ISSN 2563-8165
CAT D95-10E-PDF

CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS

JULY 2021 UPDATE

Communications Security Establishment
Centre de la sécurité des télécommunications
Canada

Communications Security Establishment
1929 Ogilvie Road,
Ottawa, ON K1J 8K6
cse-cst.gc.ca

ISSN 2563-8165
CAT D95-10E-PDF

Cyber Threats to Canada's Democratic Process
is an ad hoc document published approximately every two years

ABOUT US

THE Communications Security Establishment (CSE) is Canada's centre of excellence for cyber operations. As one of Canada's key security and intelligence organizations, CSE protects the computer networks and information of greatest importance to Canada and collects foreign signals intelligence. CSE also provides assistance to federal law enforcement and security organizations in their legally authorized activities when they need CSE's unique technical capabilities.

CSE protects computer networks and electronic information of importance to the Government of Canada, helping to thwart state-sponsored or criminal cyber threat activity on our systems. In addition, CSE's foreign signals intelligence work supports government decision-making in the fields of international affairs, defence, and security, providing a better understanding of global events and crises and helping to further Canada's national interest in the world.

As part of CSE, the Canadian Centre for Cyber Security (Cyber Centre) is home to trusted experts in cyber security with a straightforward, focused mandate to collaborate with government, the private sector, and academia to make Canada a safer place online.

CSE and its Cyber Centre play an integral role in helping to protect Canada and Canadians against foreign-based terrorism, foreign espionage, cyber threat activity, kidnapping of Canadians abroad, attacks on our embassies, and other serious threats with a significant foreign element, helping to ensure our nation's security, stability, and prosperity.

EXECUTIVE SUMMARY

EMOCRATIC processes around the world continue to be targeted by cyber threat actors. In this assessment, we review global trends in cyber threat activity against democratic processes (which we define as including voters, political parties, and elections) and evaluate the threat to Canada, with special focus on the impacts of the COVID-19 pandemic.

KEY FINDINGS

GLOBAL TRENDS

- Democratic processes remain a popular target. After increasing from 2015 to 2017, the proportion of democratic processes targeted by cyber threat actors has remained relatively stable since 2017.
- From 2015 to 2020, we judge that the vast majority of cyber threat activity affecting democratic processes can be attributed to state-sponsored cyber threat actors. These actors target democratic processes in pursuit of their strategic objectives (i.e., political, economic, and geopolitical).
- Russia, China, and Iran are very likely responsible for most of the foreign state-sponsored cyber threat activity against democratic processes worldwide.
- Cyber threat actors most often target some combination of voters, political parties, and election infrastructure. We judge that cyber threat actors likely perceive that directing their efforts at a combination of targets associated with a democratic process is more effective than targeting one group in isolation.
- Between 2015 and 2020, cyber threat activity was directed at voters more often than against political parties and elections. This activity included online foreign influence activity as well as more traditional cyber threat activities, like information theft or denying access to important websites. We assess that it is likely that cyber threat actors perceive targeting voters to be a more effective and relatively easy way to interfere with democratic processes.
- We assess that changes made around the world in response to the COVID-19 pandemic, such as moving parts of the democratic process online or incorporating new technology into the voting process, almost certainly increased the cyber threat surface of democratic processes. Most significantly, threat actors can harness and amplify false narratives related to the COVID-19 pandemic to decrease confidence in elections.

IMPLICATIONS FOR CANADA

- We assess that Canada's democratic process remains a lower-priority target for state-sponsored cyber actors relative to other countries. However, we judge it very likely that Canadian voters will encounter some form of foreign cyber interference (i.e., cyber threat activity by foreign actors or online foreign influence) ahead of, and during, the next federal election. It is unlikely to be at the scale seen in the US.
- In the event of a federal election during a pandemic, Elections Canada has plans in place to protect the health and safety of all participants in the electoral process. While any modifications to the electoral process have the potential to increase the cyber threat, we assess that the planned changes do not substantially expand the cyber threat to Canada's democratic process.

TABLE OF CONTENTS

LIST OF FIGURES

SCOPE

This report considers cyber threat activity that affects the democratic process, which we view as a combination of voters, political parties, and elections. Cyber threat activity involves the use of cyber tools (e.g., malware and spear-phishing) to compromise an information system by altering the confidentiality, integrity, and availability of a system or the information it contains. This type of activity is conducted by state-sponsored actors, cybercriminals, hacktivists, politically motivated actors, and thrill-seekers. There is a significant amount of false and misleading information online, but this assessment primarily considers **online foreign influence activity** targeting voters. This influence activity happens when foreign threat actors covertly manipulate online information, often using cyber tools, in order to influence voters' opinions and behaviours. We define **foreign interference** as covert, deceptive, or coercive activity by a foreign actor against a democratic process, conducted to advance strategic objectives. Foreign cyber interference includes cyber threat activity by foreign actors as well as online foreign influence activity. Note that these definitions are specific to our focus on cyber threats to Canada's democratic process and that similar definitions can be used differently by other Canadian federal institutions.

ABOUT THIS DOCUMENT

HIS document provides an update to the *2017* and *2019* *Cyber Threats to Canada's Democratic Process* reports released by CSE. Its purpose is to inform Canadians about cyber threats to the democratic process.

SOURCES

In producing this document, we relied on reporting from both classified and unclassified sources. CSE's foreign intelligence mandate provides us with valuable insights into adversary behaviour.

Defending the Government of Canada's information systems also provides CSE with a unique perspective to observe trends in the cyber threat environment.

LIMITATIONS

We discuss a wide range of cyber threats to global and Canadian political and electoral activities based on our access to information. Providing threat mitigation advice is outside the scope of this document.

MORE INFORMATION

For readers interested in more detailed information about cyber tools and the evolving cyber threat landscape, we refer you to the *National Cyber Threat Assessment 2020* and *An Introduction to the Cyber Threat Environment*.

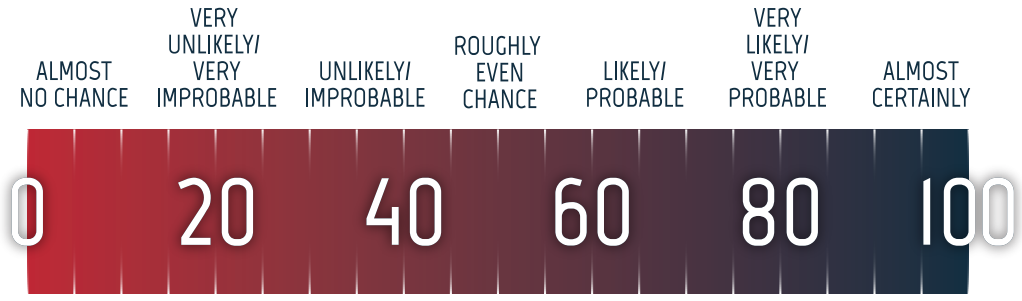
Further resources from the Cyber Centre are available online, including *Get Cyber Safe*, *Don't Take the Bait: Recognize and Avoid Phishing Attacks*, and *Cyber Hygiene*.

ESTIMATIVE LANGUAGE

Our judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases, and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

The contents of this document are based on information available as of 12 July 2021.

The chart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



INTRODUCTION

ROUND the world, democratic processes continue to be affected by cyber threat activity. A democratic process is made up of participants, like voters and political parties, and events, like elections. Cyber threat activity is carried out against these participants and events by state-sponsored actors, cybercriminals, politically motivated actors, hacktivists, and thrill-seekers. We have observed how the tactics these threat actors use have evolved over time as they adapt to emerging opportunities and new cyber tools that make it easier to target the democratic process.

Targeting democratic processes largely remains a strategic activity. State-sponsored cyber threat actors with links to Russia, China, and Iran have conducted most of the observed cyber threat activity against democratic processes worldwide.

The COVID-19 pandemic has caused significant changes to how democratic processes operate around the world, including in Canada. In many jurisdictions, political parties and candidates have moved their campaigns almost entirely online. Electoral bodies responsible for elections have been forced to plan and prepare for elections while working from home. Voting procedures have also been adapted to ensure that the health of voters and poll workers is protected and that all eligible members of a society are able to vote safely. Yet, we judge that COVID-19-related changes to electoral procedures have had limited impacts on observed cyber threat activity against elections.

However, we have seen that COVID-19-related changes to elections, such as more people choosing to vote by mail or delays in the dissemination of results, have spurred falsehoods and conspiracy theories that call into question the legitimacy of election results. This is happening at a time when the online information ecosystem is already rife with false and misleading content. Both foreign and domestic actors create and share falsehoods for political or geopolitical gain or to manipulate or harm their target audience and society. Others share the content because they believe it to be true. It is increasingly difficult to determine who is sharing false information and why. In this environment, it is easier for hostile foreign actors to conduct online influence activity, fuel divisions within society, and undermine confidence in democratic institutions.

While there are many opportunities for threat actors to target democratic processes, it is important to note that, in the past few years, there have also been significant strides towards protecting democracy around the world. This includes efforts by governments, non-governmental and research organizations, civil society, traditional media, and social media and technology companies to improve cyber security practices, raise awareness, and respond to incidents quickly. For example, Canada has implemented a broad suite of measures, including legislation (i.e., the Elections Modernization Act), agreements with social media companies, as well as several initiatives to improve communication and information sharing between Elections Canada, Canadian security and intelligence agencies, other government departments, political parties, and voters.

In this assessment, we evaluate the cyber threats directed at democratic processes around the world and assess what this means for Canada, with special focus on the impacts of COVID-19. First, we describe why an adversary would target Canada, discuss the possible consequences of cyber activity against democratic processes, and give an overview of the impacts of the COVID-19 pandemic on this threat. Next, we describe the cyber threats to voters, political parties, and elections around the world in more detail. Finally, we discuss global trends in cyber activity against democratic processes and what this means in the Canadian context.

WHY TARGET CANADA'S DEMOCRATIC PROCESS?

CANADA IN THE WORLD

Canada takes an active role in the international community, participating in key multilateral forums, including the North Atlantic Treaty Organization (NATO), the Organisation for Economic Co-operation and Development (OECD), the Group of 20 (G20), and the Group of 7 (G7).[1] Government of Canada foreign policy, military deployments, trade and investment agreements, diplomatic engagements, international aid, and immigration policy are of interest to other states. Canada's stance on an issue can affect the core interests of other countries, foreign groups, and individuals. Threat actors may use cyber tools to target Canada's democratic process to change election outcomes, influence policy makers' choices, impact governmental relationships with foreign and domestic partners, and impact Canada's reputation around the world.

CANADA IS ONLINE, AS ARE THREAT ACTORS

According to the most recent estimates, approximately 94% of Canadians were using the Internet in 2021.[2] The vast majority of Canadians use the services provided by major Internet companies, such as Facebook or Google, to obtain information, communicate with one another, and build communities. As Canadians engage with each other and access information online, they become exposed to cyber threat actors and the tools they use to interfere with democratic processes. Threat actors who want to interfere with Canadian democratic processes may take advantage of Canada's highly connected society and regularly used online services. Cybercriminals trying to make money and thrill-seekers searching for a challenge or notoriety may target Canadian democratic processes as well. While these activities lack a strategic agenda, they still impact the functioning of democratic processes and voters' perceptions of the security, legitimacy, and fairness of the results.

CYBER TOOLS AND SERVICES IMPROVING AND WIDELY AVAILABLE TO THREAT ACTORS

In the *National Cyber Threat Assessment 2020* (NCTA 2020), we assessed that the development of commercial markets for cyber tools and talent has reduced the time it takes for states to build cyber capabilities and increased the number of states with cyber programs. As more states have access to cyber tools, states that were interested in targeting democratic processes, but previously lacked sufficient capabilities, can now more readily undertake this type of cyber activity. The proliferation of state cyber programs also makes it more difficult to identify, attribute, and defend against cyber threat activity more broadly.

In addition, a large illegal market for cyber tools and services is greatly reducing the start-up time for cybercriminals and enabling them to conduct more complex and sophisticated campaigns.[A] Many online marketplaces allow vendors to sell specialized cyber tools and services that users can purchase and use to commit cybercrimes, including website defacement, cyber espionage, distributed denial of service (DDoS) attacks, and ransomware attacks.[B] Any of these tools could be used against democratic processes for financial gain, to send a political message, or to attempt to impact an election.

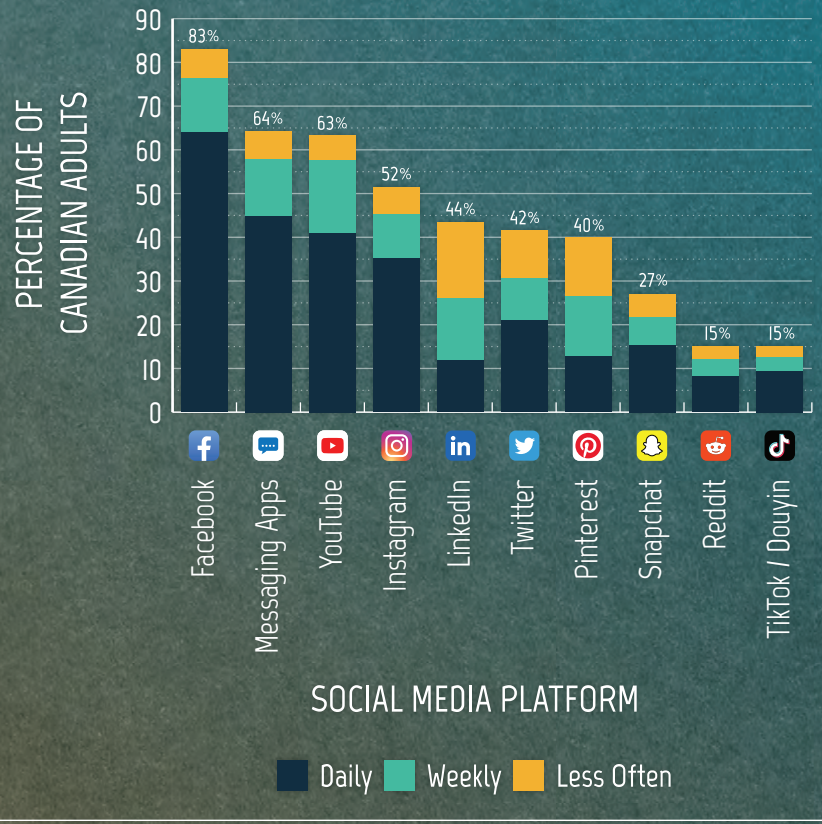
DEEPFAKES: BEYOND IMAGES AND VIDEO

Evolving technology underpinned by artificial intelligence (AI) used by cyber threat actors to create false or misleading online content has become cheaper and easier to access.[3] In *NCTA 2020*, we discussed deepfake videos and how they can be used to create synthetic videos of events or public figures that look real. While technology companies have invested resources in advancing methods to automatically detect deepfake videos, other rapidly evolving forms of AI-generated media have emerged that are harder to detect, such as AI-generated writing (i.e., deepfake text) and deepfake audio.[4] Threat actors can use deepfake text against electoral processes, including targeting voters with disinformation, spear-phishing candidates and their staff, and abusing online governmental processes.[5] Deepfake text is now largely undetectable by humans. A 2019 study found that when humans were asked to classify deepfake comments as human or bot submissions, the results were no better than the results of random guessing.[6] Threat actors can also target voters using AI-generated audio to mimic the tone, inflection, and idiosyncrasies of candidates or poll workers.

A For more information on these trends, see CSE's *National Cyber Threat Assessment 2020*.

B For definitions of these and other common cyber tools and tactics, see CSE's *An Introduction to the Cyber Threat Environment*.

FIGURE 01 | FREQUENCY OF SOCIAL MEDIA USE BY ADULTS, 2020



Google maintained 91.83% of the search engine market in Canada in January 2021.*

* Search Engine Market Share Canada | Global Stats | Accesed February 2021 | https://gs.statcounter.com/search-engine-market-share/all/canada

CANADIAN ADULTS ONLINE IN 2020

94% had a social media account on at least one platform

83% had a Facebook account

77% of those used facebook daily

The State of Social Media in Canada 2020: A New Survey Report from the Ryerson Social Media Lab | Ryerson University | 13 July 2020 | https://socialmedialab.ca/2020/07/13/the-state-of-social-media-in-canada-2020-a-new-survey-report-from-the-ryerson-social-media-lab

EFFECTS OF CYBER ACTIVITY AGAINST DEMOCRATIC PROCESSES

Cyber threat activity against democratic processes around the world can have short-, mid-, and long-term effects. In some cases, the perception of successful cyber threat activity against democratic processes can undermine public confidence in democratic institutions, even if the cyber activity never occurred or had no significant consequences. For example, the US Intelligence Community found that during the 2020 US presidential election some foreign actors spread false or inflated claims about alleged compromises of voting systems to undermine confidence in the electoral process and results.[7] Many allegations of election fraud surfaced in relation to the 2020 US election and continued to persist even after they were proven false.[8] These allegations have had lasting implications for trust in democratic processes in the US.[9]

When cyber threat activity against political parties or election infrastructure is combined with online foreign influence activities, these impacts can be greater. For example, cyber threat actors can steal sensitive information about a candidate and spread the stolen information on social media to decrease support for that candidate.

The short-term consequences of cyber threat activity include:

- amplifying false or polarizing discourse;
- burying legitimate information;
- affecting the popularity of or support for candidates;
- calling into question the legitimacy of the election process and results;
- promoting a desired election outcome;
- distracting voters from important election issues; and
- reducing voter turnout.

Mid-term and long-term consequences include:

- reducing the public's trust in the democratic process;
- lowering trust in journalism and the media;
- creating divisions in international alliances;
- increasing polarization and decreasing social cohesion;
- weakening confidence in leaders; and
- promoting the economic, geopolitical, or ideological interests of hostile foreign states.

FIGURE 02 | SHORT-, MEDIUM-, AND LONG-TERM GOALS OF STATE-SPONSORED CYBER ACTORS

IMPACTS OF THE COVID-19 PANDEMIC ON DEMOCRATIC PROCESSES

In 2020, at least 40 countries and territories around the world postponed national-level elections and referendums due to the COVID-19 pandemic. At least 79 national-level elections and referendums were held during the COVID-19 pandemic.[10] Most states implemented sanitary and distancing measures and many created additional ways to vote, allowing those in self-isolation or at higher risk to vote more safely and reducing crowding at in-person voting locations. For example, states expanded mail-in voting, enabled voting over the phone, and expanded voting hours and locations.[11]

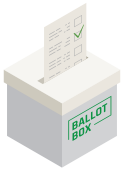
Overall, the changes to electoral procedures due to COVID-19 appear to have had limited impacts on the cyber threat to elections. While these changes created additional opportunities for cyber threat actors, we did not observe a substantial change to the frequency of their activities. While threat actors can try to disrupt information about changes to voting procedures or target online campaign activities, we judge that the most significant new opportunities for cyber threat actors are COVID-19-related narratives that can be used to undermine confidence in elections.[12] These narratives include connecting voter fraud with mail-in voting and exaggerating the public health risk of in-person voting.[13]

KEY TARGETS IN THE DEMOCRATIC PROCESS

N the *2019 Update: Cyber Threats to Canada's Democratic Process*, we identified three key enduring targets within the democratic process: voters, political parties, and elections. The following section provides additional detail on the threats faced by each target and how they have evolved in recent years, including in the context of the COVID-19 pandemic.

Voters engage with political parties, candidates, and other voters through social media. Voters also access information about voting processes online. Cyber threat actors manipulate online information to influence voters' opinions and behaviours.

Political parties compete for attention and support in elections, relying heavily on the Internet, which they use to organize and to communicate with voters. This reliance is even more pronounced during the COVID-19 pandemic where traditional in-person campaigning and fundraising events face COVID-19-related restrictions. Cyber threat actors use cyber tools to target the websites, emails, social media accounts, networks, and devices of political parties, candidates, and their staff. Cyber threat actors also target consultants, polling firms, and research companies hired by political parties.



Elections include all the processes involved when individuals vote for their government representatives—registering voters, casting ballots, counting ballots, and releasing results to the public. Voters must have confidence in the legitimacy of the process. Cyber threat actors could attempt to undermine trust in elections or suppress voter turnout by altering content on the websites, social media accounts, networks, and devices used by election management bodies.

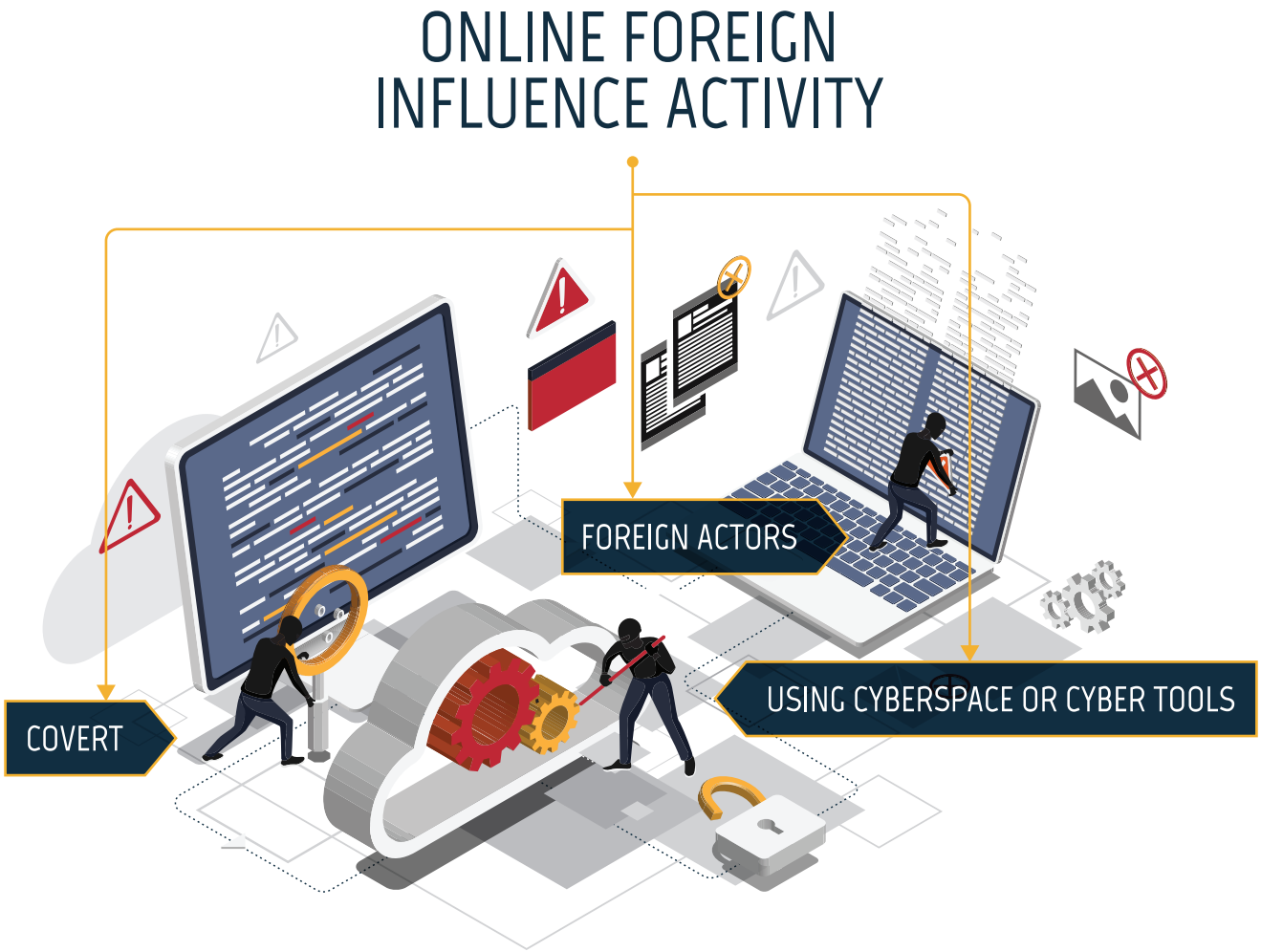
TARGETING VOTERS

We assess that the most significant cyber threat faced by voters is online foreign influence, which is when foreign actors covertly create, disseminate, or amplify false and misleading material online to influence the beliefs or behaviours of voters. Cyber threat actors also target databases of information about voters held by political parties and election management bodies as well as websites used by voters to get the information they need to vote.

Online foreign influence has become a common tool for adversaries. They use online influence to further their core interests, such as national security, economic prosperity, and ideological goals.[C] Online influence campaigns can try to:

- impact civil discourse;
- influence policy makers' choices;
- compromise government relationships and the reputations of politicians;
- delegitimize the concept of democracy and other values such as human rights and liberty; and
- exacerbate existing frictions in democratic societies.

FIGURE 03 | THREE COMPONENTS OF ONLINE FOREIGN INFLUENCE ACTIVITY



C For more information, see CSE's *National Cyber Threat Assessment 2020*.

FOREIGN INFLUENCE AND THE DOMESTIC INFORMATION ECOSYSTEM

Voters must contend with an online information ecosystem filled with false and misleading information. This information can come from both foreign and domestic sources. It is often difficult to determine the origin of information circulating online, who is spreading it, and why. While beyond the scope of this assessment, false or inaccurate information spread by domestic actors—with or without malign intent—can negatively impact voters and contribute to the goals of foreign threat actors, such as undermining voter trust in electoral processes or increasing polarization among voters.

TYPES OF FALSE INFORMATION: DISINFORMATION VS. MISINFORMATION

Disinformation is false information that is specifically created and disseminated to cause harm.[14] This can include altering official documents to make false claims appear legitimate or otherwise creating official-seeming content, like deepfakes. **Misinformation** is false information spread without the intention to cause harm.[15] In practice, it is often difficult to distinguish between misinformation and disinformation.

Social media provides a megaphone for domestic actors with many followers, such as influencers, individuals with verified accounts, or public figures. False information promoted by these prominent figures, including narratives that undermine democratic institutions and processes, can spread farther and have greater impacts on voters than when foreign actors try to do the same thing covertly. The disproportionate reach of public figures has been observed in the context of COVID-19. Researchers at the Reuters Institute found that although COVID-19 misinformation from prominent public figures made up just 20% of the claims of COVID-19 misinformation studied, they accounted for 69% of total social media engagement.[16]

Some governments and political parties employ disinformation or manipulate the online information ecosystem to influence voters.[17] For example, in the run-up to the 2021 Ugandan general election, Facebook took down a network of fake and duplicate accounts that were linked to the Ugandan government and were being used to boost the popularity of posts.[18] In the following days, the government banned social media and then shut down the Internet in Uganda.[19] Governments have increasingly restricted Internet access during elections, limiting access to information, curbing dissent, and limiting freedom of expression.[20]

ONLINE INFLUENCE FOR HIRE

Private firms increasingly provide online influence as a service to governments and political actors.[21] A 2020 Oxford study identified 48 cases of private companies deploying disinformation on behalf of a political actor. Since 2018, the same researchers have identified more than 65 firms offering disinformation as a service.[22] Private firms spread disinformation through trolling, automated accounts, human-curated accounts, and AI.[23] Governments and political actors who hire firms to conduct online influence campaigns on their behalf not only use domestic firms, but also turn to firms based in other countries.[24] For example, between 2019 and 2020, the Archimedes Group, based in Israel, ran online influence campaigns against elections in Africa, Latin America, and South East Asia.[25]

CASE STUDY: QANON AND ONLINE FOREIGN INFLUENCE

QAnon is a loose cluster of debunked conspiracy theories, whose content has increased in volume and frequency since late 2017.[26] While primarily based in the US, QAnon theories have gained a following in over 25 countries, including Canada, which is one of the top four countries driving QAnon content on social media.[27] State-sponsored groups in Russia and Iran have propagated content related to QAnon.[28] Social media and news accounts tied to Russia promoted QAnon in its early days.[29] On Twitter, accounts suspected of being controlled by Russian cyber threat actors sent a high volume of tweets related to QAnon in 2019.[30] To a lesser extent, Iranian actors have used QAnon references and content in their online influence activity, including activities during the 2020 US election.[31]

State-sponsored cyber threat actors, including from Russia and Iran, have taken advantage of domestic groups and movements in other countries and used the messages and reach of these domestic groups to better influence voters.[32] For example, state-sponsored actors have promoted content and messaging related to QAnon for the purpose of reaching voters in the US. State-sponsored actors have also pretended to be domestic groups in the US to send threatening messages to voters.[33]

Domestic journalists and intellectuals have also unknowingly been hired by foreign threat actors to write articles with a political angle that are then used in broader online foreign influence campaigns.[34] This further blurs the distinction between foreign and domestic actors. Co-opting legitimate sources to endorse specific perspectives lends credibility to messages promoted by online foreign influence campaigns.

THE INTERNET, SOCIAL MEDIA PLATFORMS, AND VOTERS

Voters around the world get a substantial amount of information online, often from social media.[35] However, social media platforms are a fertile environment for creating and disseminating false information. They rely on deep learning algorithms to suggest content to their users, which often prioritize posts that have greater prior engagement (e.g., shares, likes, comments) and end up amplifying inflammatory content.[36] As a result, voters are faced with a glut of misleading, false, and inflammatory information. In the context of COVID-19 and elections, some social media platforms have instituted measures to try to address the spread of false information by:

- demoting "borderline content" (i.e., content that almost violates community guidelines);
- shutting down inauthentic accounts;
- hiring personnel to screen posts and investigate malfeasance;
- collaborating with fact-checking and research organizations;
- flagging or demoting misleading content; and
- directing users to authoritative sources.[37]

Some social media platforms, tailored to niche audiences, play a critical role in the dissemination of hate and extreme content.[38] While sites such as 4chan, 8chan, Gab, and Parler do not have the reach of larger social media companies, they provide a space for like-minded people to interact and perpetuate extreme narratives that can spread to the rest of the Internet.[39] As more mainstream platforms increasingly remove extreme and false content, they can push individuals interested in this information from an open community, such as Twitter, into fringe environments, like Gab, that pride themselves on allowing users to post anything they like.[40] Hostile foreign actors have used these platforms for online foreign influence activity. For example, during the 2020 US election, Russian actors targeted far-right American users on Gab and Parler with online foreign influence activity that promoted President Trump and denigrated then-candidate Biden.[41]

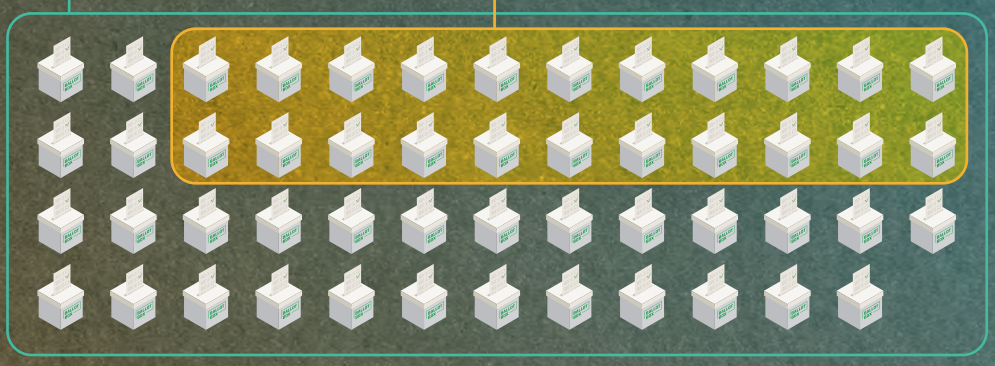
Some platforms are used primarily by specific communities and can be used to censor or cultivate messages within those communities. For example, WeChat, a do-everything app from China used by billions around the world, has magnified divisions and spread disinformation or propaganda specific to the Chinese diaspora on the platform.[42]

ONLINE FOREIGN INFLUENCE ON ENCRYPTED PLATFORMS

Encrypted messaging apps (EMAs), like WhatsApp, Signal, and Telegram, make it difficult to trace and curb the spread of false information, which is why many groups that have been de-platformed from mainstream apps are flocking to EMAs.[43] For example, after far-right groups in the US were removed from many mainstream platforms and Parler went offline due to actions by Apple, Google, and Amazon, many far-right users adopted EMAs like Signal, CloutHub, MeWe, Telegram, and Rumble.[44] Further, the closed nature of EMAs means that most users are communicating with people they consider trustworthy. The ability to forward information to large groups of people also increases the chances for false information to be misinterpreted as fact. Amid the COVID-19 pandemic, EMAs have also become a key distribution channel for medical misinformation, hoaxes, and scams.[45]

FIGURE 04 | POLITICAL CAMPAIGNING DURING THE COVID-19 PANDEMIC

A review of national elections in **51** countries held during the COVID-19 pandemic in 2020 found that **22** of the 51 countries had COVID-19 restrictions that limited opportunities for public gatherings, impacting political campaigns. In many countries, candidates responded by campaigning online.*



COVID-19 AND THE CYBER THREAT TO VOTERS

The COVID-19 pandemic offers new opportunities for online foreign influence aimed at undermining voter confidence in electoral processes and attempting to decrease voter turnout.[46] Many jurisdictions have expanded access to mail-in ballots and other alternative voting methods to decrease the size of crowds at voting locations and protect at-risk voters. However, this has created an opportunity for cyber threat actors to create or amplify false narratives linking mail-in voting and other alternative voting arrangements with voter fraud. Hostile foreign actors can also create and amplify messaging to increase voters' perception of the risk of contracting COVID-19 at voting locations in an attempt to decrease turnout. Even if turnout is not reduced, the presence of these narratives and the perception that COVID-19 decreased turnout can reduce voter confidence in the results. Finally, changes to voting procedures, such as extended voting days and expanded use of mail-in ballots, can delay the dissemination of results. This delay presents an opportunity for threat actors to spread disinformation, such as false results, before the election management body has a chance to release accurate information.

TARGETING POLITICAL PARTIES

Cyber threat actors target political parties, candidates, and their staff in many countries to:

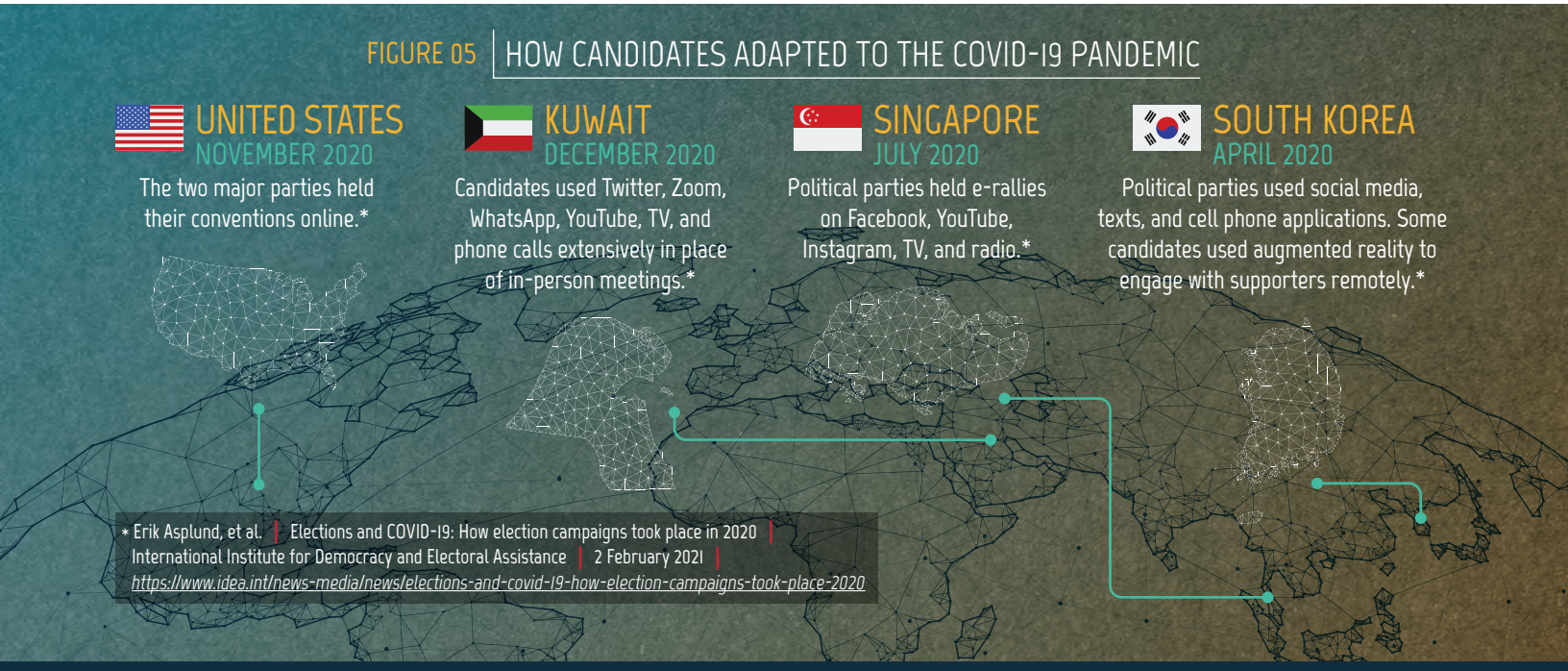
- disrupt engagement with the public for financial gain, to harm the political party or candidate, or for publicity;
- steal sensitive or proprietary information, including from databases; or
- interfere with political party procedures that are undertaken online.

We assess that cybercriminals will almost certainly continue to take advantage of the online presence of political parties or politicians for financial gain, either by hijacking the websites or accounts of political parties or politicians or by creating fake websites, accounts, or emails and other communications that are designed to look official. Cybercriminals can use ransomware or DDoS attacks to disrupt online events or pages and attempt to extort funds from politicians or political parties. According to Cloudflare, an American website security company, there was a notable amount of DDoS activity against US political campaign websites in 2020.[47] Cybercriminals can also compromise the online resources of politicians and political parties in other ways. For example, in the 2020 US election, one candidate's campaign website was compromised by cybercriminals who attempted to use it to collect cryptocurrency.[48] In addition, some cybercriminals leverage current events, including elections, to target their victims, sending phishing emails related to topics of interest to their victims so that recipients are more likely to open malicious attachments or click malicious links.[49] In the case of election-related lures, these victims can be members of political parties, candidates, their staff, voters, or other individuals interested in the election.

State-sponsored actors are also interested in the networks, websites, and email and social media accounts of political parties, candidates, and their staff. Disrupting the campaign of a candidate or political party could influence support for that party or undermine confidence in the fairness of the electoral process. Hacktivists, politically motivated actors, and thrill-seekers have also targeted the websites and events of political parties and candidates to spread their own messages as well as for publicity.[50]

In addition, sensitive information related to a political party or candidate as well as databases of personal information held by political parties are attractive to both cybercriminals and state-sponsored actors. Polling firms, research companies, and

FIGURE 05 | HOW CANDIDATES ADAPTED TO THE COVID-19 PANDEMIC



* Erik Asplund, et al. | Elections and COVID-19: How election campaigns took place in 2020 | International Institute for Democracy and Electoral Assistance | 2 February 2021 | https://www.idea.int/news-media/news/elections-and-covid-19-how-election-campaigns-took-place-2020

consultants that are hired by political parties or candidates also have information of interest to cyber threat actors. Stolen databases can be used for future cyber activity, including financially motivated activity as well as strategically motivated campaigns by state-sponsored cyber threat actors. Sensitive information stolen from compromised accounts can be leaked to tarnish the reputation of a candidate or used for extortion. Threat actors can focus online foreign influence activities against a specific candidate or party, attempting to drive voters away from that candidate and towards the opposition.

Finally, some political parties vote online. In some cases, this allows more party members to vote in leadership races.[51] However, having these votes online makes them vulnerable to cyber threat actors who may want to change the results or sow distrust within a political party. In 2021, a German political party that held its leadership vote online during a virtual party conference was targeted by a DDoS attack. The attack interrupted the conference, but the vote was not impacted because it was intentionally hosted on a different server to protect the vote from cyber threat activity.[52]

COVID-19 AND THE CYBER THREAT TO POLITICAL PARTIES

Due to the COVID-19 pandemic, in-person campaigning events, such as political rallies, fundraisers, or door-to-door canvassing, have been restricted or banned in some jurisdictions. In response, some political parties and candidates have adapted to comply with local public health restrictions through mailing information packages, car rallies, distanced door-to-door canvassing, and increasing their use of online tools for campaigning or taking internal party decisions.[53] Since the start of the pandemic, political parties have held virtual conventions, town halls, fundraisers, and turned to online video calling to canvas voters.[54] Election campaigning and fundraising had been moving online before COVID-19, but the pandemic has increased the use of digital tools.[55] This movement towards online solutions creates more opportunities for cyber threat actors interested in targeting political parties and campaigns to advance strategic goals or for financial gain and makes campaigns less resilient if online resources are compromised.

ADAPTING ELECTORAL CAMPAIGNS IN COVID-19: SOUTH KOREA

South Korea was one of the first countries to hold a major national election during the COVID-19 pandemic. Restrictions on holding events, attending public gatherings, and social distancing requirements prevented conventional campaign activities like rallies, public speeches, debates, fundraising events, and door-to-door canvassing. Instead, candidates shifted to online and digital technology such as video messages disseminated via social media, texts, and mobile phone applications. Some candidates used augmented reality to engage with supporters remotely. Some candidates also campaigned outside the digital sphere, participating in COVID-19-related volunteer work and mailing printed materials to voters.[56]

TARGETING ELECTIONS

Cyber threat actors interested in undermining democratic institutions or sabotaging election results can target electoral processes and infrastructure, altering content on the websites and social media accounts of election management bodies, stealing information such as voter registration databases, or compromising the systems or communications underlying the election. Election processes around the world involve four main steps, and each can introduce opportunities for cyber threat actors.

Voter registration is done online in many jurisdictions globally.[57] Cyber threat actors can target online voter registries to attempt to add fake voter records, erase or encrypt the data, make the website inaccessible for registration, or display misleading information. These activities can sow doubt in the minds of voters, slow down voting, cause voter frustration or suppression, and impact election results. Stolen voter registration data can be used for future threat activity, including strategic activity related to the election as well as cyber threat activity completely unrelated to the election.[D]

When voters go to **cast their ballots** in person, their identities must be checked against the list of registered voters contained in poll books. Electronic poll books are used in many countries to make it easier to look up voters. In some cases, these poll books are networked so that different locations can communicate with each other to allow people more flexibility when choosing where to vote while preventing people from voting at more than one location. However, connecting these devices and enabling them to communicate remotely increases their vulnerability to cyber threat activity. After a voter's identity is checked against the list of registered voters, they can cast their ballot. In almost all cases, this step is paper based or electronic. Estonia is the only country that uses Internet-enabled voting for all jurisdictions in national-level elections.[58]

D For more information, see CSE's *National Cyber Threat Assessment 2020*.

Once ballots are cast, they must be **counted** and the **results disseminated**. Ballots are often counted electronically, but the results can also be tabulated by hand. The results of the count must then be submitted to a central body that tallies the numbers from different polling locations and jurisdictions. The results can be submitted via phone, fax, email, or electronically. However, many jurisdictions retain paper records to enable the results to be validated or audited. The final stage of the voting process is the dissemination of the results, which is frequently done over the Internet.

Most election management bodies use some degree of technology to improve their electoral processes (e.g., standard office tools and websites, biometric voter registration databases, and Internet-enabled voting systems).[59] These solutions can increase efficiency, accuracy, and transparency, but each component of the election process that is online or electronic could be targeted by cyber threat actors. The institutions responsible for elections implement a range of measures to protect the electoral process, such as keeping crucial parts of the process paper based, maintaining back-ups of important databases, and establishing alternative procedures to allow voters to cast their ballots if the technology involved in the process malfunctions or is compromised.

After some elections, cyber threat actors have conducted operations to discredit or undermine the elected government before it takes office. These efforts do not necessarily target voters, political parties, or elections. In many cases they target government institutions broadly or even critical infrastructure. Threat actors can also spread disinformation after an election to undermine trust in the results or attempt to stop the elected government from taking office.

CASE STUDY: CYBER PROTESTS IN BELARUS

The August 2020 presidential election in Belarus has been condemned as fraudulent by many countries, including Canada, the US, and the European Union (EU).[60] Following the count, the opposition refused to concede the election, triggering widespread protests.[61] In this context, hacktivists in Belarus used various tactics, including defacing government websites and targeting government institutions, to pressure the incumbent president into resigning. In one instance, hacktivists leaked the identities and addresses of 1,000 law enforcement officers who were violently responding to protesters.[62] In August 2020, hacktivists were responsible for at least 15 cyber incidents against state-owned online resources in Belarus.[63]

COVID-19 AND THE CYBER THREAT TO ELECTIONS

Prior to the COVID-19 pandemic, some parts of the election process, like voter registration, were moving online in many jurisdictions. However, very few jurisdictions were attempting to implement Internet-enabled voting at the national-level prior to the pandemic, and it is unlikely that countries that do not already have online voting systems in place would be able to or inclined to implement Internet-enabled voting at the national-level in response to the COVID-19 pandemic.[64]

There have been some adjustments in response to COVID-19 for national-level elections worldwide, in particular new hygiene and public health requirements, changes to voting hours and registration deadlines, and additional voting options for at-risk populations and those in isolation. While most of these changes do not themselves create new cyber security threats, they must be communicated clearly to voters so that voters can take advantage of the changes and remain confident that their election remains free and fair.[65] Some democracies have relied on the Internet, email, and text messages to communicate these changes, and cyber threat actors can target these communications—disrupting them, modifying them, or disseminating false information designed to look authentic.[66]

DISRUPTIONS FROM INCREASED DEMAND

Besides threat activity, online resources related to voting and elections, such as information pages, voter registration databases, and absentee ballot request portals, may face a higher than usual demand due to the pandemic. If not mitigated, such an increase could impede access to the resources voters need to participate in an election. This was a concern expressed by election officials in the US prior to their 2020 election.[67] However, we have not seen widespread outages due to higher-than-usual demand.

In addition, like many during the pandemic, some election management bodies have been forced to work remotely as they prepare for elections. Unless using cyber security best practices, remote work arrangements could introduce additional vulnerabilities as individuals access sensitive data related to their work over home Wi-Fi networks that are often poorly secured in comparison to corporate IT infrastructure.

GLOBAL TRENDS

GLOBAL BASELINE OF KNOWN EVENTS

INCE the *2019 Update: Cyber Threats to Canada's Democratic Process*, the Cyber Centre has continued to monitor cyber threat activity against democratic processes around the world. Consistent with our previous reports, we assume that our combined data sources underestimate the total number of events targeting democratic processes around the world. Based on our observations from 2015 to 2020, we have identified four trends.

TREND 1

State-sponsored cyber threat activity focuses on specific states and regions.

TREND 3

Targeting of democratic processes remains high.

TREND 2

Most cyber threat activity against democratic processes supports strategic objectives.

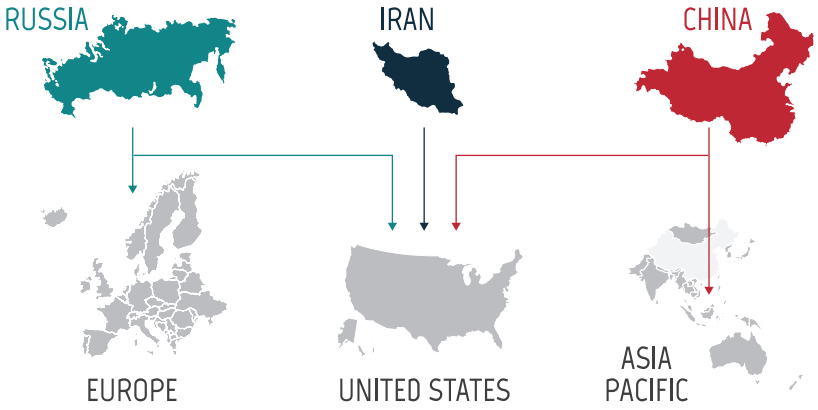
TREND 4

Cyber activity frequently impacts multiple targets within the democratic process.

TREND 1 STATE-SPONSORED CYBER THREAT ACTIVITY FOCUSES ON SPECIFIC STATES AND REGIONS

We assess that state-sponsored actors with ties to Russia, China, and Iran are responsible for the majority of cyber threat activity against democratic processes worldwide. Since 2015, over 90% of the cyber threat activity against democratic processes we observed by these states focused on countries of strategic significance to them. Specifically, most of the observed cyber activity targeting democratic processes attributed to Russia targeted the US, Ukraine, and other European states. Most of the cyber activity attributed to China targeted the US, Taiwan, and other countries in Asia and the Pacific. For Iran, most of this type of activity was against the US. The focus of state-sponsored threat activity against democratic processes is dictated by the specific interests of the threat actors and the states these actors perceive as threats to their regional and global objectives.

FIGURE 06 CYBER THREAT ACTORS TARGET STRATEGICALLY SIGNIFICANT STATES AND REGIONS

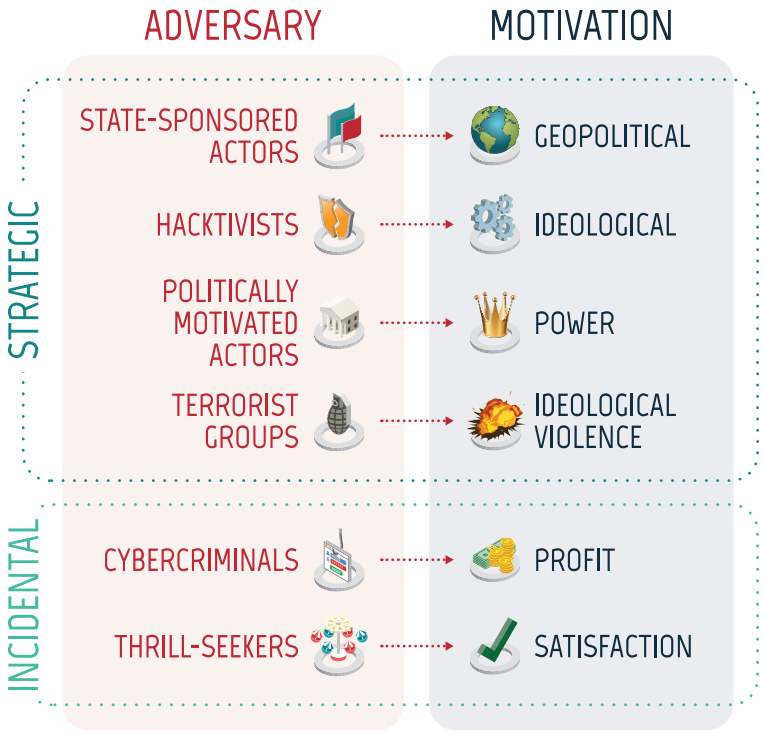


Since 2015, over **90%** of the cyber threat activity against democratic processes we observed by Russia, China, and Iran targeted states and regions of strategic significance to them.

TREND 2 MOST CYBER THREAT ACTIVITY AGAINST DEMOCRATIC PROCESSES SUPPORTS STRATEGIC OBJECTIVES

From 2015 to 2020, the vast majority of cyber threat activity affecting democratic processes around the world has been carried out to advance the strategic objectives of the threat actor. State-sponsored actors conducted 76% of the observed cyber threat activity against democratic processes for which we have an attribution. Given the potential payoff and relative ease of such an operation, we assess that state-sponsored cyber actors very likely have a greater interest in targeting democratic processes than other cyber actors. Incidental activity refers to cyber activity that impacted a democratic process but was not conducted to advance a strategic goal. Cyber threat activity by cybercriminals was the most common type of incidental activity, representing 8% of the observed cyber activity against democratic processes for which we have an attribution.

FIGURE 07 STRATEGIC AND INCIDENTAL OBJECTIVES



TREND 3 TARGETING OF DEMOCRATIC PROCESSES REMAINS HIGH

Consistent with our previous reporting, cyber threat activity targeting democratic processes remains high. After a steep increase in the proportion of elections targeted by cyber threat activity from 2015 to 2017, the proportion of democratic processes targeted by cyber threat activity related to worldwide elections, elections of OECD countries, and elections of G20 countries remained relatively stable from 2017 to 2020. These numbers do not include cases where domestic actors engaged in covert online influence activities within their own countries or where public relations firms were hired to conduct this type of activity. These firms have operated in at least 48 countries.[68]

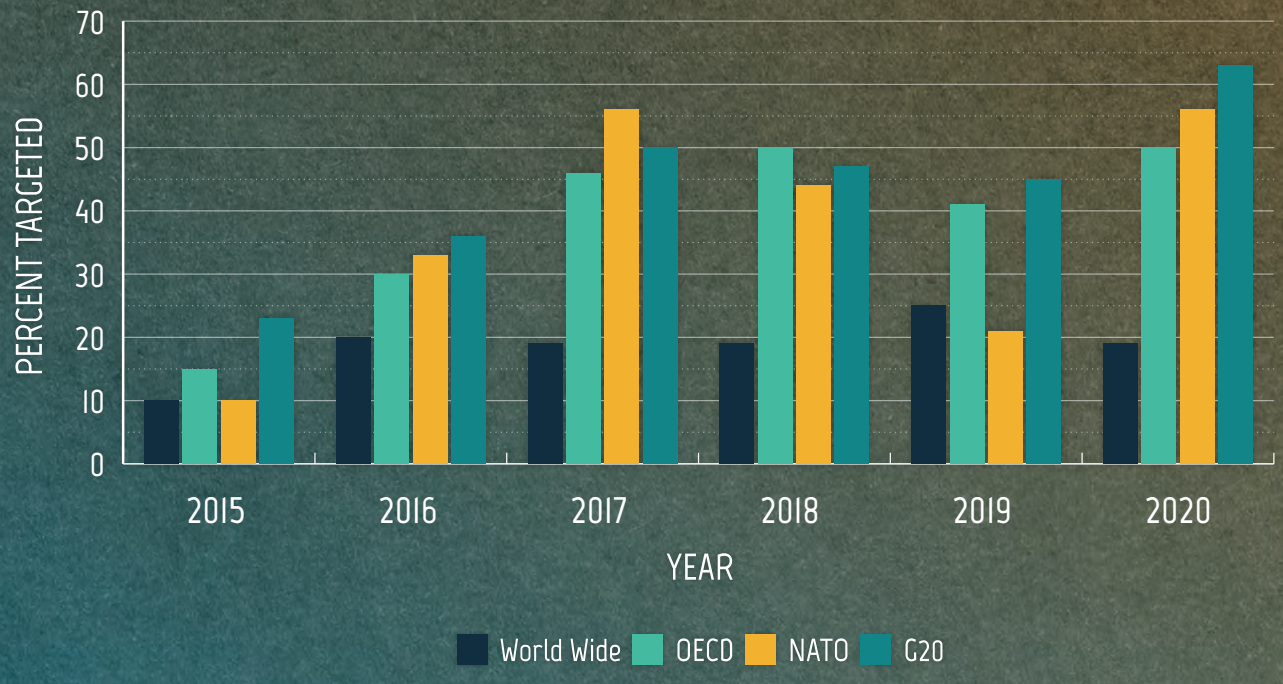
Although the percentage of elections that have been targeted each year has remained stable since 2017, these statistics do not capture variations in the amount of cyber activity experienced by each country—extensive cyber campaigns against one country and a single cyber event against another are each counted as one country targeted.

There are also countervailing trends that act to decrease the level of cyber threat activity targeting democratic processes. These trends include:

- efforts by social media companies to identify and remove accounts engaging in coordinated inauthentic behaviour online as well as flagging problematic content;
- greater media coverage and public awareness;
- mobilization of government bodies, non-governmental and research organizations, and civil society to counter false content;
- improved cyber security practices; and
- public attribution and legal indictments against threat actors.

Although there has yet to be a systematic study of the effectiveness of these practices, a comparison of the 2016 and 2020 US elections suggests that identifying and publicizing potential online foreign influence campaigns, strengthening the cyber security postures of organizations involved in the election, and improving social media companies' responses to malicious activity on their platforms can decrease the impact of hostile states' efforts to influence democratic processes through cyber means.[69] Taiwan's 2020 election also provides evidence that government investigations, civil society mobilization to counter false information, and social media company responses can mitigate foreign influence activity and protect democracy.[70]

FIGURE 08 CYBER THREAT ACTIVITY TARGETING DEMOCRATIC PROCESSES RELATED TO AN ELECTION



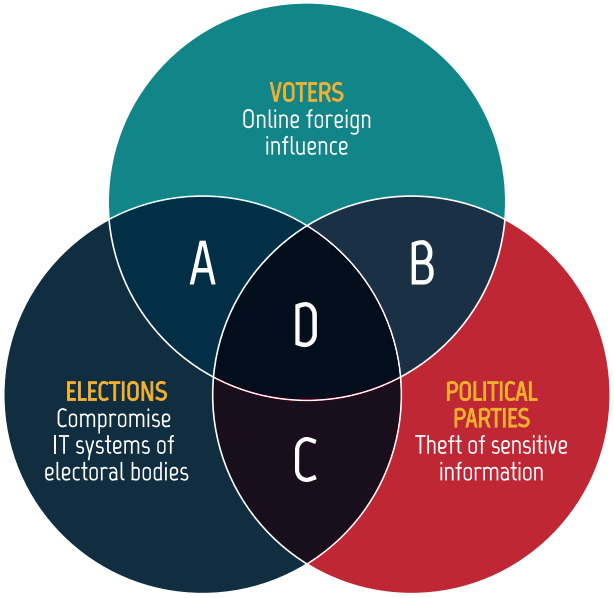
TREND 4 CYBER ACTIVITY FREQUENTLY IMPACTS MULTIPLE TARGETS WITHIN THE DEMOCRATIC PROCESS

Between 2015 and 2020, approximately one fifth of the democratic processes we studied were targeted by cyber threat activity. Of this, the majority (84%) experienced threats to more than one type of target—voters, political parties, and elections. In some cases, one incident impacted multiple types of targets, like a hack-and-leak operation that targets both a candidate and the voters exposed to the information.

Voters were victims more often than political parties and elections, being implicated in 87% of the surveyed democratic processes that experienced cyber threat activity from 2015 to 2020. Often voters were targeted in combination with political parties, elections, or both. Political parties were the second most common target after voters at 66%, followed by elections in third at 53%.

Figure 10 demonstrates that voters are targeted most often and that they are often targeted in conjunction with political parties, elections, or both. As a result, we assess that it is likely that cyber threat actors perceive targeting voters to be a more effective or efficient way to interfere with democratic processes or that targeting a combination of voters, political parties, and elections is more effective than targeting one group in isolation.

FIGURE 09 CYBER THREAT ACTIVITY CAN IMPACT MULTIPLE TARGETS



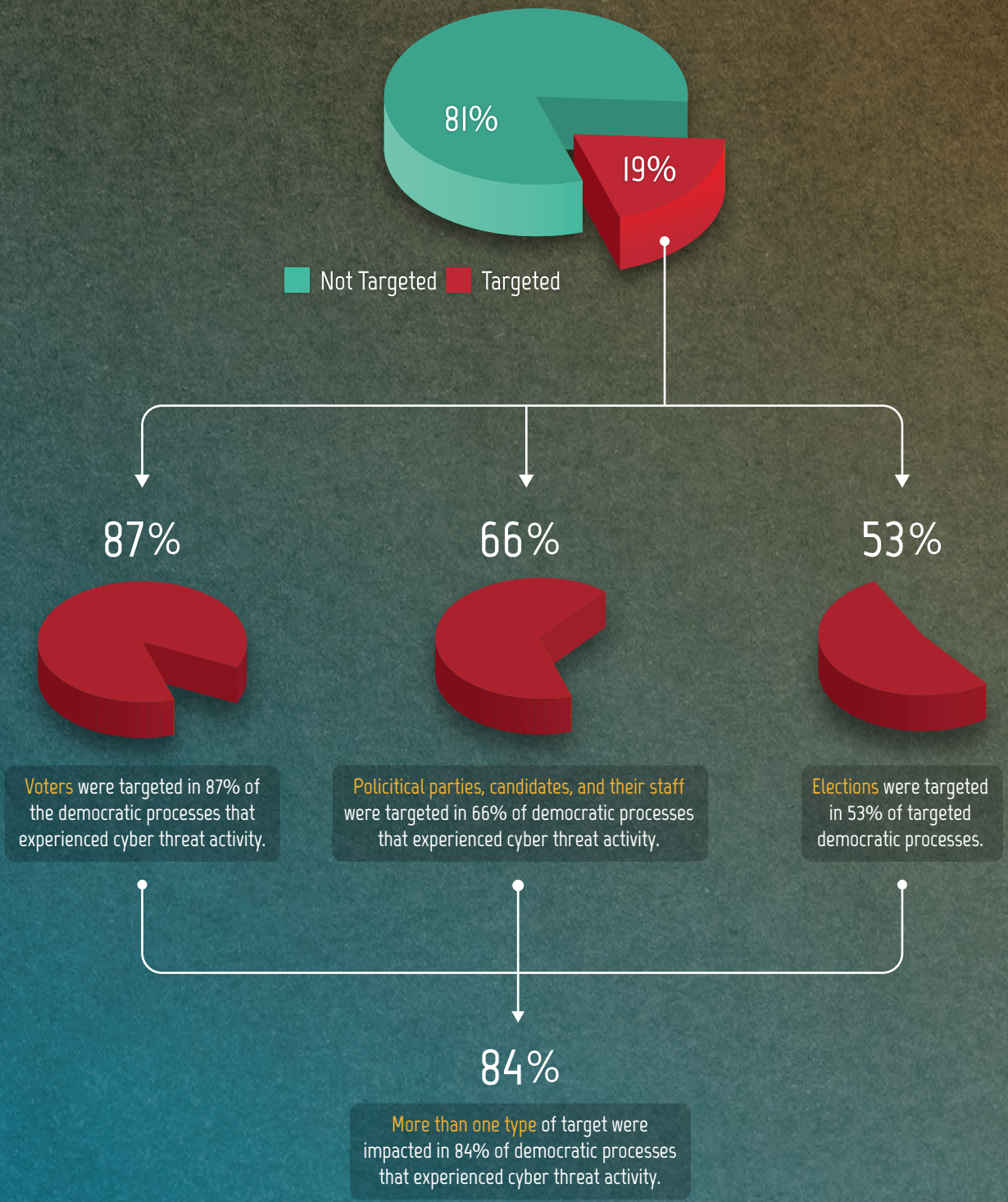
A Disrupt election website

B Hack and leak operation

C Compromise voting systems and alter the results

D Promote false allegations that a candidate benefited from voter fraud

FIGURE 10 | DEMOCRATIC PROCESSES RELATED TO ELECTIONS TARGETED WORLDWIDE, 2015–2020



CANADIAN CONTEXT

CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS

CANADA experiences only a fraction of the cyber activity we have observed targeting other democratic processes around the world. The Canadian federal election remains paper based, and Elections Canada has a number of legal, procedural, and IT measures in place that provide very robust protections against attempts to covertly manipulate election results in Canada.

Although federal elections in Canada are paper based, in sub-national elections, Canada is leading adoption of Internet-enabled voting, with some municipalities in Ontario and Nova Scotia adopting the technology and the Northwest Territories allowing absentee ballots to be cast online. At the national level, however, Canada continues to use paper ballots. See Figure 11 for an update on how elections are run at the federal, provincial/territorial, and municipal levels in Canada.

In addition, political parties at the national and provincial levels have voted online to select party leadership.[71] However, having these votes online makes them vulnerable to cyber threat actors who may want to change the results or sow distrust within a political party.

FIGURE II | TECHNOLOGY IN CANADIAN ELECTIONS

GOVERNMENT LEVEL	VOTER REGISTRY	VOTE	VOTE COUNT	DISSEMINATE RESULTS[1]
FEDERAL				
PROVINCIAL / TERRITORIAL	[2]	[3] [4]	[5]	
MUNICIPAL	[6]	[7]	[8] [9]	

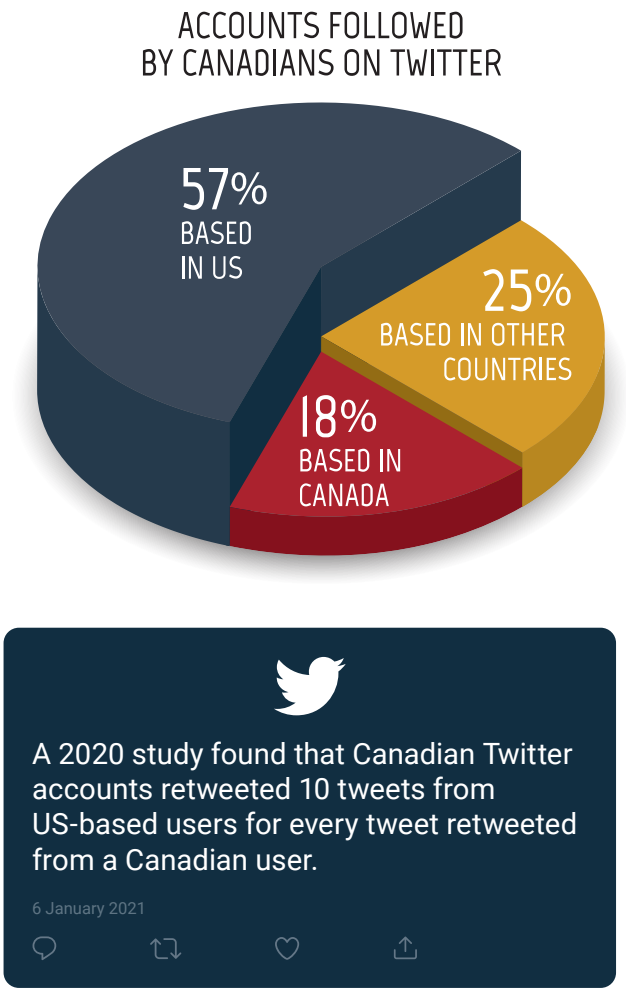
LEGEND

- Process is conducted using paper
- Process uses electronic devices that are not regularly connected to the Internet (e.g., to scan paper ballots or to store information digitally)
- Process is conducted on the Internet (e.g., Internet-enabled voting)

1. At all levels of government, unofficial results are provided on election night. In most cases, including at the federal level, election results are certified (i.e., official results) days or weeks following election night.
2. Online voter registration is available for Alberta, British Columbia, Manitoba, Newfoundland and Labrador, Nova Scotia, Northwest Territories, Ontario, Prince Edward Island, Saskatchewan, and Yukon.
3. New Brunswick uses electronic poll books. British Columbia is planning to implement them in the future.
4. Some voters may cast their absentee ballot online in the Northwest Territories.
5. New Brunswick and Ontario use electronic devices to count votes. British Columbia is planning to implement them in the future.
6. Some municipalities across Canada offer online voter registration.
7. Some municipalities in Nova Scotia and Ontario use Internet-enabled voting.
8. Some municipalities use machines to count paper ballots.
9. For municipalities that use Internet-enabled voting, the count is also online.

We assess that Canada remains a lower-priority target for online foreign influence activity relative to some other countries. However, Canada's media ecosystem is closely intertwined with that of the US and other allies, which means that when their citizens are targeted, Canadians become exposed to online influence as a type of collateral damage. In 2020 and early 2021 we have seen how disinformation and misinformation that gain traction in the US and in other allied countries can impact Canadians.

FIGURE 12 | CANADIANS ON TWITTER



Tayler Owen, et al. | Understanding vaccine hesitancy in Canada: attitudes, beliefs, and the information ecosystem | Media Ecosystem Observatory | 6 January 2021 | https://files.cargocollective.com/c745315/meo vaccine hesistancy.pdf

In 2019, the Critical Election Incident Public Protocol (CEIPP) was established as the mechanism for communicating with Canadians in a clear, transparent, and impartial manner if there had been an incident that threatened Canada's ability to have a free and fair election.[72] No threats met the CEIPP's high threshold for public announcement during the 2019 General Election, but the panel responsible for making that determination was prepared to intervene if needed. In addition, other mitigation measures were put in place, including efforts to protect voters, political parties, and elections. See Figure 13 for examples of these measures.

FIGURE 13 | MEASURES TO PROTECT CANADA'S DEMOCRATIC PROCESS

CRITICAL ELECTION INCIDENT PUBLIC PROTOCOL
- Mechanism for communicating with Canadians if an incident were to occur that threatens Canada's ability to have a free and fair election

SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE
- Comprised of officials from CSE, the Canadian Security Intelligence Service, Global Affairs Canada, and the Royal Canadian Mounted Police

CYBER CENTRE ADVICE AND BRIEFINGS
- Hotline with Elections Canada
- Briefings with political parties
- Cyber security resources for the public

EFFORTS OF ELECTIONS CANADA
- Improved cyber security posture
- Monitored information environment
- Corrected false or misleading information about electoral process

AGREEMENTS WITH SOCIAL MEDIA AND TECHNOLOGY COMPANIES
- Canada Declaration on Electoral Integrity

DIGITAL LITERACY
- Digital Citizen Initiative
- Digital Citizen Research Program
- Public Policy Forum Digital Democracy Project

COVID-19 AND THE OUTLOOK FOR DEMOCRATIC PROCESSES IN CANADA

Elections Canada has implemented measures to increase the capacity and convenience of the vote-by-mail system to meet a potential increase in demand and has indicated that an increased volume of mail-in ballots could delay the release of election results.[73] Some of these changes, such as allowing more voters to apply online to vote by mail or incorporating optical character recognition to help read some identification documents, increase the cyber threat surface. However, these changes are based on pre-existing systems, are being carefully tested and validated prior to implementation, and include a human fallback when needed. Therefore, we assess that, on balance, these changes do not substantially change the cyber threat to Canada's democratic process, especially as Canada remains a lower-priority target compared to other states and has a broad set of mitigations in place to defend Canadian elections.

COVID-19-related changes to Canadian elections, such as an increase in voting by mail or changes to voting locations, offer additional avenues for online foreign influence, providing opportunities for cyber threat actors to spread false information related to electoral processes and results. We assess that it is very likely that false information connecting voting by mail to voter fraud will circulate in Canada in relation to the next federal election. However, we assess that these false narratives will almost certainly be less prominent and less influential than they were in the US during their 2020 election.

The Cyber Centre has procedures in place to counter fraudulent attempts to imitate the Government of Canada online. Since March 2020, the Cyber Centre has worked with partners to take down more than 8,600 websites, social media accounts, and email servers impersonating the Government of Canada.

As discussed in the *NCTA 2020*, COVID-19 has pushed many organizations to remote work, adding additional vulnerabilities. While Elections Canada has also shifted its operations toward a work-from-home posture, including delivering training related to the election online, we assess that it is unlikely that sensitive information held by Elections Canada will be compromised by cyber threat actors and very unlikely that cyber activity will disrupt critical voting infrastructure. As mentioned above, Canadian federal elections are paper based, with robust defences in place to ensure the legitimacy of the results.

CASE STUDY: CANADIAN PROVINCIAL ELECTIONS DURING THE COVID-19 PANDEMIC

In 2020, the provinces of New Brunswick, Nova Scotia, British Colombia, and Saskatchewan held elections during the COVID-19 pandemic. While all four experienced a slight dip in turnout, they logged record numbers of mail-in votes and online registrations. Each province made changes to how the vote was conducted to ensure voters could vote safely, such as implementing public health and sanitary measures at polling stations, adding additional voting days and voting locations, providing additional safe and accessible voting opportunities to at-risk voters and communities, and ensuring voters who could not physically go to a polling station could still cast their ballots. All four provinces also provided guidance to political parties and candidates about how to campaign safely during the COVID-19 pandemic. Several political parties held virtual town halls, increased digital and mail-in advertising, and relied heavily on canvassing via phone.[74] Candidates also engaged in physically distanced in-person campaigning.[75] Despite this increased reliance on technological tools and the online space, there was no evidence of sophisticated online foreign influence campaigns or cyber activity targeting voters, political parties, or the elections themselves.

If the next Canadian federal election happens before the COVID-19 pandemic is over, Canadian political parties and candidates will almost certainly conduct more campaign activities online and use more online tools than in the past. We assess that it is very likely that the online activities of political parties and candidates will be targeted by cyber threat activity. We assess that this activity is very unlikely to be part of a sophisticated cyber campaign against a particular Canadian political party or candidate.

Consistent with our judgement in the *2019 Update: Cyber Threats to Canada's Democratic Process*, we assess that an increasing number of threat actors have the cyber tools, the organizational capacity, and a sufficiently advanced understanding of Canada's political landscape to direct cyber activity against future Canadian federal elections, should they have the strategic intent. We judge it very likely that Canadian voters will encounter some form of foreign cyber interference ahead of, and during, the next federal election. However, we consider foreign interference on the scale of state-sponsored activity against US elections to be improbable in Canada at this time.

CONCLUSION

CANADA remains a lower-priority target for cyber threat activity targeting its democratic process relative to some other countries. However, we judge it very likely that Canadian voters will encounter some form of foreign cyber interference ahead of, and during, the next federal election, although it is unlikely to be at the scale seen in the US.

The COVID-19 pandemic has altered democratic processes and has affected how elections are held, bringing changes that may extend beyond the duration of the pandemic. Some of these changes have increased the threat surface available to cyber threat actors. COVID-19 has also created new narratives that can be used by threat actors to undermine the perceived legitimacy of an election or weaken trust in democratic institutions, such as narratives falsely linking mail-in voting and voter fraud.

This assessment focuses on online foreign influence against democratic processes, but it is important to note how pervasive falsehoods on social media and in the domestic information ecosystem create opportunities that foreign cyber threat actors can exploit to covertly disseminate disinformation.

The Government of Canada's *Security and Intelligence Threats to Elections (SITE) Task Force*, comprised of officials from CSE, the Canadian Security Intelligence Service, Global Affairs Canada, and the Royal Canadian Mounted Police, continues to help the government assess and respond to foreign threats to Canada's electoral process.

Broader Government of Canada efforts to safeguard elections and democratic institutions, such as the Plan to Protect Canada's Democracy, can be found on the *Protecting Democracy* web page.

The Cyber Centre provides cyber security advice and guidance to all major political parties, in part through a *Cyber Security Guide for Campaign Teams*, and works closely with Elections Canada to protect its infrastructure. The Cyber Centre has also published *Cyber Security Guidance for Elections Authorities* and a *Cyber Security Playbook for Elections Authorities*.

We encourage Canadians to consult the Cyber Centre's *Focused Cyber Security Advice and Guidance During COVID-19*. CSE's *Get Cyber Safe* campaign will also continue to publish relevant advice and guidance to inform Canadians about cyber security and the steps they can take to protect themselves online.

ENDNOTES

1 **Partnerships and organizations** | *Global Affairs Canada* | 27 March 2020 | https://www.international.gc.ca/world-monde/international_relations-relations_internationales/partnerships_organizations-partenariats_organisations.aspx

2 Simon Kemp | **Digital 2021: Canada** | *DataReportal* | 9 February 2021 | https://datareportal.com/reports/digital-2021-canada

Canadian Internet Use Survey | *Statistics Canada* | 29 October 2019 | https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm

3 Tom Simonite | **What Happened to the Deepfake Threat to the Election?** | *Wired* | 16 November 2020 | https://www.wired.com/story/what-happened-deepfake-threat-election

4 Tim Huwang | **Deepfakes - Primer and Forecast** | *NATO Strategic Communications Centre of Excellence* | May 2020 | https://stratcomcoe.org/publications/deepfakes-primer-and-forecast/42

5 Tom B. Brown, et al | **Language Models are Few-Shot Learners** | *OpenAI* | 22 July 2020 | https://arxiv.org/abs/2005.14165

6 Max Weiss | **Deepfake Bot Submissions to Federal Public Comment Websites Cannot Be Distinguished from Human Submissions** | *Journal of Technology Science* | 17 December 2019 | https://techscience.org/a/2019121801

7 **Foreign Threats to the 2020 US Federal Elections** | *National Intelligence Council* | 10 March 2021 | https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

8 **The Long Fuse: Misinformation and the 2020 Election** | *Election Integrity Partnership* | 2021 | https://www.eipartnership.net/report

9 Gordon Pennycook and David G. Rand | **Research note: Examining false beliefs about voter fraud in the wake of the 2020 Presidential Election** | *Harvard Kennedy School* | 11 January 2021 | https://misinforeview.hks.harvard.edu/article/research-note-examining-false-beliefs-about-voter-fraud-in-the-wake-of-the-2020-presidential-election

10 **Global overview of COVID-19: Impact on elections** | *International Institute for Democracy and Electoral Assistance* | Accessed on 19 February 2021 | https://www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections

11 **Featured Elections Held and Mitigation Measures Taken During COVID-19** | *International Foundation for Electoral Systems* | 21 October 2020 | https://www.ifes.org/sites/default/files/elections_held_and_mitigating_measures_taken_during_covid-19.pdf

Lindsay Maizland | **How Countries Are Holding Elections During the COVID-19 Pandemic** | *Council on Foreign Relations* | 17 September 2020 | https://www.cfr.org/backgrounder/how-countries-are-holding-elections-during-covid-19-pandemic

Vote by Mail: International Practice During COVID-19 | *International Foundation for Electoral Systems* | 28 October 2020 | https://www.ifes.org/publications/vote-mail-international-practice-during-covid-19

12 Erik Asplund, et al | **Elections and COVID-19: How election campaigns took place in 2020** | *International Institute for Democracy and Electoral Assistance* | 2 February 2020 | https://www.idea.int/news-media/news/elections-and-covid-19-how-election-campaigns-took-place-2020

Julian E. Barnes | **Schiff Sees Rise in Russian Disinformation as Trump Attacks Mail-In Voting** | *New York Times* | 29 September 2020 | https://www.nytimes.com/2020/09/29/us/politics/mail-in-voting-russian-disinformation.html

13 Josh Margolin and Lucien Bruggeman | **Russia is 'amplifying' claims of mail-in voter fraud, intel bulletin warns** | *ABC News* | 3 September 2020 | https://abcnews.go.com/Politics/russia-amplifying-claims-mail-voter-fraud-intel-bulletin/story?id=72799959

Kirsten Korosec | **'Stay home' robocalls on Election Day prompt warnings, investigation** | *TechCrunch* | 3 November 2020 | https://techcrunch.com/2020/11/03/stay-home-robocalls-on-election-day-prompt-warnings-investigation/?guccounter=1

14 **Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training** | *United Nations Educational, Scientific and Cultural Organization* | Accessed 25 February 2021 | https://en.unesco.org/fightfakenews

Claire Wardle and Hossein Derakhshan | **Information disorder: Toward an interdisciplinary framework for research and policy making** | *Council of Europe* | 27 September 2017 | https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

15 **Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training** | *United Nations Educational, Scientific and Cultural Organization* | Accessed 25 February 2021 | https://en.unesco.org/fightfakenews

Claire Wardle and Hossein Derakhshan | **Information disorder: Toward an interdisciplinary framework for research and policy making** | *Council of Europe* | 27 September 2017 | https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

16 Scott Brennen, Felix Simon, Philip N. Howard, and Rasmus Kleis Nielsen | **Types, sources, and claims of COVID-19 misinformation** | *Reuters Institute* | 7 April 2020 | https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation

17 Serena Giusti and Elisa Piras (editors) | **Democracy and Fake News: Information Manipulation and Post-Truth Politics** | *Routledge* | 2020 | https://doi.org/10.4324/9781003037385

18 **Uganda elections 2021: Facebook shuts government-linked accounts** | *BBC News* | 11 January 2021 | https://www.bbc.com/news/world-africa-55623722

19 Stephen Kafeero | **Uganda has cut off its entire internet hours to its election polls opening** | *Quartz Africa* | 13 January 2021 | https://qz.com/africa/1957137/uganda-cuts-off-internet-ahead-of-election-polls-opening

Stephen Kafeero | **Uganda has shut down all social media two days ahead of a tense election** | *Quartz Africa* | 12 January 2021 | https://qz.com/africa/1956188/uganda-shuts-social-media-ahead-of-election-army-out-in-streets

20 Felicia Anthonio, Carolyn Tackett, Leanna Garfield, and Sage Cheng | **How internet shutdowns are threatening 2020 elections, and what you can do about it** | *Access Now* | 15 October 2020 | https://www.accessnow.org/internet-shutdowns-2020-elections

Miguel Angel Lara Otaola | **Annex: Internet restriction during elections** | *ACE Electoral Knowledge Network* | Accessed 25 February 2021 | https://aceproject.org/ace-en/topics/me/annex/case-studies/internet-restriction-during-elections

21 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 January 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

22 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 January 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

23 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 January 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

Andy Carvin | **Operation Carthage: How a Tunisian company conducted influence operations in African presidential elections** | *Atlantic Council* | 5 June 2020 | https://www.atlanticcouncil.org/wp-content/uploads/2020/06/operation-carthage-002.pdf

McKay Coppins | **The Billion-Dollar Disinformation Campaign to Reelect the President** | *The Atlantic* | March 2020 | https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530

24 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 January 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

25 Craig Timberg and Tony Romm | **Facebook shuts down Israel-based disinformation campaigns as election manipulation increasingly goes global** | *Washington Post* | 16 May 2019 | https://www.washingtonpost.com/technology/2019/05/16/facebook-shuts-down-israel-based-disinformation-campaigns-election-manipulation-increasingly-goes-global

26 **The Making of QAnon: A Crowdsourced Conspiracy** | *Bellingcat* | 7 January 2021 | https://www.bellingcat.com/news/americas/2021/01/07/the-making-of-qanon-a-crowdsourced-conspiracy

27 Brenna Owen | **Canada not immune to QAnon as pandemic fuels conspiracy theories, experts say** | *CTV News* | 22 December 2020 | https://www.ctvnews.ca/sci-tech/canada-not-immune-to-qanon-as-pandemic-fuels-conspiracy-theories-experts-say-1.5226762

Matthew Remski | **When QAnon Came to Canada** | *The Walrus* | 3 December 2021 | https://thewalrus.ca/when-qanon-came-to-canada

Melanie Smith | **Interpreting Social Qs: Implications of the Evolution of QAnon** | *Graphika* | 24 August 2020 | https://graphika.com/reports/interpreting-social-qs-implications-of-the-evolution-of-qanon

28 A 2021 report by The Soufan Center links Russia, China, Iran, and Saudi Arabia with QAnon. However, there is some debate about its methodology | Jason Blazakis, et al | **Quantifying the Q Conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon** | *The Soufan Center* | April 2021 | https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon

David Gilbert | **No, Russia and China Didn't 'Weaponize' QAnon. It's a Homegrown Nightmare** | *Vice* | 22 April 2021 | https://www.vice.com/en/article/pkby9z/no-russia-and-china-didnt-weaponize-qanon-its-a-homegrown-nightmare

29 Joseph Menn | **QAnon received earlier boost from Russian accounts on Twitter, archives show** | *Reuters* | 2 November 2020 | https://www.reuters.com/article/us-usa-election-qanon-cyber-idUSKBN27I18I

30 Joseph Menn | **Russian-backed organizations amplifying QAnon conspiracy theories, researchers say** | *Reuters* | 24 August 2020 | https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T

31 Shayan Sardarizadeh | **US election 2020: Twitter removes Iranian accounts disrupting debate** | *BBC News* | 1 October 2020 | https://www.bbc.com/news/election-us-2020-54373314

32 Joseph Menn | **Russian-backed organizations amplifying QAnon conspiracy theories, researchers say** | *Reuters* | 24 August 2020 | https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T

33 Jen Kirby | **US intelligence officials say Iran and Russia obtained voter registration information to interfere in election** | *Vox* | 21 October 2020 | https://www.vox.com/2020/10/21/21527784/iran-russia-fbi-ratcliffe-voter-registration-emails

34 Sheera Frenkel | **A Freelance Writer Learns He Was Working for the Russians** | *New York Times* | 2 September 2020 | https://www.nytimes.com/2020/09/02/technology/peacedata-writer-russian-misinformation.html

Jack Stubbs | **Duped by Russia, freelancers ensnared in disinformation campaign by promise of easy money** | *Reuters* | 2 September 2020 | https://www.reuters.com/article/us-usa-election-facebook-russia-idUSKBN25T35E

35 Stephan Heblich | **The effect of the internet on voting behavior** | *IZA World of Labor* | Accessed 25 February 2021 | https://wol.iza.org/articles/effect-of-internet-on-voting-behavior/long

Nic Newman, et al | **Reuters Institute Digital News Report 2020** | *Reuters Institute* | June 2020 | https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf

36 Chris Meserole | **How misinformation spreads on social media—And what to do about it** | *Brookings Institution* | 9 May 2018 | https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it

Jack Nicas | **How YouTube Drives People to the Internet's Darkest Corners** | *Wall Street Journal* | 7 February 2018 | https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478

Trudeaus and Trudeaun'ts – memes polarize in Canadian elections | *Digital Forensic Research Lab* | 19 November 2019 | https://medium.com/dfrlab/trudeaus-and-trudeaunts-memes-have-an-impact-during-canadian-elections-4c842574dedc

Katherine J. Wu | **Radical ideas spread through social media. Are the algorithms to blame?** | *PBS NOVA* | 28 March 2019 | https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms

37 Julia Alexander | **YouTube claims its crackdown on borderline content is actually working** | *The Verge* | 3 December 2019 | https://www.theverge.com/2019/12/3/20992018/youtube-borderline-content-recommendation-algorithm-news-authoritative-sources

Julia Alexander | **YouTube introducing changes to give people more control over recommended videos** | *The Verge* | 26 June 2019 | https://www.theverge.com/2019/6/26/18759840/youtube-recommendation-videos-homepage-changes-algorithm-harmful-content

Josh Constine | **Facebook will change algorithm to demote "borderline content" that almost violates policies** | *TechCrunch* | 15 November 2018 | https://techcrunch.com/2018/11/15/facebook-borderline-content

Ronald J. Deibert | **Reset: Reclaiming the Internet for Civil Society** | *House of Anansi Press* | 2020

Kaveh Waddell | **On Social Media, Only Some Lies Are Against the Rules** | *Consumer Reports* | 13 August 2020 | https://www.consumerreports.org/social-media/social-media-misinformation-policies

Queenie Wong, Andrew Morse, and Richard Nieva | **Here's how social media companies are fighting election misinformation** | *CNet* | 7 November 2020 | https://www.cnet.com/news/heres-how-social-media-companies-are-fighting-election-misinformation

38 Kevin Roose | **'Shut the Site Down,' Says the Creator of 8chan, a Megaphone for Gunmen** | *New York Times* | 4 August 2019 | https://www.nytimes.com/2019/08/04/technology/8chan-shooting-manifesto.html

39 Ben Nimmo | **Russian Narratives on Election Fraud** | *Election Integrity Partnership* | Accessed 25 February 2021 | https://www.eipartnership.net/rapid-response/russian-narratives-on-election-fraud

40 **When Twitter Bans Extremists, GAB Puts Out the Welcome Mat** | *Anti-Defamation League* | 11 March 2019 | https://www.adl.org/blog/when-twitter-bans-extremists-gab-puts-out-the-welcome-mat

41 **Step into My Parler** | *Graphika* | 1 October 2020 | https://graphika.com/reports/step-into-my-parler

42 Nicole Hong | **WeChat, Wild Rumors and All, Is Their Lifeline. Washington May End That** | *New York Times* | 5 October 2020 | https://www.nytimes.com/2020/10/05/nyregion/us-wechat-ban.html

Paul Mozur | **Forget TikTok. China's Powerhouse App is WeChat, and Its Power Is Sweeping** | *New York Times* | 4 September 2020 | https://www.nytimes.com/2020/09/04/technology/wechat-china-united-states.html

Joe Fitzgerald Rodriguez, Shannon Lin, and Jessica Huseman | **Misinformation Image on WeChat Attempts to Frighten Chinese Americans Out of Voting** | *ProPublica* | 2 November 2020 | https://www.propublica.org/article/misinformation-image-on-wechat-attempts-to-frighten-chinese-americans-out-of-voting

Yaqiu Wang | **WeChat Is a Trap for China's Diaspora** | *Human Rights Watch* | 14 August 2020 | https://www.hrw.org/news/2020/08/14/wechat-trap-chinas-diaspora

Jeanne Whalen | **Chinese censorship invades the U.S. via WeChat** | *Washington Post* | 7 January 2021 | https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban

43 Harrison Mantas | **Growing usage of encrypted messaging apps could make it harder to combat misinformation** | *Poynter* | 14 January 2021 | https://www.poynter.org/fact-checking/2021/growing-usage-of-encrypted-messaging-apps-could-make-it-harder-to-combat-misinformation

44 Kyle Daly and Sarah Fischer | **The online far right is moving underground** | *Axios* | 12 January 2021 | https://www.axios.com/the-online-far-right-is-moving-underground-e429d45d-1b30-46e0-82a3-6e240bf44fef.html

45 Jasmine Garsd | **WhatsApp's privacy features make it a hotbed for COVID-19 hoaxes** | *Marketplace* | 23 March 2020 | https://www.marketplace.org/2020/03/23/misinformation-about-covid19-spread-whatsapp

46 Lindsay Maizland | **How Countries Are Holding Elections During the COVID-19 Pandemic** | *Council on Foreign Relations* | 17 September 2020 | https://www.cfr.org/backgrounder/how-countries-are-holding-elections-during-covid-19-pandemic

47 Jocelyn Woolbright | **Election Cybersecurity: Protecting the 2020 U.S. Elections** | *Cloudflare* | 17 August 2020 | https://blog.cloudflare.com/election-cybersecurity-preparing-for-the-2020-u-s-elections

48 Devin Coldewey | **Trump's campaign website hacked by cryptocurrency scammers** | *TechCrunch* | 27 October 2020 | https://techcrunch.com/2020/10/27/trumps-campaign-website-hacked-by-cryptocurrency-scammers

49 Axel F. | **Emotet Makes Timely Adoption of Political Elections Lures** | *Proofpoint* | 1 October 2020 | https://www.proofpoint.com/us/blog/threat-insight/emotet-makes-timely-adoption-political-and-elections-lures

50 Katie Shepherd | **Racist trolls hijacked a Zoom town hall to hurl slurs at Connecticut's first Black congresswoman** | *Washington Post* | 14 October 2020 | https://www.washingtonpost.com/nation/2020/10/14/jahana-hayes-zoom-racial-slurs

Byron Tau | **Scammers, hackers and spies hit trail** | *Politico* | 7 July 2014 | https://www.politico.com/story/2014/07/campaign-technology-data-security-voter-information-108585

51 **Federal Liberal leadership race: Countdown to the vote** | *CityNews* | 1 April 2013 | https://toronto.citynews.ca/2013/04/01/federal-liberal-leadership-race-countdown-to-the-vote

Ryan Van Horne | **Nova Scotia Liberal Party opens up leadership voting to all members** | *CTV News* | 14 September 2020 | https://atlantic.ctvnews.ca/nova-scotia-liberal-party-opens-up-leadership-voting-to-all-members-1.5104224

52 Janosch Delcker | **Cyber threat looms large over German election** | *Deutche Welle* | 6 May 2021 | https://www.dw.com/en/cyber-threat-looms-large-over-german-election/a-56775960

53 **Election Considerations in the Pacific During an Infodemic** | *International Foundation for Electoral Systems* | 20 July 2020 | https://www.ifes.org/news/election-considerations-pacific-during-infodemic

Joe Biden hosts drive-in campaign rallies amid coronavirus pandemic ahead of US election | *ABC News* | 19 October 2020 | https://www.abc.net.au/news/2020-10-19/joe-biden-rally-drive-in-us-election-votes-donald-trump/12781206

A look at other Canadian elections that took place during the COVID-19 pandemic | *CityNews* | 15 January 2021 | https://ottawa.citynews.ca/national-news/a-look-at-other-canadian-elections-that-took-place-during-the-covid-19-pandemic-3266403

David McGrane | **Campaigning in Canada during a pandemic** | *Policy Options* | 28 December 2020 | https://policyoptions.irpp.org/magazines/december-2020/campaigning-in-canada-during-a-pandemic

54 Benjamin Barber | **Deep canvassing effort in Georgia aims to flip the U.S. Senate** | *Facing South* | 17 December 2020 | https://www.facingsouth.org/2020/12/deep-canvassing-effort-georgia-aims-flip-us-senate

B.C.'s virtual COVID-19 election campaign lacks human touch: expert | *CityNews* | 9 October 2020 | https://ottawa.citynews.ca/national-news/bcs-virtual-covid-19-election-campaign-lacks-human-touch-expert-2784083

Kendall Karson and Benjamin Siegel | **2020 Democratic National Convention Viewer's Guide: Biden anchored in Delaware, a virtual nomination and history to be made** | *ABC News* | 17 August 2020 | https://abcnews.go.com/Politics/2020-democratic-national-convention-viewers-guide-biden-anchored/story?id=72234720

Lisa Mascaro | **To door knock or not? Campaigning for Congress in COVID era** | *AP News* | 14 September 2020 | https://apnews.com/article/senate-elections-health-elections-philadelphia-campaigns-94c06fe50821979d6b4280968178e5aa

Marianna Sotomayor | **Biden's first virtual event encounters technological glitches** | *NBC News* | 14 March 2020 | https://www.nbcnews.com/politics/meet-the-press/blog/meet-press-blog-latest-news-analysis-data-driving-political-discussion-n988541/ncrd1158951#blogHeader

Trudeau takes questions in Liberal party's first-ever virtual fundraiser | *CTV News* | 10 September 2020 | https://www.ctvnews.ca/politics/trudeau-takes-questions-in-liberal-party-s-first-ever-virtual-fundraiser-1.5100439

2020 Convention November 7 | *Green Party of Ontario* | Accessed 1 March 2021 | https://gpo.ca/convention2020

55 **Adapting to the New Normal: Political Parties During Lockdown and Social Distancing** | *International Institute for Democracy and Electoral Assistance* | 2020 | https://www.idea.int/sites/default/files/publications/adapting-to-the-new-normal-political-parties-during-lockdown-and-social-distancing.pdf

Ricki Harris | **How the Pandemic Reshaped Election Campaigns—Maybe Forever** | *Wired* | 21 August 2020 | https://www.wired.com/story/pandemic-reshaped-2020-election-campaigns-democrats-republicans

56 Antonio Spinelli | **Managing Elections under the COVID-19 Pandemic: The Republic of Korea's Crucial Test** | *International Institute for Democracy and Electoral Assistance Technical Paper 2/2020* | 30 July 2020 | https://www.idea.int/sites/default/files/publications/managing-elections-during-pandemic-republic-korea-crucial-test.pdf

57 **Vote by Mail: International Practice During COVID-19** | *International Foundation for Electoral Systems* | 28 October 2020 | https://www.ifes.org/publications/vote-mail-international-practice-during-covid-19

58 Meredith Applegate, Thomas Chanussot, and Vladlen Basysty | **Considerations on Internet Voting: An Overview for Electoral Decision-Makers** | *International Foundation for Electoral Systems White Paper* | 7 April 2020 | https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

59 Meredith Applegate, Thomas Chanussot, and Vladlen Basysty | **Considerations on Internet Voting: An Overview for Electoral Decision-Makers** | *International Foundation for Electoral Systems White Paper* | 7 April 2020 | https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

60 **Belarus: EU imposes sanctions for repression and election falsification** | *Council of the European Union* | 2 October 2020 | https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/belarus-eu-imposes-sanctions-for-repression-and-election-falsification

Jordan Fabian | **Belarus Election 'Fraudulent,' White House Spokeswoman Says** | *BNN Bloomberg* | 9 September 2020 | https://www.bnnbloomberg.ca/belarus-election-fraudulent-white-house-spokeswoman-says-1.1491536

Statement by Minister Champagne on Belarusian presidential elections | *Global Affairs Canada* | 17 August 2020 | https://www.canada.ca/en/global-affairs/news/2020/08/statement-by-minister-champagne-on-belarusian-presidential-elections.html

61 Nika Aleksejeva | **Lukashenka's regime confused by protest-driven cyber attacks** | *Digital Forensic Research Lab.* | 1 October 2020 | https://medium.com/dfrlab/lukashenkas-regime-confused-about-belarus-cyber-partisans-activity-29f4bb530956

62 Nika Aleksejeva | **Lukashenka's regime confused by protest-driven cyber attacks** | *Digital Forensic Research Lab* | 1 October 2020 | https://medium.com/dfrlab/lukashenkas-regime-confused-about-belarus-cyber-partisans-activity-29f4bb530956

63 Nika Aleksejeva | **Lukashenka's regime confused by protest-driven cyber attacks** | *Digital Forensic Research Lab* | 1 October 2020 | https://medium.com/dfrlab/lukashenkas-regime-confused-about-belarus-cyber-partisans-activity-29f4bb530956

64 Meredith Applegate, Thomas Chanussot, and Vladlen Basysty | **Considerations on Internet Voting: An Overview for Electoral Decision-Makers** | *International Foundation for Electoral Systems White Paper* | 7 April 2020 | https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

65 **Election Considerations in the Pacific During an Infodemic** | *International Foundation for Electoral Systems* | 20 July 2020 | https://www.ifes.org/news/election-considerations-pacific-during-infodemic

66 **Featured Elections Held and Mitigation Measures Taken During COVID-19** | *International Foundation for Electoral Systems* | 21 October 2020 | https://www.ifes.org/sites/default/files/elections_held_and_mitigating_measures_taken_during_covid-19.pdf

Lindsay Maizland | **How Countries Are Holding Elections During the COVID-19 Pandemic** | *Council on Foreign Relations* | 17 September 2020 | https://www.cfr.org/backgrounder/how-countries-are-holding-elections-during-covid-19-pandemic

67 Tim Starks | **Looking back at a landmark law on government IT modernization** | *Politico* | 10 August 2020 | https://www.politico.com/newsletters/weekly-cybersecurity/2020/08/10/looking-back-at-a-landmark-law-on-government-it-modernization-789782

68 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 January 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

69 Scott Jasper | **Why foreign election interference fizzled in 2020** | *Atlantic Council* | 23 November 2020 | https://www.atlanticcouncil.org/blogs/new-atlanticist/why-foreign-election-interference-fizzled-in-2020

70 **When Election Interference Fails** | *Council on Foreign Relations* | 29 January 2020 | https://www.cfr.org/blog/when-election-interference-fails

71 **Federal Liberal leadership race: Countdown to the vote** | *CityNews* | 1 April 2013 | https://toronto.citynews.ca/2013/04/01/federal-liberal-leadership-race-countdown-to-the-vote

Ryan Van Horne | **Nova Scotia Liberal Party opens up leadership voting to all members** | *CTV News* | 14 September 2020 | https://atlantic.ctvnews.ca/nova-scotia-liberal-party-opens-up-leadership-voting-to-all-members-1.5104224

72 James Judd | **Report on the assessment of the Critical Election Incident Public Protocol** | *Government of Canada* | May 2020 | https://www.canada.ca/en/democratic-institutions/services/reports/report-assessment-critical-election-incident-public-protocol.html

73 **Impact of COVID-19** | *Elections Canada* | 5 January 2021 | https://www.elections.ca/content.aspx?section=med&dir=cor&document=index&lang=e

74 Olamide Olaniyan | **BC's Party Insiders on Campaigning in a Pandemic** | *The Tyee* | 3 November 2020 | https://thetyee.ca/News/2020/11/03/BC-Party-Insiders-Campaigning-Pandemic

David McGrane | **Campaigning in Canada during a pandemic** | *Policy Options* | 28 December 2020 | https://policyoptions.irpp.org/magazines/december-2020/campaigning-in-canada-during-a-pandemic

Laura Brown | **Pandemic forces New Brunswick politicians to think outside the box while campaigning** | *CTV News* | 25 August 2020 | https://atlantic.ctvnews.ca/pandemic-forces-new-brunswick-politicians-to-think-outside-the-box-while-campaigning-1.5079399

Andy Walker | **The race is on for P.E.I.'s first electoral test in COVID-19 era** | *Saltwire* | 13 October 2020 | https://www.saltwire.com/opinion/local-perspectives/andy-walker-the-race-is-on-for-peis-first-electoral-test-in-covid-19-era-508856

75 Olamide Olaniyan | **BC's Party Insiders on Campaigning in a Pandemic** | *The Tyee* | 3 November 2020 | https://thetyee.ca/News/2020/11/03/BC-Party-Insiders-Campaigning-Pandemic

David McGrane | **Campaigning in Canada during a pandemic** | *Policy Options* | 28 December 2020 | https://policyoptions.irpp.org/magazines/december-2020/campaigning-in-canada-during-a-pandemic

Laura Brown | **Pandemic forces New Brunswick politicians to think outside the box while campaigning** | *CTV News* | 25 August 2020 | https://atlantic.ctvnews.ca/pandemic-forces-new-brunswick-politicians-to-think-outside-the-box-while-campaigning-1.5079399

Andy Walker | **The race is on for P.E.I.'s first electoral test in COVID-19 era** | *Saltwire* | 13 October 2020 | https://www.saltwire.com/opinion/local-perspectives/andy-walker-the-race-is-on-for-peis-first-electoral-test-in-covid-19-era-508856

CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS