in most of the West, including Canada, until recently.

France

France's global influence and its importance within the EU alongside its opposition to Russia's aggression in Ukraine and Syria have made the country a primary target for Russian interference. In the French presidential election of 2017, for example, the threat of Russian influence remained a continual source of anxiety. The French had good reason to be anxious given what the staff of candidate (and later president) Emmanuel Macron called a "massive and coordinated" hacking operation.

On May 7, 2017, for example, prior to the presidential election, tens of thousands of documents and emails were hacked from Macron's campaign and uploaded to the public domain (Bulckaert 2018; Brattberg and Maurer 2018). Prior to the cyber leaks, then US National Security Agency Director Mike Rogers had informed his French counterparts that the agency had detected possible Russian hacking of France's election system (Matishak 2017). Yet, despite many brazen attempts from Russia, France was able to effectively counter Russian interference, thanks to the significant precautions taken by French security officials and Emmanuel Macron's campaign team.

> *Despite many brazen attempts from Russia, France was able to effectively counter Russian interference.*

During the electoral campaign, Macron made the point of frequently criticizing Russian meddling and went so far as to ban both Sputnik and RT from covering his campaign. Having personally experienced this Russian interference, President Macron has emerged as a leading European voice against Russian government interference and disinformation. During a press conference with the Russian president shortly after being elected, Macron bluntly told reporters that "Russia Today and Sputnik were agents of influence and propaganda that spread falsehoods about me and my campaign" (Serhan 2017).

Notably, during the election, France's National Commission for Control of the Electoral Campaign banned the country's media outlets from publishing information garnered from the hack, with the threat of criminal charges if they did so (Rosenberg 2017). Yet media outlets also cooperated in countering disinformation campaigns, including the French newspaper *Le Monde*, which released an index with "hundreds of websites and their level of reliability." Google also developed a "CrossCheck fact-checking platform," in partnership with various newspapers, television, and other media platforms (Brattberg and Maurer 2018).

Meanwhile, the National Cybersecurity Agency of France (ANSSI) had warned that there was "an extremely high risk" of cyber attacks and electoral hacking. As a result, ANSSI suspended electronic voting for French citizens overseas in both the legislative and presidential elections in 2017 (Brattberg and Maurer 2018; McAuley 2017). ANSSI also played a proactive role in educating campaign staff on cyber security, and even visited the Macron campaign headquarters to warn of a possible attack (Vilmer 2018).

Following the ANSSI warnings, Macron's team took additional steps to protect against cyber threats, including only using emails to "exchange open information" and switching from the Telegram app, which is a Russian application, to the end-to-end encrypted WhatsApp (Bulckaert 2018). Macron's party also used unconventional methods. For example, according to Mounir Mahjoubi, who led Macron's digital team, "You can flood these addresses with multiple passwords and log-ins, true ones, false ones, so the people behind them use up a lot of time trying to figure them out" (Dickey 2017).

French authorities were very quick to respond to a foreign threat on their electoral system by issuing "clear public declarations and warnings" (Brattberg and Maurer 2018). And, once they realized that they were under attack, the Macron campaign was also very quick to publicly declare that they were the victim of a "massive and coordinated" attack. As Erik Brattberg and Tim Maurer noted, "This raised the stakes for the attackers considerably and mitigated its impact" (Brattberg and Maurer 2018)

French society also seems particularly resilient to disinformation campaigns, which is another important reason why the disruption did not succeed. According to a recent study, "75 percent of the French people surveyed trust information from traditional media, while only 32 percent trust information from online media and only 25 percent trust information from social networks" (Brattberg and Maurer 2018). Notably, *Le Monde* has developed "a suite of public-facing fact-checking tools" in the form of Décodex, which uses a large database of websites and social media profiles that users can filter in order to ascertain their legitimacy (Owen 2017).

In addition, President Macron has proposed an anti-fake-news law that will crack down on "fake news" spread on social media. The new legislation would also demand that websites make their financing more transparent. For instance, Macron suggested that websites would have to show "who is financing them" and for what (Independent 2018). "If we want to protect liberal democracies, we must have strong legislation," Macron told a news conference in early 2018 (Independent 2018).

Germany

Classified by the European Values think tank's "Kremlin Watch" program as "awakened" (Kremlin Watch 2018), Germany is still failing to deliver concrete results, even though it is a key target of hostile actors in the EU (Janda and Víchová 2017). The German government and its lawmakers have been contemplating the problem (Deutscher Bundestag 2019a) from different angles for three years now but have not issued any official document outlining a clear and comprehensive policy. The German efforts are a patchwork of niche initiatives which are often poorly funded and remain uncoordinated.

Part of the problem is Germany's historical experience. Security professionals understand well that countering hybrid threats takes a comprehensive, inter-ministerial approach. But so far, the government is reluctant to create an effective inter-ministerial centre with executive capabilities and international links. The upshot of this situation is a fairly strong German approach to tackling threats in cyberspace and social media (like bot nets), but failing to attack the physical part of the hybrid network (economics, finances, politics, sociology).

The Ministry of Foreign Affairs is fighting disinformation. It has established a web page that relies entirely on the work of the EU Stratcom division, though no specific German policy has been articulated there either (Germany, Federal Foreign Office 2018). German lawmakers have also started to focus on the sources of disinformation and have repeatedly put the issue on the parliamentary agenda (Deutscher Bundestag 2019b). In addition to the security of digital infrastructure, German authorities are also focused on the role of social media in spreading disinformation. However, no concrete regulation has yet been developed.

Contrary to misleading statements made in front of the US Senate (Stelzenmüller 2017), the German law on hate speech is not able to fight disinformation. Simply put, this law does not have enforceable mechanisms to combat disinformation, as others have reported (BBC 2018). As Daniel Funke rightly noted: “Having gone into effect Jan. 1, Germany’s law against hate speech on Facebook is perhaps the most realized – but often misunderstood – effort to quell potentially harmful content online” (Funke 2018).

The German law on hate speech is not able to fight disinformation.

This law forces online platforms to remove “obviously illegal” posts within 24 hours or risk fines of up to €50 million. Aimed at social networks with more than two million members (e.g., Facebook, YouTube, and Twitter), the law gave platforms until the end of the year to prepare for the regulation. The law’s implementation points to the Bundestag’s willingness to move against questionable online content, but its enforcement has been rocky. A satirical magazine called *Titanic* published a piece with insults and was banned from Twitter (Reuters 2018), and even the minister of justice – who helped author the NetzDG – had his tweets censored (The Local 2018). In early March 2018, officials considered revising the law following criticism that too much content was being blocked (Thomasson 2018). Among those revisions were ones allowing users to get incorrectly deleted content restored, as well as pushing social media companies to set up independent bodies to review questionable posts.

Until recently, the Federal Republic of Germany relied broadly on NGOs to confront disinformation, despite them being ill equipped for such a role. Critics voiced concerns after seeing media monitoring initiatives and NGO representatives who had been facilitating disinformation operations on German soil in the past, now claiming to be fighting Russian influence. Indeed, some of the NGO representatives even gave long interviews to Russian disinformation channels, granting legitimacy to these media. Others openly spread Kremlin narratives during the so-called US National Security Agency (NSA) surveillance scandal (Reuters in Berlin 2015), which contributed widely to the rise of anti-Americanism in German society and which served the Kremlin’s agenda very well.

The main expertise in confronting hybrid threats in civil society remains with Germany's Ministry of the Interior. It oversees the activities of the BSI (*Bundesamt für Sicherheit in der Informationstechnik*), which covers the cyber security dimension of influence operations, as well as the domestic intelligence agency of the Federal Republic of Germany (*Bundesamt für Verfassungsschutz*) entrusted with the monitoring and assessment of hybrid attacks. Due to the fragmentation of its structure, the ministry has proven itself in the past to be relatively slow in the collection and assessment of threats.

A step in the right direction is the new Agency for Cybersecurity linking the Ministry of Defense and the Ministry of the Interior's research capabilities in cyberspace (Bundesministerium der Verteidigung 2019). Yet this initiative faces obstacles: The German Constitution poses certain limits on the concentration of resources. The Ministry of Defense, the Ministry of the Interior, and intelligence agencies have strict limits on their areas of operation. For instance, Articles 87a and 87b of Germany's Basic Law restricts the domestic use of the armed forces (Germany, Federal Republic Undated). It leads to the paradox that experienced operative information units can be deployed in support of German armed forces during their missions abroad, but their use or even the exploitation of their expertise is strictly prohibited on German soil.

Canada's Experience Fighting Disinformation

In the Cold War, Canada's proximity to the United States, its leadership role in NATO, and its position as a trusted middle power had made the country a particularly attractive target for Soviet subversion. Indeed, nearly 20 Soviet intelligence agents from both the KGB and GRU were operating in Canada, as well as 17 identified Canadian agents, according to a 1946 Royal Commission known as the Gouzenko Report. The Soviets focused on both promoting communist philosophies and values and identifying issues that had the potential to divide, including Quebec's separatist movements and other areas of social unrest.

Today, Canada's growing international leadership on issues of human rights, Kremlin aggression, and its role in NATO and the G7, all stand in the way of Vladimir Putin's objective of reestablishing Russia's Cold War hegemony in Central and Eastern Europe and beyond. The threat of Russian disinformation has been known for some time. In the 2015 election, the Conservative Party committed to creating and funding a Digital Freedom Fund to counter Kremlin disinformation. The Canadian Security Establishment later confirmed that the 2015 election was targeted by foreign digital interference.

The Kremlin may not have an obvious champion in the coming 2019 federal election, given the largely cross-party consensus on the need to stand firm alongside our NATO allies against Vladimir Putin's regime. Indeed, unlike in European countries, Canada lacks a significant far-right party that is aligned with the Kremlin or with Vladimir Putin's United Russia Party. However, attempts to amplify narratives that threaten to divide Canadians on both the right and left – such as those that promote anti-immigration, anti-globalism, and anti-pipeline – will intensify. Similarly, the ongoing targeting of critics of Russian President Vladimir Putin's regime, including MPs, candidates, ethnic groups, NGOs, and prominent activists, will likely escalate as Russia seeks to discredit them and their positions.

The Kremlin's no-holds-barred attitude to information warfare has demonstrated that any issue that offers an opportunity to undermine western society is seized upon and exploited. This includes the anti-vaccination campaign, which has been actively promoted and amplified by the Kremlin's trolls and which has contributed to the emerging international health crisis (Kolga 2019a). Truth and borders are no issue for the Kremlin troll farm, as was exposed in a recent report on its active role in suppressing anti-government protests in Sudan. Among other false narratives, these trolls effectively blamed the West for the protests and proposed "public executions of looters and other spectacular events to distract the protest-minded audience" (Lister, Shukla, and Elbagir 2019). Kremlin-supported diaspora organizations, such as "Russkiy Mir," have also promoted and advanced pro-Kremlin positions (see text box).

Many of the 500,000 Russian speakers living in Canada receive their news from Russian state television, including Russia 1 and its flagship show *Vesti*, which recently produced and aired a piece that disparaged Canada's Ukrainian minority as fascists who "dictate Canadian foreign policy" (Brown 2019). The claim was characterized as "bizarre" by Ukrainian Canadian Congress President Alexandra Chyczij in a rebuttal where she reminded Canadians that the program's host, Dmitry Kiselyov, has been placed on Canada's sanctions list as Vladimir Putin's chief propagandist at the Russian state media agency, *Rossiya Segodnya* (Chyczij 2019). The same channel supports Russian government narratives that claim the Ukrainian government is run by "fascists," despite the fact that both the prime minister and president are themselves Jewish.

> *The Kremlin is not the exclusive source of disinformation threats to Canada's democracy and elections.*

English-language Russian state propaganda also has a direct pipeline into Canadian homes via RT (formerly known as Russia Today). In Canada, the Russian government pays to have RT bundled on basic cable and international news packages (Robertson 2017). While RT has faced multiple fines in other jurisdictions, such as the UK, for violating broadcast regulations requiring news outlets not to broadcast false news or information, Canada's CRTC offers no such mechanisms. Any such regulation is therefore left to Canadian cable operators to apply voluntarily.

The Kremlin is not the exclusive source of disinformation threats to Canada's democracy and elections. Iran and China are among other states that have been identified as threats. In April 2019, for instance, an allegedly forged letter on Prime Minister Trudeau's letterhead and bearing his signature conveyed congratulations to a mysterious new Tibetan organization that seems to promote pro-Beijing views about Tibet. Liberal MP Arif Virani alerted constituents on Facebook, writing that he was "alarmed to learn that the 'letter of support' from Prime Minister Justin Trudeau to the newly created 'Tibetan Association of Canada' is a forgery. This matter has been reported to officials who are looking into this further" (Virani 2019).

Regardless of regime, proxy groups that are organized to sow mischief and promote and advance pro-regime positions represent a serious threat to our democratic processes. These groups have been particularly interested in tricking political leaders and media into believing that they legitimately represent the interests of Canadian communities. Over the past years, foreign trolls, proxies and media platforms have also targeted Canadian political leaders and activists who are critical of them in efforts to discredit them (Carley 2017; Babalich 2017; Helmer 2019a). And attempts to interfere in Canada's national debates and elections have been documented by national and international media.

The Canadian government announced several major initiatives to counter foreign disinformation in January 2019. Former Estonian President Toomas Hendrik Ilves, who is also a commissioner with the Transatlantic Commission for Election Integrity, has stated that Canada is in many ways leading the effort to address foreign disinformation.

The remainder of this paper will explore what Canada has recently announced it will do to address this threat. In recent months, the government of Canada has put together a number of initiatives that are designed to address the threat of foreign interference in our elections. Many of these measures can be commended, although as Ilves himself has acknowledged, when it comes to Canada's efforts, we are "still not doing enough," underscoring the depth of the challenge. With that in mind, this section will conclude with some recommendations on what other measures we need to implement to address this threat.

Canadian measures against foreign interference

Election Modernization Act

Bill C-76, also known as the *Elections Modernization Act*, amended the *Canadian Elections Act*. The omnibus legislation was passed in December 2018 and introduced a number of new measures to the elections law to help prevent foreign interference in the election. These measures include regulating spending by third-party advocacy groups and restricting the amount of money that political parties spend on their election campaigns.

Bill C-76 imposes fresh transparency obligations on platforms that publish political advertisements (i.e., Internet sites and Internet applications). The bill requires the owners of all online platforms to maintain a registry of (the eligible parties') advertisements that includes a copy of the ad displayed as well as certain prescribed information (i.e., the identity of the party that authorized the advertising). Any person or entity that intends to affect the results of an election by means that include electromagnetic, intercepts, destroying or altering data, illegally accessing the system, or any other mechanical means, could also be charged under the Act.

The Act also prohibits parties from using foreign money to fund partisan activities during a federal election. When there is a violation, there will be penalties of up to five times the amount of foreign money used. Clause 349.02 of the Act clearly says: "No third party shall use funds for a partisan activity, for advertising or for an election survey if the source of the funds is a foreign entity" (Justice Laws Website 2018).

In addition, Bill C-76 prohibits undue influence of overseas Canadians by foreigners. The law extended the right to vote to expatriate Canadians, no matter how long they've lived outside the country, rather than the previous five-year limit. There are around two million Canadians who live outside the country, of which only about 30,000 ex-pats will actually take advantage of the right to cast a vote. Some, including some Conservative senators, have been critical of this provision, arguing that these Canadians might potentially be compelled to vote a certain way by unfriendly foreign governments.

TARGETING CANADIAN POLITICAL LEADERS

Events marking European Unity Day are held in cities throughout Europe and throughout the world on May 9th to celebrate peace and unity in Europe. The Kremlin holds events on the same day to celebrate the Soviet Union's World War 2 victory over the Nazi regime, which has been more recently used to glorify the Soviet occupation of much of Central and Eastern Europe and Russian military power more generally.

On May 9th 2019, a Facebook group declaring itself the Canadian representative of Russkiy Mir – a Russian compatriot non-governmental group that was formed by a decree issued by Vladimir Putin in 2007 (Russkiy Mir Foundation Undated) – claimed on its Facebook page that it had been invited to participate in the EU Unity Day flag raising ceremony at Ontario's Provincial legislature in Toronto's Queen's Park. According to EU representatives in Canada, the flag held in the photo posted by Russkiy Mir emerged after the official flag raising ceremony and was held upside-down by the group in the photo (Nachetoi 2019). No official invitation had been extended to this Facebook group.

The Ukrainian Congress in Canada identified a connected post by a Canadian "Immortal Regiment" Facebook group run by the same Russkiy Mir group, which stated that the group had visited with an Ontario MPP and "worked to remove reference to the Holodomor from Bill 97." Introduced by MPP Aris Babikian, Bill 97 is meant to proclaim a Genocide Awareness, Commemoration, Prevention and Education Month in Ontario. As translated by the UCC, the Immortal Regiment/Russkiy Mir Canada post had openly stated that they:

> *were able to ensure that the reference to the Holodomor-genocide of Ukrainians, was removed from the bill! We promised to support Bill 97 […] on the condition that the point about the Holodomor as a genocide of Ukrainians will not be there. The MPP who promotes the bill came to our Immortal Regiment. He saw how strong and friendly our community is, how many of us there are, and immediately agreed to our conditions and gratefully accepted our support. (Ukrainian Canadian Congress, 2019)*

In a statement issued on May 13, MPP Aris Babikian responded, stating that:

> *I would like to assert that the Russian organization's statement that they had any influence in removing reference to the Holodomor in Bill 97 is a complete lie and fabrication. I would note that what they're claiming is incorrect. My bill does not change the way Ontario treats the Holodomor. Not at all. I have had no dealings with them whatsoever. (Babikian 2019)*

While we may not know who exactly runs the Canada Russkiy Mir page, it is clear that attempts have been made to influence public perceptions on these issues. All Canadian media and legislators should be aware of such attempts, and that they will likely continue to be made from actors who are aligned with malign foreign regimes, ahead of the fall federal election and should take precautions to avoid them.

Digital Citizen Initiative

The government of Canada has introduced a mechanism known as the Digital Citizen Initiative. It is a multi-component strategy that aims to support democracy and social cohesion in Canada by building citizen resilience against online disinformation and building partnerships to support a healthy information ecosystem. This initiative supports and funds citizen-focused activities that will help people critically assess online information, acquire skills that enable them to avoid being susceptible to manipulation online, and effectively engage in public discourse online.

Digital Democracy Project

Ottawa is proposing to set up a new project through the Heritage Department to increase the public's ability to identify online disinformation. The Digital Democracy Project will receive $19.4 million in funding over the next four years. That funding, according to the budget, will "support research and policy development on online disinformation in the Canadian context" (Canada 2019b). The government will also leverage the new project to lead an international initiative aimed at creating guiding principles to be used around the world to combat online disinformation.

G7 Rapid Response Mechanism

In an effort to keep a closer eye on international threats, the government has activated a Rapid Response Mechanism, a new initiative that Canada signed on to at the G7 meeting in 2018 and has taken leadership of. It was part of a multi-pronged commitment to defend democracies from foreign threats. Global Affairs Canada's unit monitors foreign social media activities to identify whether those activities pose a threat to Canadian democracy, and produces regular reports that are distributed to G7 members, but are not available to the public.

Critical Election Incident Public Protocol

The federal government has established yet another new mechanism known as the Critical Election Incident Public Protocol to determine the seriousness of threats to the 2019 federal election. The protocol includes senior public servants such as the national security advisor and the deputy minister of Global Affairs Canada, who will determine which incidents seriously threaten the integrity of the election process. If any egregious incident that could affect the election result is detected, the group will notify Canadian citizens. However, questions have been raised about incident thresholds. So too have questions about potential partisanship (Kolga 2019b), which need to be addressed to ensure trust in this system.

Security and Intelligence Threats to Elections (SITE) Task Force

Composed of RCMP, CSIS, CSE, and Global Affairs members, the Security and Intelligence Threats to Elections (SITE) Task Force will monitor foreign disinformation and, according to the government website, "improve awareness of foreign threats and support assessment and response" (Canada 2019a). Notably, however, there is very little detail about which awareness will be improved – whether public, government, media, or other.

Bill C-59

Bill C-59 gives the Canadian Security Establishment (CSE) the power to engage in "defensive cyber operations" and "active cyber operations" (CSE 2019). Live cyber operations are to be deployed “through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to Canada’s defence, security or international affairs.” This could include any threat to Canada’s national security, including cyber or information warfare.

This legislation received royal assent, and once implemented, would allow the CSE to interfere and disrupt foreign cyber attacks that target Canada, including by launching cyber attacks of its own for the first time in its history (Tunney 2019). C-59 introduces the real threat of Canadian counterattacks against cyber and other digital infrastructures as well as digital information environments. The use of “active cyber operations” could not only proactively shut down the source of a possible cyber attack against Canada, but also serve as a source of deterrence against the use of such tools in the first place. For that reason, Ottawa should ensure that foreign malign actors are made aware of these capabilities, and Canada’s willingness to use them, including in the event of major cyber attacks during the 2019 federal elections.

Social media

Today’s Wild West social media environment has been taken advantage of by malign actors and foreign countries in efforts to expand existing divisions by amplifying resentment on both the left and right. The government has expected that social media platforms will police themselves in order to deter and eliminate foreign digital interference. Yet, as Canada’s minister for democratic institutions told reporters in April 2019, she was “not feeling great about where we are right now” (Lum 2019). Some form of government regulation seems inevitable if social media platforms do not take additional steps to protect users.

However, recent reporting about social media’s role (Kolga 2019c) in exacerbating the emerging global measles epidemic demonstrates that these platforms are perfectly capable of self-regulating when they feel compelled to. For example, Facebook announced earlier this year that it would take measures to combat anti-vaccine information by adapting its algorithms to lower the ranking of Facebook pages where false information about vaccinations are published (Weeks 2019), clearly establishing the fact that social media algorithms can be adapted to filter out foreign disinformation narratives.

Canadian Election Integrity Initiative (Facebook)

In 2017, Facebook Canada announced the Canadian Election Integrity Initiative, a measure that is especially designed for Canada to ensure that the 2019 election is not abused by malicious actors. The initiative had a two-year digital news literacy program to improve the ability of readers to evaluate information. It also features a new Cyber Hygiene Guide (Facebook Undated) and training program for all federal political parties and politicians. The company also said that a new cyber threats crisis email line will be provided for politicians and political parties in the event that their accounts are compromised.

Also, Facebook has stated that it is currently working on a series of measures to comply with changes to Canada’s election law. Kevin Chan, head of public policy for Facebook Canada, said in the spring that the company was at that time building its advertisement library that would be available in June, a few months ahead of the federal election. “The company is serious about trying to prevent foreign interference and about respecting recent changes to Canada’s elections law,” Chan added (Thompson 2019a).

Facebook has removed fake accounts from its platform, yet many pages and groups remain that promote narratives that amplify Russian and other malign foreign government propaganda.

Google

In a recent opinion piece, Google identified its own role as being to "organize the world's information and make it universally accessible and useful" (Gingras and McKay 2019). By defining itself in this way, it places enormous responsibility upon itself to ensure that its systems are not used to promote, amplify, or enable the spread of disinformation aimed at undermining our democracy.

Google has stated that it won't accept any political advertising during the election campaign (Cardoso 2019) because it would be too difficult for the company to comply with the law. Democratic Institutions Minister Karina Gould said that the government will try to convince Google to change its mind about refusing to run election advertising during the upcoming federal campaign (Thompson 2019b). Google Canada, however, responded by pointing to its team of people who are employed to "prevent abuse of our systems from bad actors," and also noted that Google is helping fund digital literacy initiatives (Gingras and McKay 2019).

It should be noted that known pro-Kremlin conspiracy theory media platforms, such as Global Research and Russia Insider, openly display ads from Google's Ad Choices on their websites; in turn, these ad services fund their activities. Google should reconsider its policies to ensure that such websites do not benefit from ad revenues. Google has stated that in the case of "malicious political-influence operations" it will "cut off advertising revenue, disable these accounts and share threat information with other companies and law-enforcement officials when appropriate" (Gingras and McKay 2019).

Recommendations

It is an unfortunate fact that malign foreign actors exploit our principles of free expression and open debate in efforts to divide, intimidate, and silence us. However, our responses to these dark forces must remain consistent with our democratic values and freedoms lest we resort to the same tactics as the dictators and authoritarians that seek to subvert our democracy. Ultimately, it is citizen awareness and the ability to consume information with a critical filter, in the form of media and cyber literacy, that will provide the most robust resilience against disinformation and influence campaigns. The tools to help citizens make informed decisions, to protect our information environment, and ultimately, our democracy, are not yet complete. The social and legal norms that guide traditional media have developed over a century, and we unfortunately do not have the same luxury of time when it comes to online and social media platforms. We must act quickly to establish these new norms.

Social media

A recent poll of Canadians found that a majority of Canadians – 52 percent – get their news from Twitter, Facebook, and Instagram (Sevunts 2019), and only one-third actually trust the news from these platforms. Yet, unlike traditional media companies, social media platforms have often failed at self-governing their behaviour – and they have often refused to take editorial responsibility for their content. There are also no regulations or laws that can ensure social media platforms are held accountable.

The power of social media platforms is well documented through their impact on events, both good and terrible. Government should work with social media companies to adopt appropriate policies that will help to assure trust among users and the general public in the role of these increasingly important platforms. The following recommendations should be considered:

- Require users to confirm their identity in order to use the social media platforms, which could potentially eliminate a large number of bot and troll accounts.
- Adjust social media algorithms to keep known foreign regime owned propaganda platforms off search listings and prevent them from receiving ad placement revenue (e.g., Google ad placements).
- Identify and label foreign propaganda, such as RT and PressTV broadcasting on YouTube, and ban them from generating revenue from advertising.
- Create a social media watchdog within existing federal communications regulator offices or ministries, where citizens can raise complaints and concerns.
- Adopt parts of the German model that requires social media platforms to remove hate messaging within 24 hours.
- Require social media providers to produce a report to Parliament about the disinformation operations they've identified on their platforms before and during the election period.

Security protocols

Drawing from US experience and lessons from the Baltic states, it is critical for western nations to ensure that their domestic political parties develop and deploy robust security protocols to protect supporter data. Political parties should voluntarily adopt the following measures:

- Apply two-factor authentication (2FA) for all email and database access – from national levels down to local electoral district campaigns and volunteers.
- Drawing from the Swedish example, require all campaign staff and volunteers to take mandatory cyber training to encourage good cyber practices – such as being able to identify potential phishing attacks and not opening incoming attachments from unknown email addresses.

Expanded international cooperation and solidarity

Canada's leadership in the G7 Rapid Response Mechanism is commendable but is limited. A much broader international response is required – one that includes Canada's NATO allies and recognizes that media and information are strategic assets. On the one hand, we need to ensure that NATO countries remain resilient to possible attacks on such assets in accordance with Article 3 of the Washington Treaty. On the other hand, NATO leaders have recently agreed that cyber attacks should be included under the Article 5, which states that an attack against one ally should be viewed as an attack against all allies. Member states are currently trying to ascertain when a cyber attack would trigger a response (Agence France-Presse 2018), though we can expect a certain amount of purposeful vagueness as well (Stoltenberg 2018). Still, we should be clear that attacks against our strategic assets, including our media and our democratic processes, could trigger a commensurate response under Article 5.

Such measures would send a strong message to Moscow, Beijing, Tehran, and other malign actors that NATO is taking the threat of disinformation and digital disruption of our democracies seriously. Furthermore, western nations should consider applying coordinated sanctions, using mechanisms such as Magnitsky sanctions, against foreign officials who lead state organs that engage in information warfare against western democracies, as well as their agents.

Most importantly, information about future and ongoing disinformation campaigns should not just be shared internally, but made public in a coordinated manner, so that citizens can make critical assessments about the news they receive and consume. In addition, the government should issue a stern warning to malign foreign actors that, if they attempt to influence or disrupt the election process, they will be identified and held responsible, and that reprisals could include targeted sanctions.

NATO Centers of Excellence

All NATO nations, including Canada, should also join and actively participate in NATO's Centers of Excellence (COE), especially those in the Baltic states. At the moment, Canada contributes to the Strategic Communications (StratCom) COE in Latvia and recently joined the Cooperative Cyber Defence COE in Estonia.

The Cooperative Cyber Defence COE is especially important, in so far as it helps NATO countries develop coordinated defences against both state and non-state cyber attacks targeting military and civilian infrastructure – including power, transportation, and other strategic infrastructure. Coordination of active offensive counter-measures that target and neutralize foreign cyber attackers, including Russia's APT28 and APT29, is required. Indeed, with Bill C-50 having received royal assent, such counter-measures will soon be an option for Canada.

Canada should also join the NATO Energy Security COE in Lithuania, which is meant to help develop coordinated energy security strategies. The Kremlin currently benefits from a dangerous monopoly in the European energy market. Canada has a potentially important role in that regard; Alberta oil and gas could provide a reliable alternative source of energy to our European allies.

Propaganda, disinformation and fake news

In May, UK Foreign Secretary Jeremy Hunt declared Russian state cable news outlet RT, "a weapon of disinformation." RT has been fined for violating UK broadcast regulations on a number of occasions – including 7 in the last year – for broadcasting false news. RT is central to Russia's manipulation of media and the spreading of "fake news" (Wintour and Waterson 2019). Britain's NATO and G7 allies should view all Russian and foreign propaganda through a similar lens and take the following measures to limit their citizens' exposure to it and raise public awareness when foreign disinformation attack narratives emerge:

- Canada should update CRTC policies and regulations to hold foreign cable news license holders accountable for propaganda and false news that are broadcast by channels to which they hold licenses, much like OFCOM in the UK.
- Just as programming with excessive violence, sex, and offensive language is labelled, so too should foreign propaganda.
- The Baltic states have demonstrated that publicly identifying and debunking news is an effective way of making the public aware of disinformation campaigns and discrediting them – Canada should consider doing the same.

- In France, *Le Monde* has created the Décodex project, which enables users to verify websites and social media profiles to check their legitimacy. Canadians would benefit from a similar website to filter out and check for conspiracy theory and pro-regime websites.

- Canada should support and promote the creation of civil society groups like the Lithuanian Elves (Weiss 2017), Estonia's Civil Defence group Propastop, and Latvia's investigative journalism portal RE:Baltica (RE:Baltica 2019).

- Canada should educate youth about how to detect disinformation and how to develop a critical lens through which to consume news and media, similar to the Swedish model where a popular children's cartoon character teaches children about disinformation (Roden 2017b).

- All political parties, their leaders, and candidates, should sign a code of conduct, pledging them to defend the integrity of the election by committing to not engage in disinformation or use bots to amplify messaging.

- The government should require intelligence agencies to produce a report about disinformation attacks and attempts to disrupt the election 30 days after the election, and develop legislation that would automatically apply sanctions against foreign governments that have engaged in such activity.

- Western governments should consider following the Baltic example of supporting existing domestic foreign-language television news and other third language media platforms in an effort to create credible alternatives to malign foreign state media broadcasts. In Canada, this would include networks such as OMNI.

- The federal government should fully implement Bill C-59, giving Canadian security agencies the means to actively defend against disinformation by having the capability to strike back against attackers.

Forgeries and deep fakes

The doctoring of images and forgery of documents isn't a new phenomenon. Josef Stalin regularly changed history by wiping out enemies both literally and in images (Blakemore 2018) and history books (RT 2009) by simply erasing them – a habit that remains with the Kremlin propagandists to this day. In 2015, for instance, the Kremlin created forged negative letters from leading Swedish cabinet ministers, which were then posted to social media and international media sites to create a negative impression of Sweden's foreign policy (The Local 2017b). In spring 2019, a similar situation emerged in Canada regarding a forged congratulatory letter from the Canadian prime minister to a questionable Tibetan group (Cole 2019).

Of greater concern is the emerging technological ability to seamlessly manipulate videos and audio to make it seem and sound like people are saying things they never said, also known as "deep fakes." Such technology could be used to affect major policy issues and elections. Spotting high quality deep fakes is currently very difficult without sophisticated software. Having said that,

- as soon as any such forgeries are discovered, they should be made public immediately – as was the case with the forged Canadian letter to the Tibetan group;

- Canadian security agencies must quickly research and address this emerging threat.

WHAT CITIZENS CAN DO

Before sharing news with exciting headlines on social media, check the source. If the headline sounds outrageous, the story could be fake. Search the title online to see if major, credible media is reporting on it. If they’re not, the story is probably fake.

Before the Internet, we trusted the news we read in major newspapers and magazines, and on broadcast news. Established media continue to have editorial policies that require reporters to verify facts for anything they report. Fly-by-night online platforms that generate revenue from clicks, issues-based websites, and foreign-sponsored media generally have no editorial policy, aside from generating as many viewers as possible, often with the intent of deceiving them. Most importantly, social media posts should never be considered credible sources of news, as the ultimate source of those reports can be obfuscated.

As a rule: always verify the source before reading and sharing.

The EU Eastern Stratcomm (EU vs. Disinfo 2019) has identified some warning indicators that media consumers can use to alert themselves to pro-Kremlin and other pro-foreign regime narratives:

Table 1: How To Identify Foreign Influence and Disinformation Campaigns?

Deflection & False Moral Equivalence

- Attempts to deflect and redirect debate by raising false moral equivalence. For example:

The Syrian White Helmets that Canada helped rescue are not heroes, but “contain numerous members who have participated in or supported criminal acts in Syria, including torture, assassinations, beheading, and kidnapping of civilians, as well as inciting Western military intervention in Syria” (Bartlett 2018).

OR

- Canada may not recognize Russia’s annexation of Crimea, but a referendum was held and “96% of the participants have voted to reunite with Russia… to the best of my recollection, I haven’t heard about a referendum in Kosovo” (Harris 2014).

OR

- How can Canada criticize foreign human rights abuses when “The streets are strewn with homeless” and “Canada is one of the world’s worst oppressors of women” (Hopper 2018).

Whitewashing

- Foreign regime aligned experts who use their credentials to promote pro-regime positions.

The EU vs. Disinfo (2019) defines a Kremlin whitewasher as “Someone who is sympathetic to the Kremlin and seeks to justify or excuse its bad behaviour at all costs, typically by blaming the West for alienating Russia and destroying the relationship. ‘Russia’s ‘aggression’ is simply a response to Western neoimperialism and the expansion of NATO!’”

Comments from Kremlin whitewashers can include such narratives as:

Canada and the West have provoked Russian aggression through the vast expansion of NATO and by spending billions stoking anti-Russian sentiment and regime change in Russia’s neighbourhood.

OR

Vladimir Putin is just a supporter of Russian national identity and a defender of Christian values. Does that make him a monster?

Aggressive Conflation

- Raising doubts about a policy position by implying a threat to random and unrelated issues. For instance, the Russian embassy reacted to Canada’s criticism of Russian involvement in the Skripal poisoning with the following Tweet:

“We regret PM Trudeau’s confrontational rhetoric at yesterday’s Toronto press-conference prompted by UK slanderous Russophobic hysteria. This language of ultimatums is totally unacceptable & counterproductive, especially for bilateral dialogue on important issues, like the Arctic” (Dickson, 2018).

The Grey Zone

- Prevarication on issues is often used to muddle obvious facts and truths.

  Such as the downing of Malaysian Airlines MH17 by a Russian supplied BuK missile:

  "...claim [that] the Russians were responsible was invented from the start" (Helmer 2019b).

OR

- The Russian initiated and supported war in Eastern Ukraine:

  "We need to step up concerted information and protest action that can help end Kyiv's carnage and shelling rampage in eastern Ukraine" (Annis 2014).

Conspiracy Theories

- Conspiracy theories are nearly impossible to debunk as any denial of their existence is further used as evidence of their existence by conspiracy theorists.

  These types of stories include those mentioning the Zionists, Deep State, LGBT lobby, Jewish Conspiracies, Aliens, The Elites, Antivaxx, etc., which should be viewed with healthy skepticism. As RT (Russia Today) itself reminds us with their slogan, "question everything" (Horner 2018).

Blame Fascism

- EU vs. Disinfo (2019) explains that "Russia's frequent invocations of fascism are the consequence of the national mythologisation of the unique role of the Soviet army in the victory over Nazi Germany in World War 2. Russia is still fighting that war to keep its own glory alive, and sees mythical fascists at every turn."
- Attempts have been made by foreign propagandists to discredit western leaders and entire communities with this label. Canadian Minister of Foreign Affairs, Chrystia Freeland was a target (Glavin 2017a, 2017b) as was former Estonian President, Toomas Hendrik Ilves (Estonian Internal Security Service 2018).

Conclusion

Warnings about Russian and other foreign disinformation that are intended to undermine our democracy and disrupt our elections are becoming increasingly common, from Europe to North America. Some western states have been conscious of these efforts for more than a decade while others are just waking up to the threats and would benefit from learning from those nations that have dedicated significant time and resources to developing defences against information warfare. Our allies in Eastern Europe and the Baltic Sea region have long been targets of Kremlin disinformation and propaganda. Canada could learn a lot from their experiences and knowledge as it works on developing a strategy to deal with this threat.

While not all threats to our democracies may initially be apparent or obvious, it does not mean that they are not present. The 2019 EU elections were an example: broad information warfare offensives have not yet been specifically identified, but Kremlin-linked activities were detected – such as those outlined in Estonia, which has seen the far-right party EKRE enter into a coalition government. Notably, this party is connected with the Kremlin-supported French National Rally party and promotes extremist views that align with the Kremlin's promotion of far-right extremist narratives, both at home and abroad.

Ultimately, a well informed and educated public, media, and policy-makers will provide the most resilient form of defence against foreign malign influence and disinformation campaigns. The public should be given the necessary tools and opportunities to enhance their ability to consume media with a critical eye, to check facts, and question the platforms that promote and amplify foreign disinformation and false narratives that are aimed at manipulating our views and undermining the stability of our democracy and society. However, it is important that efforts to educate and inform Canadians about disinformation campaigns are undertaken independently of government and that any efforts to inform the Canadian public about disinformation include independent, civil society experts.

The serious and real risk that one or more political parties will be baited by foreign disinformation must also be further addressed by building and reinforcing trust among political parties through regular, scheduled dialogue and the transparent sharing of information about disinformation campaigns.

As we have witnessed in many other states, interference and disruption of our media and information environment can have serious adverse effects on our democracy and society. Canada should clearly define our information environment as a strategic asset, and just as NATO regards cyber attacks against member state infrastructure as an Article 5 attack, so should Canada see disinformation and foreign interference attacks in the same way. By ensuring that malign foreign states pay the consequences and potential cost for their actions, we may hold them accountable and deter them from engaging in such actions. Finally, Canada should expand its cooperation on disinformation and digital foreign interference beyond the G7 to include a broader range of allies, specifically those in NATO as well as non-NATO partners in the Baltic Sea region, such as Sweden and Finland.

Canadians can take comfort in the fact that the government has developed a plan to address the threat of foreign disinformation. However, we must also learn from the lessons of our allies – including the Baltic states, Sweden, France, Germany, and others – and apply those lessons to the further expansion and implementation of our strategies.

About the Authors

Marcus Kolga is a Senior Fellow at the Macdonald-Laurier Institute's Centre for Advancing Canada's Interests Abroad. He is an international award-winning documentary filmmaker, journalist, digital communications strategist, and a leading Canadian expert on Russian and Central and Eastern European issues.

Marcus has a focus on communications and media strategies as tools of foreign policy and defence, and continues to write commentary for national and international media including the *Globe and Mail* and *Toronto Star*. He is the co-founder and publisher of UpNorth.eu, an online magazine that features analysis and political and cultural news from the Nordic and Baltic region. He frequently comments on Russian, Eastern and Central European issues on North American radio and television and at foreign policy conferences.

Marcus is involved with international human rights organizations and national political organizations. In 2008 he spearheaded an effort to make August 23rd, the anniversary of the Molotov-Ribbentrop Pact, a Canadian national day of remembrance for the European victims of Nazism and communism – Black Ribbon Day – by drafting a parliamentary resolution that was introduced and passed by Hon. Bob Rae. In 2015, Marcus was awarded the Estonian Order of the White Star by President Toomas Hendrik Ilves.

Jakub Janda is Head of the Kremlin Watch Program and Director of the European Values Think-Tank based in Prague. He specializes in response of democratic states to hostile disinformation and influence operations. He is Associate Fellow at Slovak Security Policy Institute and regular contributor for the Atlantic Council. He serves a member of Editorial Board of expert portal AntiPropaganda.sk and as a proud member of Active Reserves of the Czech Armed Forces. In 2016 - 2017, he was tasked by Czech security and intelligence institutions to consult on "Influence of Foreign Powers" chapter within Audit of National Security conducted by the Czech government, where he was involved in the Czech policy shift on this issue. Since 2019, he serves as a member of Programming Board of the Centre Anne de Kyiv. Since 2015, he was asked to provide briefings or trainings in more than 20 countries. In the past he worked for humanitarian agency ADRA International and for a Member of the Czech Parliament.

Nathalie Vogel is a Non-Resident Senior Fellow with the Kremlin Watch Program. She has dedicated her career to the defence and the promotion of democracy and democratic movements around the world. A graduate of the Institute of Political Sciences of the University of Innsbruck, Nathalie taught international relations at the University of Bonn, Germany. She has served as a project officer and consultant for youth and civil society at the NATO Office in Moscow. Until 2015, Nathalie Vogel was a Fellow at the Institute of World Politics in Washington DC and worked as a contractor with the USG. She is a political consultant for youth branches of political parties and student movements in the Balkans, Eastern Europe and Latin America, and serves as an advisor to several think tanks in Central Eastern Europe, Latin America and the Caucasus. Nathalie has been monitoring influence operations in Germany since 2007 and advises lawmakers and think tanks. She is a reserve Officer in the German AF.

References

Agence France-Presse. 2018. “NATO Should Adopt Hybrid Warfare Trigger: Special Rapporteur.” Shephard Media, May 28. Available at https://www.shephardmedia.com/news/defence-notes/nato-should-adopt-hybrid-warfare-trigger-special-r/.

Annis, Roger. 2019. “Can Kyiv sustain its war in eastern Ukraine? The view from Canada.” *rabble.ca*, July 25. Available at rabble.ca/blogs/bloggers/roger-annis/2014/07/can-kyiv-sustain-its-war-eastern-ukraine-view-canada.

Babalich, Igor. 2017. “Appeal to Prime Minister Trudeau to question Minister Freeland’s integrity.” Russian Congress of Canada, March 21. Available at https://russiancongresscanada.org/geopolitics-en/appeal-to-prime-minister-trudeau-to-question-minister-freelands-integrity/.

Bartlett, Eva. 2018. “Decision to bring White Helmets to Canada dangerous and criminal.” RT, August 10. Available at https://www.rt.com/op-ed/435670-white-helmets-canada-syria/.

BBC. 2018. “Germany Starts Enforcing Hate Speech Law.” *BBC News*, January 1. Available at http://www.bbc.com/news/technology-42510868.

Blakemore, Erin. 2018. “How Photos Became a Weapon in Stalin’s Great Purge.” *History*, April 20. Available at https://www.history.com/news/josef-stalin-great-purge-photo-retouching.

Brattberg, Erik, and Tim Maurer. 2018. *Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks*. Carnegie Endowment for International Peace, May 23. Available at https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

Brown, Chris. 2017. “Anti-Canada Propaganda Greets Troops in Latvia.” CBC, June 16. Available at https://www.cbc.ca/news/world/latvia-propaganda-1.4162612.

Brown, Chris. 2019. “Top Russian News Host Takes Aim at Ukrainian Canadians.” CBC, January 17. Available at https://www.cbc.ca/news/world/top-russian-news-host-takes-aim-at-ukrainian-canadians-1.4980859.

Bulckaert, Ninon. 2018. “How France Successfully Countered Russian Interference during the Presidential Election.” Freya Kirk, tr. *Euractiv*, July 17. Available at https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/.

Bundesministerium der Verteidigung. 2019. “BMVg und BMI geben Standort für neue Cyberagentur bekannt.” Bundesministerium der Verteidigung, January 31. Available at https://www.bmvg.de/de/aktuelles/standort-fuer-neue-cyberagentur-30534.

Canada. 2019a. “Safeguarding Elections.” *Democratic Institutions*. Government of Canada. Available at https://www.canada.ca/en/democratic-institutions/news/2019/01/safeguarding-elections.html.

Canada. 2019b. “Budget 2019: Chapter 4: Delivering Real Change.” Government of Canada. Available at https://www.budget.gc.ca/2019/docs/plan/chap-04-en.html?wbdisable=true.

Cardoso, Tom. 2019. "Google to Ban Political Ads Ahead of Federal Election, Citing New Transparency Rules." *Globe and Mail*, March 5. Available at https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/.

Carley, Michael Jabara. 2017. "Chrystia Freeland: Kiev's Minister of Foreign Affairs in Ottawa." Russian Congress of Canada, January 23. Available at https://russiancongresscanada.org/geopolitics-en/chrystia-freeland-kievs-minister-of-foreign-affairs-in-ottawa/.

Chyczij, Alexandra. 2019. "Canada Is a Target of Russia's Disinformation. Let's Be Ready – The Hill Times." Ukrainian Canadian Congress, January 30. Available at https://ucc.ca/2019/01/30/canada-is-a-target-of-russias-disinformation-lets-be-ready-the-hill-times/.

Cole, J. Michael. 2019. "Pro-Beijing Tibetan Group Hints at China's Influence Operations in Canada. *Inside Policy*, April 26. Macdonald-Laurier Institute. Available at https://www.macdonaldlaurier.ca/pro-beijing-tibetan-group-hints-chinas-influence-operations-canada-j-michael-cole-inside-policy/.

Colliver, Chloe, Peter Pomerantsev, Anne Applebaum, and Jonathan Birdwell. 2018. *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election*. Institute of Global Affairs, October. Available at https://www.isdglobal.org/wp-content/uploads/2018/11/Smearing-Sweden.pdf.

Communications Security Establishment [CSE]. 2019. *Foreign Cyber Operations*. Government of Canada. Available at https://www.cse-cst.gc.ca/en/cse-act-loi-cst/cyberop.

Dagens Nyheter. 2017. "New Study: Russian Spread of Fake News in Sweden Is Increasing." *Dagens Nyheter*, January 7. Available at http://www.dn.se/nyheter/sverige/ny-studie-rysk-spridning-av-falska-nyheter-i-sverige-okar/.

Dearden, Lizzie. 2017. "Nato Intercepting Highest Number of Russian Military Planes since the Cold War as 780 Incidents Recorded in 2016." *Independent*, April 22. Available at https://www.independent.co.uk/news/world/europe/nato-russian-planes-intercepted-eu-europe-fighter-jets-scrambled-bombers-raf-typhoons-alaska-putin-a7696561.html.

Denisenko, Viktor. 2018. *Lithuania: Disinformation Resilience Index*. Ukrainian Prism Foreign Policy Council. Available at http://prismua.org/en/9065-2/.

Deutscher Bundestag. 2019a. "Meinungsbildung und Meinungsmanipulation liegen oft eng beieinander." Deutscher Bundestag. Available at https://www.bundestag.de/dokumente/textarchiv/2019/kw15-pa-digitale-agenda-633610.

Deutscher Bundestag. 2019b. "Öffentliche Anhörungen zum Thema 'Resilienz von Demokratien im digitalen Zeitalter im Kontext der Europawahl'." Deutscher Bundestag. Available at https://www.bundestag.de/ausschuesse/a23_digital/anhoerungen#url=L2F1c3NjaHVlc3NlL2EyM19kaWdpdGFsL2FuaG9lcnVuZ2VuL2FuaG9lcnVuZy01OTIzNzA=&mod=mod557988.

Dickey, Christopher. 2017. "Fighting Back Against Putin's Hackers." *Daily Beast*, May 5. Available at https://www.thedailybeast.com/fighting-back-against-putins-hackers.

Dickson, Janice. 2018. "Trudeau's Putin Comments 'Counterproductive': Russian Embassy." *iPolitics*, March 22. Available at https://ipolitics.ca/2018/03/22/trudeaus-putin-comments-counterproductive-russian-embassy/.

Digital Forensic Research Lab [DFRLab]. 2018a. "#BalticBrief: Vesti Investing in Pro-Kremlin Audience Online." DFRLab, February 11. Available at https://medium.com/dfrlab/balticbrief-vesti-investing-in-pro-kremlin-audience-online-8198de3c7049.

Digital Forensic Research Lab [DFRLab]. 2018b. *#ElectionWatch: The 'Russian Factor' Government in Latvian Elections*. DFRLab, October 7. Available at https://medium.com/dfrlab/electionwatch-the-russian-factor-in-latvian-elections-56d3f3270d66.

Dorell, Oren. 2018. "Tiny Latvia can teach the U.S. a lesson or two about Russian meddling." *USA Today*, March 7. Available at https://www.wkyc.com/article/news/nation-now/tiny-latvia-can-teach-the-us-a-lesson-or-two-about-russian-meddling/465-845bd58f-8f9f-426c-88d9-2911a49c2ee7.

Eglitis, Aaron. 2018. "How to Russia-Proof an Election." *Bloomberg*, September 20. Available at https://www.bloomberg.com/news/articles/2018-09-21/hacks-phishing-and-fake-news-russia-proofing-a-baltic-election.

Estonia, Ministry of Defence. 2011. *National Defence Strategy: Estonia*. Government of Estonia. Available at http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

Estonian Internal Security Service. 2018. *Annual Review 2018*. Estonian Internal Security Service Available at https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202018.pdf.

European Integration Studies Centre [EISC]. 2018. *Lithuanian-Swedish Roundtable Expert Discussions on Social Resilience and Psychological Defence: Policy Brief*. EISC. Available at http://www.eisc.lt/uploads/documents/files/EISC_policy%20brief(1).pdf.

EU vs. Disinfo. 2019. "What Can You Do? – Watch Out for These Warning Signs." EU vs. Disinfo, April 2. Available at https://euvsdisinfo.eu/what-can-you-do/.

Facebook. Undated. *Doing Our Part to Protect and Safeguard the Integrity of Elections*. Facebook, Canadian Election Integrity Initiative. Available at http://facebookcanadianelectionintegrityinitiative.com/.

Fried, Daniel, and Alina Polyakova. 2018. *Democratic Defense Against Disinformation*. Atlantic Council, March 5. Available at https://www.atlanticcouncil.org/publications/reports/democratic-defense-against-disinformation.

Funke, Daniel. 2018. "Here's what the world is doing to tackle fake news. India can learn." *The Print*, July 25. Available at https://theprint.in/opinion/heres-what-the-world-is-doing-to-tackle-fake-news-india-can-learn/88195/.

Galano, Juvien. 2019. "i-Voting – the Future of Elections?" e-Estonia, March. Available at https://e-estonia.com/i-voting-the-future-of-elections/.

Galeotti, Mark. 2019. "Russian Intelligence Operations Shifting Tactics Not Goals." *NATO Review Magazine*, April 26. Available at https://www.nato.int/docu/review/2019/Also-in-2019/russian-intelligence-operations-shifting-tactics-not-goals/EN/index.htm.

Germany, Federal Foreign Office. 2018. "Fake News, Bots and Provocative Statements – Disinformation on the Internet." Government of Germany. Available at https://www.auswaertiges-amt.de/en/aussenpolitik/themen/disinformation-on-the-internet/2125634.

Germany, Federal Republic. Undated. "Article 87a [Armed Forces]" and "Article 87b [Federal Defence Administration]." *Basic Law for the Federal Republic of Germany*. Government of Germany. Available at https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0458.

Gingras, Richard, and Colin McKay. 2019. "Fake News is Bad for Canadians and Google Alike – and Here's How We'll Fight It." *Globe and Mail*, May 2. Available at https://www.theglobeandmail.com/opinion/article-fake-news-is-bad-for-canadians-and-google-alike-and-heres-how-well/.

Glavin, Terry. 2017a. "Enter the Freeland-Nazi Conspiracy—and the Amping-up of Russia's Mischief in Canada." *National Post*, March 8. Available at https://nationalpost.com/opinion/terry-glavin-enter-the-freeland-nazi-conspiracy-and-the-amping-up-of-russias-mischief-in-canada.

Glavin, Terry. 2017b. "How Russia's Attack on Freeland Got Traction in Canada." *Maclean's*, March 14. Available at https://www.macleans.ca/politics/how-russias-attack-on-freeland-got-traction-in-canada/.

Harris, Kathleen. 2014. "Ambassador Alexander Darchiev: 'Crimea is Russia - once and forever.'" CBC, December 22. Available at https://www.cbc.ca/news/politics/ambassador-alexander-darchiev-crimea-is-russia-once-and-forever-1.2881847.

Helmer, John. 2019a. "Ukraine's Anti-Globalist Vote Bad News for Canada's Russia Hating Foreign Minister Freeland." Russia Insider, April 25. Available at https://russia-insider.com/en/ukraines-anti-globalist-vote-bad-news-canadas-russia-hating-foreign-minister-freeland/ri26857.

Helmer, John. 2019b. "Malaysian Prime Minister Mahathir accuses US and allies of MH17 fabrication, violation of rule of law." *Dances with Bears*, June 4. Available at johnhelmer.net/malaysian-prime-minister-mahatir-accuses-us-and-allies-of-mh17-fabrication-violation-of-rule-of-law/.

Higgins, Andrew. 2015. "Latvian Region Has Distinct Identity, and Allure for Russia." *New York Times*, May 20. Available at https://www.nytimes.com/2015/05/21/world/europe/latvian-region-has-distinct-identity-and-allure-for-russia.html.

Hopper, Tristan. 2018. "Canada is the world's worst oppressor of women': Saudi Arabia's bizarre propaganda campaign." *National Post*, August 10. Available at https://nationalpost.com/news/canada/saudi-arabias-bizarre-propaganda-campaign-against-canada.

Horner, Tommy. 2018. "Russia's RT is contesting the very meaning of 'truth.'" *America Abroad*, May 11. Available at https://www.pri.org/stories/2018-05-11/russias-rt-contesting-very-meaning-truth.

Ilves, Toomas Hendrik. 2019. Personal communication. July 23, 2019.

Independent. 2018. "Macron Proposes Anti-Fake News Election Law." *Independent*, January 4. Available at https://www.independent.co.uk/news/world/europe/macron-fake-news-law-elections-facebook-social-media-a8140721.html.

Janda, Jakub, and Veronika Víchová. 2017. "Germany's Key Role in Fighting Kremlin Subversion in Europe." Atlantic Council, August 3. Available at https://www.atlanticcouncil.org/blogs/ukrainealert/germany-s-key-role-in-fighting-kremlin-subversion-in-europe.

Justice Laws Website. 2018. "Prohibition on Use of Foreign Funds by Third Parties." *An Act to Amend the Canada Elections Act and Other Acts and to Make Certain Consequential Amendments*. Statutes of Canada (2018), Chapter 31 (Bill C-76). 1st Sess., 42nd Parl. Government of Canada. Available at https://laws-lois.justice.gc.ca/eng/annualstatutes/2018_31/page-26.html.

Kolga, Marcus. 2019a. "Russian Disinformation Is Attacking Our Democracy and Making Us Sick." *Toronto Star*, February 21. Available at https://www.macdonaldlaurier.ca/russian-disinformation-attacking-democracy-making-us-sick-marcus-kolga-toronto-star/.

Kolga, Marcus. 2019b. "Canada's Plan to Counter Foreign Interference Is a Good Start, but the Work's Not Done." *Globe and Mail*, February 8. Available at https://www.macdonaldlaurier.ca/canadas-plan-counter-foreign-interference-good-start-works-not-done-marcus-kolga-globe-mail/.

Kolga, Marcus. 2019c. "Russian Disinformation is Attacking Our Democracy and Making us Sick." *The Star*, February 21. Available at https://www.thestar.com/opinion/contributors/2019/02/21/russian-disinformation-is-attacking-our-democracy-and-making-us-sick.html.

Kremlin Watch. 2018. *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations*. Kremlin Watch, June 13. Available at https://www.kremlinwatch.eu/countries-compared-states/eu/.

Kremlin Watch. 2019. *Sweden*. Kremlin Watch. Available at https://www.kremlinwatch.eu/countries-compared-states/sweden/.

Król, Aleksander. 2017. "Russian Information Warfare in the Baltic States — Resources and Aims." *Warsaw Institute Review*, July 20. Available at https://warsawinstitute.org/russian-information-warfare-baltic-states-resources-aims/.

Lister, Tim, Sebastian Shukla, and Nima Elbagir. 2019. "Fake News and Public Executions: Documents Show a Russian Company's Plan for Quelling Protests in Sudan." CNN, April 25. Available at https://www.cnn.com/2019/04/25/africa/russia-sudan-minvest-plan-to-quell-protests-intl/index.html.

The Local. 2016. "Russia Biggest Source of Cyberattacks on Sweden: Intelligence Head." *The Local (Sweden)*, December 12. Available at https://www.thelocal.se/20161212/russia-biggest-source-of-cyberattacks-on-sweden-intelligence-head.

The Local. 2017a. "Swedish PM 'Can't Rule Out' Russian Interference in Swedish Elections." *The Local (Sweden)*, January 9. Available at https://www.thelocal.se/20170109/sweden-pm-cant-rule-out-russian-interference-in-swedish-elections.

The Local. 2017b. "Russia Spreading Fake News and Forged Docs in Sweden: Report." *The Local (Sweden)*, January 7. Available at https://www.thelocal.se/20170107/swedish-think-tank-details-russian-disinformation-in-new-study.

The Local. 2018. "Justice Minister Falls Victim to Own Social Media 'Censorship' Law." *The Local (Germany)*, January 8. Available at https://www.thelocal.de/20180108/justice-minister-falls-victim-to-own-social-media-censorship-law.

Lum, Zi-Ann. 2019. "Gould 'Not Feeling Great' About Social Media Giants' Response To Election Meddling Fears." *HuffPost*, April 8. Available at https://www.huffingtonpost.ca/2019/04/08/canada-elections-foreign-interference_a_23708335/.

Matishak, Martin. 2017. "NSA Chief: U.S. Warned France about Russian Hacks before Macron Leak." *Politico*, May 9. Available at https://www.politico.com/story/2017/05/09/us-warned-france-russia-hacking-238152.

McAuley, James. 2017. "France Starts Probing 'Massive' Hack of Emails and Documents Reported by Macron Campaign." *Washington Post*, May 6. Available at https://www.washingtonpost.com/world/macrons-campaign-says-it-has-been-hit-by-massive-hack-of-emails-and-documents/2017/05/05/fc638f18-3020-11e7-a335-fa0ae1940305_story.

Nachetoi, Yury. 2019. "Growing prestige of the Russian community in the eyes of the rest of Toronto's communities." *Facebook*, May 11, 9:33 a.m. Available at https://www.facebook.com/photo.php?fbid=132373994603037&set=a.111556480018122&type=3&theater.

Ottis, Rain. Undated. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Estonia, Cooperative Cyber Defence Centre of Excellence. Available at https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Owen, Laura Hazard. 2017. "After a Rocky Reception, *Le Monde*'s Décodex is Almost a Year into Fighting *Intox* (Fake News) in France." NiemanLab, November 30. Available at https://www.niemanlab.org/2017/11/after-a-rocky-reception-le-mondes-decodex-is-almost-a-year-into-fighting-intox-fake-news-in-france/.

Past, Liisa, and Keith Brown. 2019a. "Estonia Is Winning the Cyber War Against Election Meddling." *Quartz*, March 28. Available at https://qz.com/1582916/estonia-is-winning-the-cyber-war-against-election-meddling/.

Past, Liisa, and Keith Brown. 2019b. "Attacks against Elections Are Inevitable – Estonia Shows What Can Be Done." *The Conversation*, March 3. Available at http://theconversation.com/attacks-against-elections-are-inevitable-estonia-shows-what-can-be-done-109222.

Peel, Michael. 2019. "Fake News: How Lithuania's 'Elves' Take on Russian Trolls." *Financial Times*, February 4. Available at https://www.ft.com/content/b3701b12-2544-11e9-b329-c7e6ceb5ffdf.

Propastop. Undated. Blog. Available at https://www.propastop.org/eng/

Re:Baltica. 2019. "Re:Baltica Launches Fact-Checking and Social Media Research Lab Re:Check." Re:Baltica, June 28. Available at https://en.rebaltica.lv/2019/06/rebaltica-launches-fact-checking-and-social-media-research-lab-recheck/.

Reuters. 2018. "German Hate Speech Law Tested as Twitter Blocks Satire Account." *Reuters*, January 3. Available at https://www.reuters.com/article/us-germany-hatecrime/german-hate-speech-law-tested-as-twitter-blocks-satire-account-idUSKBN1ES1AT.

Reuters in Berlin. 2015. "NSA Tapped German Chancellery for Decades, WikiLeaks Claims." *The Guardian*, July 8. Available at https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel.

Robertson, Susan Krashinsky. 2017. "Canadian TV Providers Being Paid to Carry Russian 'Propaganda Machine'." *Report on Business. Globe and Mail*, December 21. Available at https://www.theglobeandmail.com/report-on-business/canadian-tv-providers-receive-payments-to-carry-russian-propaganda-machine/article37400743/.

Roden, Lee. 2017b. "Why This Swedish Comic Hero Is Going to Teach Kids About Fake News." *The Local (Sweden)*, January 17. Available at https://www.thelocal.se/20170116/why-this-swedish-comic-hero-is-going-to-teach-kids-about-fake-news-bamse

Roonemaa, Holger and Inga Springe. 2018. "Moscow's Mouthpieces." Re:Baltica, August 28. Available at https://en.rebaltica.lv/2018/08/moscows-mouthpieces/.

Rosenberg, David. 2017. "France Bars Publication of Hacked Macron Emails Ahead of Vote." *Israel National News*, July 5. Available at http://www.israelnationalnews.com/News/News.aspx/229245.

Russia Today [RT]. 2009. "'Estonia has an Apartheid Regime.'" *Russia Today*, May 26. Available at https://www.rt.com/russia/estonia-has-an-apartheid-regime/.

Russkiy Mir Foundation. Undated. "Russkiy Mir Foundation Created Pursuant to a Decree of the President of the Russian Federation, Vladimir Putin, on June 21, 2007." Russkiy Mir Foundation. Available at https://russkiymir.ru/en/fund/index.php.

Ruus, Kertu. 2008. "Cyber War I: Estonia Attacked from Russia." *European Affairs*, 9, 1-2 (Winter/Spring). Available at https://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

Sarlo, Alexandra Wiktorek. 2017. *Fighting Disinformation in the Baltic States*. Foreign Policy Resarch Institute, July 6. Available at https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/.

Serhan, Yasmeen. 2017. "Macron, Standing Alongside Putin, Says Russian Media Spread 'Falsehoods'." *The Atlantic*, May 30. Available at https://www.theatlantic.com/news/archive/2017/05/macron-rt-supnik-are-agents-of-influence/528480/.

Sevunts, Levon. 2019. "Canadians Get News from Social Media but Don't Trust It: Poll." Radio Canada International, April 9. Available at http://www.rcinet.ca/en/2019/04/09/canadians-social-media-news-poll/.

Springe, Inga. 2017. "How Russian Propaganda Becomes Even Nastier in Baltic News." Re:Baltica, March 29. Available at https://en.rebaltica.lv/2017/03/how-russian-propaganda-becomes-even-nastier-in-baltic-news/.

Standish, Reid. 2017. "The Ominous, Massive Military Exercises in Eastern Europe." *The Atlantic*, September 18. Available at https://www.theatlantic.com/international/archive/2017/09/zapad-russia-baltics-lithuania-estonia-finland-trumpnato-eu/540126/.

Stelzenmüller, Constanze. 2017. *The Impact of Russian Interference on Germany's 2017 Elections*. Brookings Institution, June 28. Available at https://www.intelligence.senate.gov/sites/default/files/documents/sfr-cstelzenmuller-062817b.pdf.

Stoltenberg, Jens. 2018. “Stoltenberg Provides Details of NATO’s Cyber Policy.” Atlantic Council, May 16. Available at https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy.

SVT Nyheter. 2016. “Must-chefen pekar ut Ryssland som it-hot.” *SVT Nyheter*, December 11. Available at https://www.svt.se/nyheter/inrikes/must-chefen-den-aktor-vi-framfor-allt-ser-ar-ryssland.

Sytas, Andrius. 2019. “Lithuania Fears Russia will Attempt to Sway Its Elections.” Reuters, February 5. Available at https://www.reuters.com/article/us-lithuania-russia-cyber/lithuania-fears-russia-will-attempt-to-sway-its-elections-idUSKCN1PU1O3.

Tamkin, Emily. 2017. “10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?” *Foreign Policy*, April 27. Available at https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

Taylor, Adam. 2018. “Putin Says He Wishes the Soviet Union Had Not Collapsed. Many Russians Agree.” *Washington Post*, March 3. Available at https://www.washingtonpost.com/news/worldviews/wp/2018/03/03/putin-says-he-wishes-he-could-change-the-collapse-of-the-soviet-union-many-russians-agree/.

Teperik, Dmitri. 2019. “Who Benefits from Our Communications Illiteracy?” *Blog*, January 30. International Centre for Defence and Security [ICDS]. Available at https://icds.ee/who-benefits-from-our-communications-illiteracy/.

Thomasson, Emma. 2018. “Germany Looks to Revise Social Media Law as Europe Watches.” Reuters, March 8. Available at https://www.reuters.com/article/us-germany-hatespeech/germany-looks-to-revise-social-media-law-as-europe-watches-idUSKCN1GK1BN.

Thompson, Elizabeth. 2019a. “Facebook Introducing Measures to Prevent Election Disruption.” CBC, March 18. Available at https://www.cbc.ca/news/politics/facebook-canadian-election-interference-1.5059626.

Thompson, Elizabeth. 2019b. “Gould Wants Google to Change Its Mind About Refusing Election Ads.” CBC, March 6. Available at https://www.cbc.ca/news/politics/google-election-advertising-gould-1.5044364.

Tunney, Catharine. 2019. “Canada’s National Security Landscape Will Get a Major Overhaul This Summer.” CBC, June 23. Available at https://www.cbc.ca/news/politics/bill-c59-national-security-passed-1.5182948.

Ukrainian Canadian Congress. 2019. “Statement on Ontario Bill 97 and Holodomor.” Ukrainian Canadian Congress, May 11. Available at https://ucc.ca/2019/05/11/statement-of-ontario-bill-97-and-holodomor/.

United States Senate, Committee on Foreign Relations. 2018. *Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security.* Minority Staff Report. One Hundred Fifteenth Congress, Second Session, January 10. Available at https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

Vahtla, Aili. 2019. “Sinisalu: Russia trying to influence Estonia via Western countries.” ERR, March 6. Available at https://news.err.ee/917155/sinisalu-russia-trying-to-influence-estonia-via-western-countries.

Vilmer, Jean-Baptiste Jeangène. 2018. *Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks*. Centre for Strategic and International Studies [CSIS], June. Available at https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

Virani, Arif. 2019. "Alarm at fake letter of support from prime minister." *Facebook*, April 23. 4:33 p.m. Available at https://www.facebook.com/ArifViraniMP/photos/a.1451944955032239/2562200950673295/?type=3&theater.

Wasserman, Anatoly. 2017. "Memo for Latvians: Before You Refuse a NATO Soldier, Think Twice." *Sputnik News*, June 20. Available at https://lv.sputniknews.ru/columnists/20170620/5093872/anatolij-vasserman-pamjatka-latyshkam-pribytie-soldat-nato.html.

Weeks, Carly. 2019. "Mother Whose Son Died of the Flu Says She's become a Target of Anti-Vaccine Groups on Facebook." *Globe and Mail*, April 30. Available at https://www.theglobeandmail.com/canada/article-mother-whose-son-died-of-the-flu-says-shes-become-a-target-of-anti/.

Weiss, Michael. 2017. "The Baltic Elves Taking on Pro-Russian Trolls." *Daily Beast*, April 13. Available at https://www.thedailybeast.com/the-baltic-elves-taking-on-pro-russian-trolls.

Wintour, Patrick, and Jim Waterson. 2019. "Jeremy Hunt: Russian TV Station a 'Weapon of Disinformation'." *The Guardian*, May 1. Available at https://www.theguardian.com/media/2019/may/01/jeremy-hunt-russian-tv-station-a-weapon-of-disinformation.

Endnotes

[1] The campaign was indeed well-coordinated in terms of messaging and props, but the efforts were local, and the effects marginal. Moreover, vigilant citizens reported the campaign to the police almost immediately.

[2] Alternative for Sweden got less than one percent of the vote. The Neo-Nazis (NMR, the Nordic Resistance Movement), which is considered pro-Kremlin, got less than 1,000 votes.

[3] It can be argued that Russia focused on the most cost effective engagement: interfering in the US midterms. Even the Latvian elections saw little engagement from the Kremlin besides the standard agitition aimed at the Russian-speaking population.

[4] Prior to the EU elections in May, Russia conducted influence activities aimed at migration: specifically, a string of narratives designed such that the pro-Russian and western alt-right sources supported and amplified each other's rhetoric.

MLI

True North in
Canadian public policy

Critically Acclaimed, Award-Winning Institute

The Macdonald-Laurier Institute fills a gap in Canada's democratic infrastructure by focusing our work on the full range of issues that fall under Ottawa's jurisdiction.

- One of the top five think tanks in Canada and No. 1 in Ottawa according to the University of Pennsylvania.
- Cited by five present and former Canadian Prime Ministers, as well as by David Cameron, the British Prime Minister.
- First book, *The Canadian Century: Moving out of America's Shadow*, won the Sir Antony Fisher International Memorial Award in 2011.
- *Hill Times* says Brian Lee Crowley is one of the 100 most influential people in Ottawa.
- The *Wall Street Journal*, the *Economist*, the *Globe and Mail*, the *National Post* and many other leading national and international publications have quoted the Institute's work.

"The study by Brian Lee Crowley and Ken Coates is a 'home run'. The analysis by Douglas Bland will make many uncomfortable but it is a wake up call that must be read."
former Canadian Prime Minister Paul Martin on MLI's project on Aboriginal people and the natural resource economy.

Ideas Change the World

Independent and non-partisan, the Macdonald-Laurier Institute is increasingly recognized as the thought leader on national issues in Canada, prodding governments, opinion leaders and the general public to accept nothing but the very best public policy solutions for the challenges Canada faces.

Where You've Seen Us

CTV

cpac FOR THE RECORD

corus ENTERTAINMENT

CBC news

FP Foreign Policy

tvo

The Economist

WALL STREET JOURNAL

THE HILL TIMES

THE GLOBE AND MAIL
CANADA'S NATIONAL NEWSPAPER • FOUNDED 1844

NATIONAL POST

For more information visit: www.MacdonaldLaurier.ca

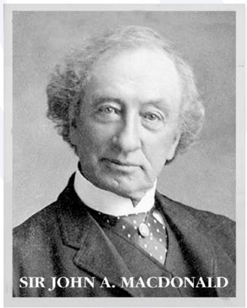
About the Macdonald-Laurier Institute

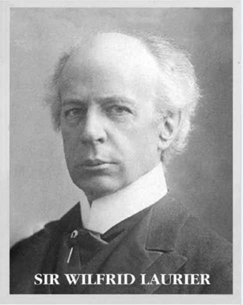
What Do We Do?

When you change how people think, you change what they want and how they act. That is why thought leadership is essential in every field. At MLI, we strip away the complexity that makes policy issues unintelligible and present them in a way that leads to action, to better quality policy decisions, to more effective government, and to a more focused pursuit of the national interest of all Canadians. MLI is the only non-partisan, independent national public policy think tank based in Ottawa that focuses on the full range of issues that fall under the jurisdiction of the federal government.

What Is in a Name?

The Macdonald-Laurier Institute exists not merely to burnish the splendid legacy of two towering figures in Canadian history – Sir John A. Macdonald and Sir Wilfrid Laurier – but to renew that legacy. A Tory and a Grit, an English speaker and a French speaker – these two men represent the very best of Canada's fine political tradition. As prime minister, each championed the values that led to Canada assuming her place as one of the world's leading democracies. We will continue to vigorously uphold these values, the cornerstones of our nation.


SIR JOHN A. MACDONALD


SIR WILFRID LAURIER

Working for a Better Canada

Good policy doesn't just happen; it requires good ideas, hard work, and being in the right place at the right time. In other words, it requires MLI. We pride ourselves on independence, and accept no funding from the government for our research. If you value our work and if you believe in the possibility of a better Canada, consider making a tax-deductible donation. The Macdonald-Laurier Institute is a registered charity.

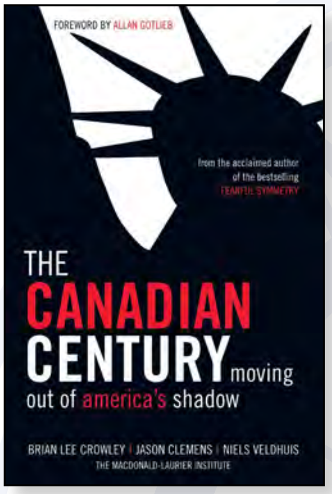
Our Issues

The Institute undertakes an impressive program of thought leadership on public policy. Some of the issues we have tackled recently include:

- Aboriginal people and the management of our natural resources;
- Making Canada's justice system more fair and efficient;
- Defending Canada's innovators and creators;
- Controlling government debt at all levels;
- Advancing Canada's interests abroad;
- Ottawa's regulation of foreign investment; and
- How to fix Canadian health care.

For more information visit: www.MacdonaldLaurier.ca

Macdonald-Laurier Institute Publications


FOREWORD BY ALLAN GOTLIEB
from the acclaimed author of the bestselling FEARFUL SYMMETRY
THE CANADIAN CENTURY moving out of america's shadow
BRIAN LEE CROWLEY | JASON CLEMENS | NIELS VELDHUIS
THE MACDONALD-LAURIER INSTITUTE

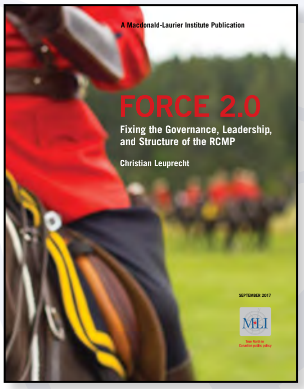
Winner of the Sir Antony Fisher International Memorial Award BEST THINK TANK BOOK IN 2011, as awarded by the Atlas Economic Research Foundation.

The Canadian Century
By Brian Lee Crowley,
Jason Clemens, and Niels Veldhuis

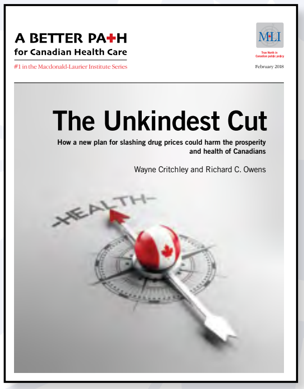
Do you want to be first to hear about new policy initiatives? Get the inside scoop on upcoming events?

Visit our website www.MacdonaldLaurier.ca and sign up for our newsletter.

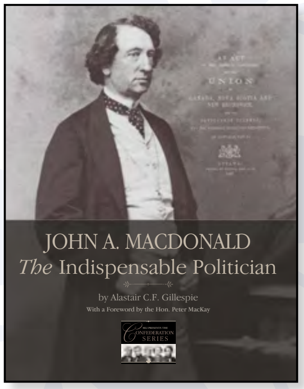
RESEARCH PAPERS


A Macdonald-Laurier Institute Publication
FORCE 2.0
Fixing the Governance, Leadership, and Structure of the RCMP
Christian Leuprecht
SEPTEMBER 2017
MLI

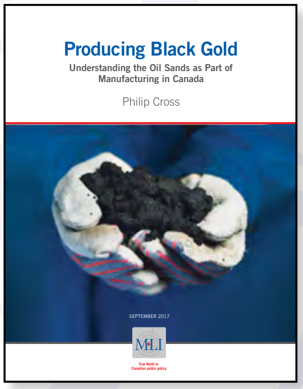
Force 2.0
Christian Leuprecht


A BETTER PATH for Canadian Health Care
MLI
The Unkindest Cut
How a new plan for slashing drug prices could harm the prosperity and health of Canadians
Wayne Critchley and Richard C. Owens
HEALTH

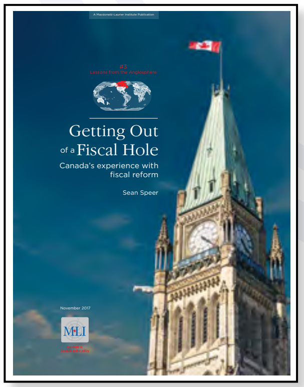
The Unkindest Cut
Wayne Critchley and
Richard C. Owens


JOHN A. MACDONALD
The Indispensable Politician
by Alastair C.F. Gillespie
With a Foreword by the Hon. Peter MacKay
CONFEDERATION SERIES

John A. Macdonald: The Indispensable Politician
Alastair C.F. Gillespie


Producing Black Gold
Understanding the Oil Sands as Part of Manufacturing in Canada
Philip Cross
SEPTEMBER 2017
MLI

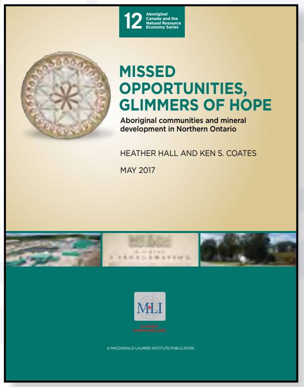
Producing Black Gold
Philip Cross


Getting Out of a Fiscal Hole
Canada's experience with fiscal reform
Sean Speer
November 2017
MLI

Getting Out of a Fiscal Hole
Sean Speer

MLI
#3
Getting the Big Picture:
How regional assessment can pave the way for more inclusive and effective environmental assessments
Bram Noble
A MACDONALD-LAURIER INSTITUTE PUBLICATION
JUNE 2017

Getting the Big Picture
Bram Noble


12
MISSED OPPORTUNITIES, GLIMMERS OF HOPE
Aboriginal communities and mineral development in Northern Ontario
HEATHER HALL AND KEN S. COATES
MAY 2017
MLI
A MACDONALD-LAURIER INSTITUTE PUBLICATION

Missed Opportunities, Glimmers of Hope
Heather Hall and
Ken S. Coates

RUNNING OUT OF TIME
Demographic Pressures and the Future of Canadian Health Care
Brian Ferguson, Sean Speer, and Ariel Freeman-Fawcett
November 2017
MLI

Running Out of Time
Brian Ferguson, Sean Speer,
and Ariel Freeman-Fawcett

For more information visit: www.MacdonaldLaurier.ca

True North in
Canadian public policy

CONTACT US: Macdonald-Laurier Institute
323 Chapel Street, Suite #300
Ottawa, Ontario, Canada
K1N 7Z2

TELEPHONE: (613) 482-8327

WEBSITE: www.MacdonaldLaurier.ca

CONNECT WITH US:

@MLInstitute

www.facebook.com/
MacdonaldLaurierInstitute

www.youtube.com/
MLInstitute

What people are saying about the Macdonald-Laurier Institute

In five short years, the institute has established itself as a steady source of high-quality research and thoughtful policy analysis here in our nation's capital. Inspired by Canada's deep-rooted intellectual tradition of ordered liberty – as exemplified by Macdonald and Laurier – the institute is making unique contributions to federal public policy and discourse. Please accept my best wishes for a memorable anniversary celebration and continued success.

THE RIGHT HONOURABLE STEPHEN HARPER

The Macdonald-Laurier Institute is an important source of fact and opinion for so many, including me. Everything they tackle is accomplished in great depth and furthers the public policy debate in Canada. Happy Anniversary, this is but the beginning.

THE RIGHT HONOURABLE PAUL MARTIN

In its mere five years of existence, the Macdonald-Laurier Institute, under the erudite Brian Lee Crowley's vibrant leadership, has, through its various publications and public events, forged a reputation for brilliance and originality in areas of vital concern to Canadians: from all aspects of the economy to health care reform, aboriginal affairs, justice, and national security.

BARBARA KAY, NATIONAL POST COLUMNIST

Intelligent and informed debate contributes to a stronger, healthier and more competitive Canadian society. In five short years the Macdonald-Laurier Institute has emerged as a significant and respected voice in the shaping of public policy. On a wide range of issues important to our country's future, Brian Lee Crowley and his team are making a difference.

JOHN MANLEY, CEO COUNCIL