ISSN 2563-8165
CAT D95-10E-PDF

Cyber threats to CANADA'S democratic process | 2023 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

TABLE OF CONTENTS

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 may need CSE's unique technical capabilities.

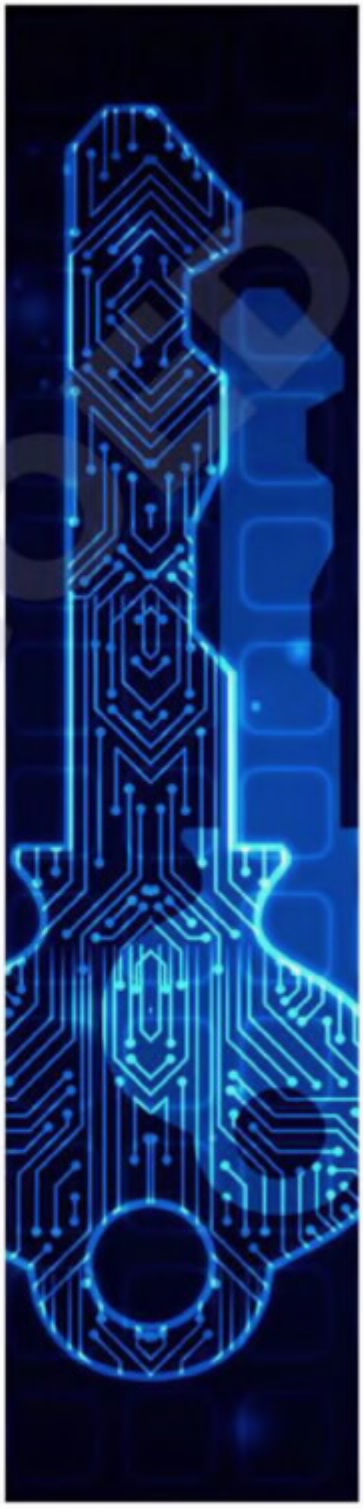
CSE protects computer networks and electronic information of importance to the Government of Canada, helping to thwart state-sponsored or criminal cyber threat activity on our systems. In addition, CSE's foreign signals intelligence work supports government decision-making in the fields of national security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

Part of CSE is the Canadian Centre for Cyber Security (Cyber Centre), Canada's technical authority on cyber security. The Cyber Centre is the single unified source of expert advice, guidance, services, and support on cyber security for Canadians and Canadian organizations.

CSE and the 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

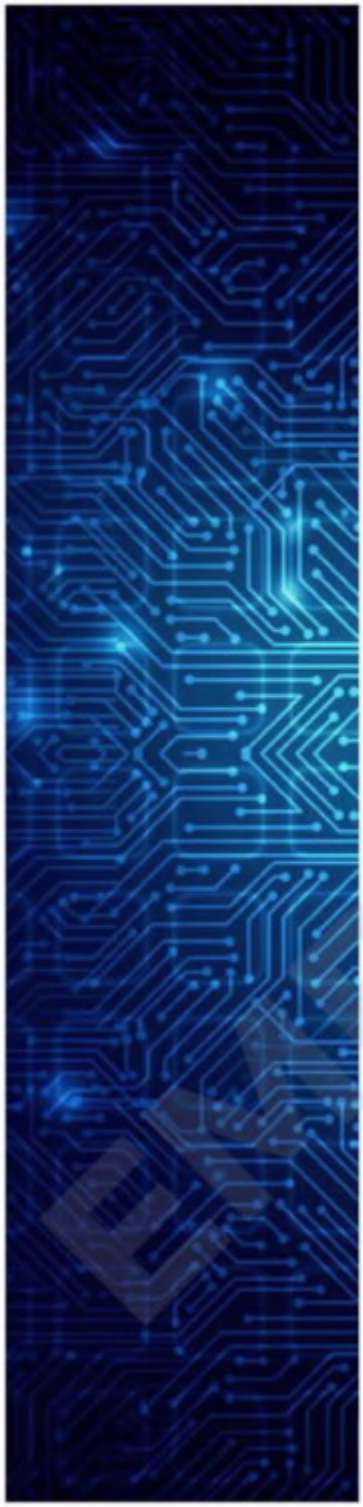
Foreign adversaries are increasingly using cyber tools to target democratic processes around the world. Disinformation has become ubiquitous in national elections, and adversaries are now using generative artificial intelligence (AI) to create and spread fake content. This report addresses cyber threat activity targeting elections, and the growing threat that generative AI poses to democratic processes globally and in Canada.



Key findings and global trends

- Cyber threat activity targeting elections has increased worldwide. The proportion of elections targeted by cyber threat activity relative to the total number of national elections globally has increased from 10% in 2015 to 26% in 2022. Since our publication of Cyber Threats to Canada's Democratic Process: July 2021 update,[1] we observed that the proportion of elections targeted increased from 23% in 2021 to 26% in 2022.[2]
- In 2022, we found that slightly over a quarter (26%) of all national elections globally had at least one reported cyber incident. Of the countries whose national elections were targeted by cyber threat activity from 2015 to 2022, approximately 25% are NATO countries and approximately 35% are OECD (Organisation for Economic Co-operation and Development) countries.
- We observe that state-sponsored cyber threat actors with links to Russia and China continue to conduct most of the attributed cyber threat activity targeting foreign elections since 2021. Russia and China's cyber threat activity includes attempts to conduct distributed denial of service (DDoS) attacks against election authority websites, accessing voter personal information or information relating to the election, and vulnerability scanning on online election systems.[3] We assess it very likely that Russia and China will continue to be responsible for most of the attributed cyber threat activity targeting foreign elections in the next two years and will focus on targeting countries of strategic significance to them.

Executive Summary



- State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by adversaries. During periods of heightened bilateral tensions, cyber threat actors can be called upon to conduct cyber activity or influence operations targeting events of national importance, including elections. We assess that increased tensions or antagonism between Canada and a hostile state is very likely to result in cyber threat actors aligned with that state targeting Canada's democratic processes or disrupting Canada's online information ecosystem ahead of a national election.
- The majority of cyber threat activity targeting elections is unattributed. Since the publication of the Cyber Threats to Canada's Democratic Process: July 2021 update,[4] more than half of the perpetrators of cyber threat activity targeting national elections were unknown. In 2022, 85% of cyber threat activity targeting elections was unattributed, meaning that these cyber incidents are not ascribed or credited to a state-sponsored cyber threat actor. When the perpetrators were known, only two countries were reported to actively target foreign elections in the last two and a half years: Russia and China. We assess it very likely that cyber threat actors are increasingly using obfuscation techniques and/or are outsourcing their cyber activities in order to hide their identities or links to foreign governments.
- From the publication of the Cyber Threats to Canada's Democratic Process: July 2021 update[5] until Spring of 2023, we found that all national elections globally (146 in total) were subject to online disinformation geared towards influencing voters and the election. We also detected an increase in the amount of synthetic content being produced relating to national level elections, almost certainly related to the increased accessibility of generative AI. However, we note that the number of reported cases where synthetic content is being used to spread disinformation about elections remains relatively low compared to the amount of synthetic content observed online. We assess that the use of generative AI for synthetic content related to national elections will almost certainly increase in the next two years, as this technology becomes more widely available.

ABOUT THIS REPORT

This report is the fourth iteration of Cyber Threats to Canada's Democratic Process and provides an update to the 2017, 2019 and 2021 reports released by CSE. Its purpose is to inform Canadians about the cyber threats to our democratic process in 2023.

Scope

This report considers cyber threat activity that affects democratic processes. Cyber threat activity involves the use of cyber tools and techniques (e.g. malware and spear phishing) to compromise the security of an information system by altering the confidentiality, integrity, and availability of a system or the information it contains. This assessment considers cyber threat activity and cyber-enabled influence campaigns, which occur when cyber threat actors use cyber threat activity or generative AI to covertly manipulate online information in order to influence opinions and behaviors.

Sources

In producing this report, 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, particularly in the context of Canada's next federal election, currently set for 2025. Providing threat mitigation advice is outside the scope of this report, however, we do refer to additional resources in the "More information" section and the "Looking ahead" sections of this document.

About this report

More information

Further resources can be found on the Cyber Centre's cyber security guidance page[6] and on the Get Cyber Safe[7] website.

For readers interested in more detailed information about cyber tools and the evolving cyber threat landscape, we refer you to the following:

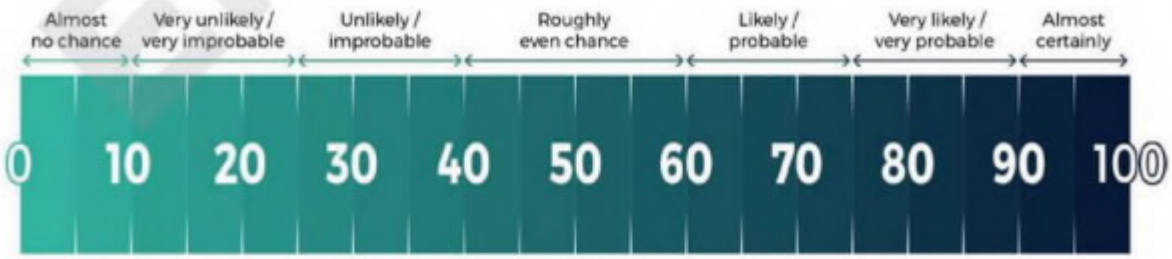
- National Cyber Threat Assessment 2023-2024[8]
- An Introduction to the Cyber Threat Environment[9]
- How to identify misinformation, disinformation, and malinformation[10]

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 according to the chart below.

The contents of this report are based on information available as of October 26, 2023.

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

This assessment is the fourth version of "Cyber Threats to Canada's Democratic Process" and is an update on the global cyber threat activity trends targeting national elections since the last publication in 2021. It also provides information on how cyber threat activity can target election infrastructure, how cyber-enabled influence campaigns impact Canada's information ecosystem, and how generative AI technologies will shape the future of democratic debate online.

Canada's democratic process: A target for cyber threat activity?

Cyber threat activity poses a real and growing threat to Canada's democratic processes. Cyber threat actors, including state-sponsored cyber threat actors, hacktivists, and cybercriminals, interfere with the democratic process and seek to impact Canada's ability to have fair and free elections. Canada's efforts to promote international trade and development, international peace and security, as well as international human rights, increase the likelihood that it will become a target for cyber threat actors looking to change election outcomes in order to influence policy or diplomatic relations. Canada's membership in key organizations, such as NATO (North Atlantic Treaty Organization) and the G7 (Group of Seven), its role in the Indo-Pacific region, as well as its support for Ukraine almost certainly make it a target for cyber threat activity and influence campaigns, including those directly targeting our democratic processes.

We have observed that voters are the most frequent targets of cyber threat activity affecting elections worldwide, and Canadian voters are among some of the most connected in the world, making them a larger potential target for cyber threat activity.[11] Because a large number of Canadians share information online, cyber threat actors looking to influence Canadian voters' opinions and behaviours can manipulate online information using cyber techniques to conduct influence operations (e.g., hack-and-leak) or use AI technologies to generate fake content (e.g., deepfakes). Increased tensions between Canada and other states could lead to state-sponsored cyber threat actors targeting Canada's election and disrupting Canada's democratic process. During periods of heightened bilateral tensions, cyber threat actors can be called upon to conduct cyber activity or influence operations targeting events of national importance, including elections. We assess that increased tensions or antagonism between Canada and a hostile state is very likely to result in cyber threat actors aligned with that state targeting Canada's democratic processes or disrupting Canada's online information ecosystem ahead of a national election.

Foreign adversaries are using cyber capabilities to threaten democratic processes

Foreign adversaries use cyber capabilities to influence political outcomes and threaten a country's democratic process by targeting voters, politicians, political parties, and election infrastructure. Cyber threat actors can directly compromise websites, social media accounts, networks, and devices used by election management bodies, or pollute the information ecosystem by spreading disinformation and by conducting influence campaigns ahead of elections.

Introduction

Examples of cyber activity that we have observed globally since 2021 include:

- distributed denial of service (DDoS) attacks against election authority websites and electronic voting systems
- unauthorized access to voter databases to collect private information
- spear phishing attacks against elections officials and politicians
- attempts to manipulate election results by compromising election worker voter database access
- use of bots and inauthentic social media accounts to influence political discourse

It is becoming increasingly difficult to determine which adversaries are responsible for cyber threat activity targeting democratic processes. Outsourcing cyber threat activity to third parties, such as hacktivists and cybercriminals, or purchasing cyber tools and services from commercial providers and online marketplaces can help foreign adversaries obfuscate their operations. Foreign adversaries have access to a wide range of cyber tools and services on illegal markets that supplement their in-house cyber capabilities. Influence-for-hire firms can also help hide the source of influence campaigns by providing tools and services that spread disinformation and manipulate political discourse.

For example, in February 2023, a team of journalists uncovered an Israeli "influence-for-hire" firm's hacking and disinformation operations which claimed to have helped clients, including foreign governments, target more than 30 elections across the globe.[12] In addition, foreign adversaries outsource their cyber activities to non-state cyber groups, such as cybercriminal groups and hacktivists, to avoid direct attribution and access enhanced cyber capabilities.

Cyber threat activity and AI technology: Cyber threat actor goals

Short-term goals	Mid-term goals	Long-term goals
Put into question the results of the election	Weaken confidence in leadership	Create distrust that the electoral process is democratic
Promote polarizing political discourse by manipulating social media algorithms with fake bot accounts	Online public discourse becomes "one-sided" and political polarization fuels discontent and social movements	Co-opt domestic social movements to promote foreign economic, military, or ideological interests
Reduce voter turnout	Weaken confidence in election infrastructure	Voters become disenfranchised and apathetic to elections
Generate misleading deepfake videos and other AI generated synthetic content	Increase skepticism of information online	Create disbelief in information online

GLOBAL TRENDS

The Cyber Centre has been analyzing cyber threat activity targeting national level elections globally since 2015. Not all cyber threat activity is reported – much of it is covert. Therefore, we assess that our data almost certainly underestimates the total number of events targeting democratic processes around the world. Based on our observations from 2015 to 2023, we identified four global trends.

Trend 1: Targeting of democratic processes has increased

The proportion of elections targeted by cyber threat activity relative to the total number of national elections globally has increased from 10% in 2015 to 26% in 2022. Since our last publication of the Cyber Threats to Canada's Democratic Process: July 2021 update,[13] we observe that the proportion of national elections targeted increased from 23% in 2021 to 26% in 2022.[14] The percentage of elections targeted in 2020 was noticeably lower than other years, and we assess that this is almost certainly an anomaly co-related with the COVID-19 pandemic. Additionally, we found that in 2022 over a quarter (26%) of all national elections had at least one cyber incident. These findings demonstrate a high level of cyber threat activity, however, some cyber threat activity targeting democratic processes remains unidentified or unreported, and we assess that it is very likely that these findings represent conservative estimates.

We found that the number one type of cyber incident affecting national elections was a denial of access or distortion of election commission websites, followed by internet shutdowns during elections. The total share of targeted elections that were in NATO countries increased from 2.8% in 2021 to 3.7% in 2022. (Figure 1a) The COVID-19 pandemic likely explains why fewer OECD countries elections were targeted in 2020 and 2021, as we observed an uptick in the share of targeted elections that were in OECD countries, from 4% in 2021 to 13% in 2022. (Figure 1b)

Figure 1: Percentage of national-level elections targeted by cyber activity by year

Figure 1a

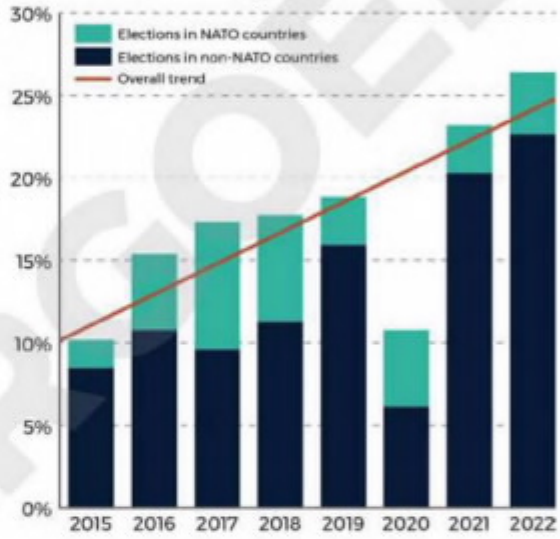
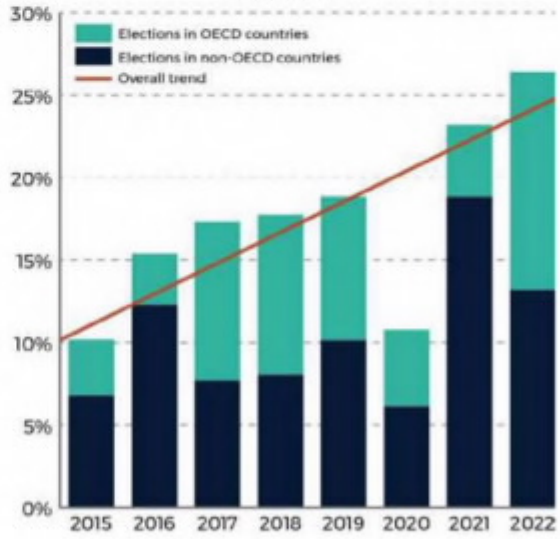


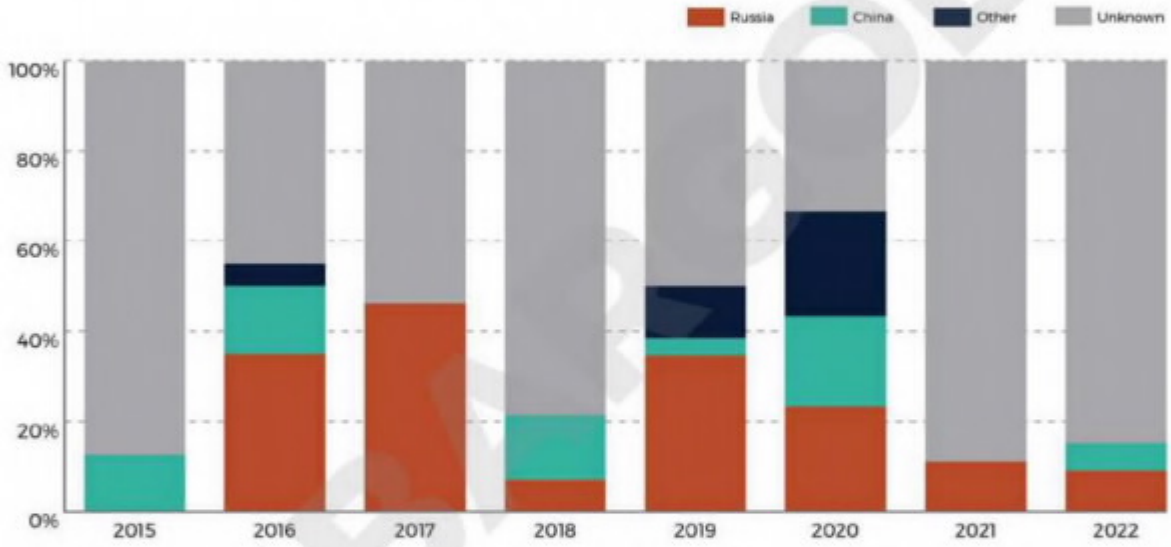
Figure 1b



Trend 2: Russia and China continue to conduct most of the attributed cyber threat activity targeting foreign elections

We observe that state-sponsored cyber threat actors with links to Russia and China continue to conduct most of the attributed cyber threat activity targeting foreign elections since 2021. Russia has consistently been responsible for observed cyber threat activity interfering with foreign elections since 2016, and China has been active every year since 2015, with the exception of 2017 and 2021 (Figure 2). Russia and China's cyber threat activity includes attempted DDoS attacks against election authority websites, accessing voter personal information or information relating to the election, and vulnerability scanning on online election systems.

Figure 2: Proportion of cyber incidents attributed to countries targeting foreign national-level elections by year



We assess that attributed cyber threat activity is almost certainly focused on influencing elections to fulfill strategic objectives in geopolitical regions of interest to Russia and China. In some cases, cyber activity is politically motivated and will target a country's democratic processes as a form of retribution. For example, pro-Russia state-affiliated cyber actors have targeted elections of countries who have provided assistance to Ukraine. We assess it very likely that Russia and China will continue to be responsible for most of the attributed cyber threat activity targeting foreign elections and will focus on targeting countries of strategic significance to them. We note that upcoming European elections in 2023 and 2024 could be a significant target for Russia due to the military and economic importance of Europe's support to Ukraine.

Trend 3: The majority of cyber threat activity targeting elections is unattributed

Since the publication of the Cyber Threats to Canada's Democratic Process: July 2021 update,[15] more than half of the perpetrators of cyber threat activity targeting national elections were unknown. In 2022, 85% of cyber threat activity targeting elections was unattributed, meaning that these cyber incidents are not ascribed or credited to a state-sponsored cyber threat actor. We assess it very likely that cyber threat actors are increasingly using obfuscation techniques and/or are outsourcing their cyber activities in order to hide their identities or links to foreign governments.

By outsourcing malicious cyber threat activities, foreign adversaries can avoid public attribution and diplomatic consequences. Foreign adversaries have been increasing their use of non-state cyber threat groups to avoid cyber activities being linked back to their government. Non-state cyber threat groups have less government oversight, do not abide by the same conventions and norms, and can organize cyber activities, such as distributed denial-of-service (DDoS) attacks, quickly and with little warning. Foreign adversaries are also using influence-for-hire firms to conduct influence operations under the radar. Since 2011, at least 27 online information operations have been partially or wholly attributed to commercial public relations or marketing firms.[16] Services related to election interference represent a growing market, and if the use of third-party proxies continues, we assess that in the next two years, governments will likely have difficulties linking cyber threat activities targeting elections back to the foreign adversaries responsible.[17]

Trend 4: Generative AI is increasingly being used to influence elections

Cyber threat actors are using generative AI technologies to shape the future of democratic debate online. In August 2019, researchers found that there has been an increase in dark web source activities, as well as an increase in advertising for customized deepfake service offerings.[18] Since the publication of the Cyber Threats to Canada's Democratic Process: July 2021 update,[19] we have detected an increase in the amount of synthetic content (e.g. deepfakes) relating to elections, almost certainly due to the increased accessibility of many of these technologies. However, we note that the number of reported cases where synthetic content is being used to spread disinformation about elections remains relatively low compared to the amount of synthetic content observed online. We assess that AI synthetic content generation related to national elections will almost certainly increase in the next two years, as this technology becomes more widely available. As synthetic content generation increases and becomes more widespread, it will almost certainly become more difficult to detect, making it harder for Canadians to trust online information about politicians or elections.

CYBER THREAT ACTIVITY AGAINST ELECTION INFRASTRUCTURE

Elections around the world are increasingly relying on digital technologies, meaning that the threat of cyber attacks against election infrastructure is growing. Cyber threat actors target election infrastructure to directly impact the elections process. Examples include conducting a DDoS attack shutting down an election commission website, gaining unauthorized access to a voter database via phishing email, or attacking election infrastructure such as voting machines.

Figure 3: Election infrastructure

Unlike influence campaigns which aim to influence voter behaviour, cyber threat actors targeting election infrastructure seek to attack the electoral process directly, modify results, or reduce access to voting. There are three stages in which cyber threat actors can target election infrastructure: when voters register, when they vote, and when the votes are tallied. Cyber threat activity compromising any of these three stages of the electoral process can jeopardize the integrity of an election.

Voter registration

In almost all countries voters must register. In Canada, voters can register for national elections either at the polls or online.[20] Online registration can speed up the election process and voter registries can be kept secure through safety measures such as controlling registry access, physically protecting associated hardware, and providing additional I.T. security measures. However, voting registries contain valuable data which can be a target for malicious cyber threat actors. For example, cyber threat actors can attempt to alter online voter records, erase or encrypt data, make the website inaccessible for registration, or display misleading information about registration. Cyber threat actors can also attempt to by-pass security measures to access voter databases and use this personal information to target voters. For instance, on October 22, 2020, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) publicly denounced an Iranian campaign to obtain US voter information and send threatening email messages to intimidate voters and disseminate disinformation pertaining to the election.[21]

Casting the ballot

Once a voter's identity is confirmed they can cast their vote either by using a paper ballot or by selecting an option on a screen. In Canada, only paper ballots are used in federal elections. Other countries, such as the United States, France, and Brazil, use direct-recording electronic (DRE) machines, commonly referred to as "voting machines," in their elections.[22] DRE machines are susceptible to tampering by malicious cyber threat actors, and cyber security experts have in the past demonstrated several vulnerabilities within these systems.[23] Since 2023, 11 countries have abandoned e-voting citing concerns about trust and security of the vote.[24] Some DRE machines do not record voters' choices onto paper, which can lead to complications in recounting votes.[25]

Vote tally and the paper trail

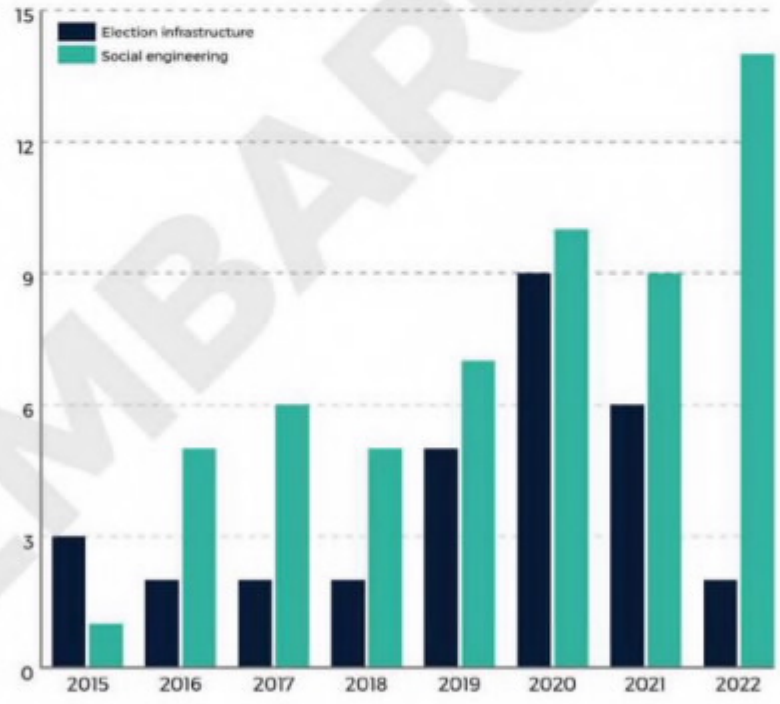
Most countries use some form of technology to process and tally the votes. One of the most common technologies to tally votes are optical scan machines. While some of Canada's municipal and provincial elections use optical scan machines, all federal election results are counted by hand.[26] These machines scan paper ballots to register the voters' marks, and to store the results electronically. This system allows for a quicker tallying of the votes but also ensures that the paper ballots can be compared to the scanner's tabulation. Like other types of computer-based technology, optical scan machines are susceptible to compromises and physical access to these machines must be protected in order to ensure the software's integrity.[27] Relying on an online system to collect and tabulate votes, without having a paper audit trail as a backup, can make it difficult to detect errors or compromises made to voting machines software or hardware.

CYBER THREAT ACTIVITY AND ELECTION INFLUENCE CAMPAIGNS

Cyber threat activity can generate disinformation that influences voters ahead of elections. This disinformation can be part of a wider election influence campaign, where cyber threat actors use social engineering tactics and techniques to manipulate voters' emotions and behaviours.[28] Gaining unauthorized access to privileged information can influence public discourse online and potentially affect voters' opinions and voting preferences. This type of cyber threat activity can include a hack-and-leak of sensitive information from a political party's database, hacking into a politician's social media account to post disinformation, or defacing a political party's website with disinformation. Rather than targeting election infrastructure directly, cyber threat actors will use cyber capabilities to try to influence or manipulate the electorate.

Cyber activity against democratic processes worldwide is more often conducted to influence the electorate prior to elections rather than to target election infrastructure (Figure 4). Based on these findings, we assess that on average, cyber threat actors targeting elections favour manipulating the information environment over attempts to directly impact the voting process.

Figure 4: Number of observed incidents targeting national-level elections via election infrastructure vs. social engineering by year



There are several reasons why cyber threat actors conduct social engineering rather than target election infrastructure. These include:

- having a broader set of targets to choose from
- needing fewer bespoke techniques, tactics, and procedures (TTPs) to gain access to privileged information
- targeting sources of information that do not have the protection of an IT team (e.g. obtaining information from a political staffer's personal email account)
- justifying hack-and-leaks as being altruistic and providing the public with important information that they "should know about"
- being able to outsource influence activities to a marketing or PR firm
- having more plausible deniability; targeting the electorate is less direct, and harder to trace

Foreign adversaries conducting influence campaigns

Foreign adversaries will use cyber threat activity to influence elections by creating, circulating, and/or amplifying disinformation in online public spaces. They do this to manipulate a country's population covertly in the hopes that the outcome of the election will align with their strategic objectives abroad. Foreign adversaries may also consider targeting another country's electorate as being less escalatory than targeting the country's election infrastructure. Nevertheless, foreign adversaries will attempt to obfuscate their involvement in influence campaigns and the cyber activities that feed into these influence campaigns. Geo-spoofing and encrypted messaging platforms make it extremely difficult to identify disinformation's origin.[29] In some cases, they will hire a third party to conduct influence campaigns to target elections. These third parties are commonly referred to as "influence-for-hire" firms and are part of a thriving industry that has grown since 2019. Researchers at the Oxford Internet Institute found 48 instances of states working with influence-for-hire firms from 2019 to 2020, a 128% increase since the 2017 to 2018 period.[30] Foreign adversaries will also use social botnets to amplify certain narratives online and push content onto voters with the same political views, worsening the effect of political echo chambers and increasing political polarization ahead of elections.[31] We assess almost certainly that influence campaigns propagated by state-sponsored cyber threat actors represent an ongoing, persistent threat to Canadians.

Online news environment

The *Online News Act* requires tech companies to compensate Canadian media organizations for the news content that appears on their online platforms.

Some tech companies have refused to comply and will block Canadian news from their platforms. In 2019, almost 50% of Canadians aged between 18 and 24 relied on social media as their main source of news.[32]

We assess that in the absence of Canadian news sources, younger Canadians are very likely at a higher risk of being exposed to misleading news content, which may be part of wider disinformation and influence campaigns.

GENERATIVE AI THREATENS DEMOCRATIC PROCESSES

Generative artificial intelligence (AI) can produce various types of content, including text, images, audio, and video, sometimes referred to as "deepfakes." This synthetic content can be used in influence campaigns to covertly manipulate information online, and as a result, influence voter opinions and behaviours. Despite the potential creative benefits of generative AI, its ability to pollute the information ecosystem with disinformation threatens democratic processes worldwide.

In recent years, generative AI has become increasingly popular as its ability to generate synthetic content (text, images, or videos) has become accessible through large tech companies like OpenAI, Meta, and Google. Unfortunately, cyber threat actors are also using these capabilities to generate or amplify disinformation online. Between August 2019 and January 2021, third-party monitoring recorded an uptick in dark web source activities on deepfake-related topics as well as an increase in advertising for customized deepfake service offerings.[34] We assess it very likely that cyber threat actors will increasingly use generative AI in influence campaigns targeting elections.

Machine Learning

Generative AI is an application of machine learning. Machine learning is when computers learn how to complete a task from given data without explicitly programing a step-by-step solution. Machine learning programs have progressed to the point where the content they produce is often nearly impossible to tell apart from human-made content.[33]

Figure 5: Types of synthetic content created by Generative AI

In most cases, it is unclear who is behind AI-generated disinformation. However, we assess it very likely that foreign adversaries or hacktivists will use generative AI to influence voters ahead of Canada's next federal election. We have observed that cyber threat actors are already using this technology to pursue strategic political objectives abroad. For example, pro-Russia cyber threat actors have used generative AI to create a deepfake of Ukrainian President Zelenskyy surrendering following Russia's invasion of Ukraine.[35] We assess that foreign adversaries and hacktivists are likely to weaponize generative AI within the next two years to create deepfake videos and images depicting politicians and government officials and to further amplify and automate inauthentic social botnets using text and image generators.

Deepfake videos influencing elections

The term "deepfake video" – combining "deep learning" and "fake" – refers to machine learning models that use image and audio synthesis techniques to generate fake videos that can appear realistic and genuine to viewers. Generative AI is used to reverse engineer real audio or video of a person to convincingly mimic their image and style of speech, producing a video of events that never actually occurred.[36] Deepfake videos of political figures risk deceiving voters and creating further political polarization. For example, in February of 2023, a deepfake was circulated on social media depicting Joe Biden making anti-transgender comments, despite his administration's public support for the LGBTQ community.[37] This example is only one among thousands of deepfakes of politicians circulating on social media, making it harder for voters to distinguish between real and fake political messaging.[38] The public's own understanding of the prevalence of deepfake videos online can also bring into question legitimate sources of information. For example, political debates can be a source of crucial information for voters in the lead up to the election since they present political party platforms and have been shown to change swing voters' candidate preferences.[39] However, if cyber threat actors circulate deepfakes altering debate content, voters may be deceived. Even if the truth is made clear later on, the damage may lead voters to question the legitimacy of political debates in the future. While most social media platforms, such as Instagram, Facebook, and YouTube, are making efforts to flag and remove deepfakes from their platforms, they are not always able to detect and remove deepfake content quickly before it can be widely circulated.

Social media companies' ability to detect and remove deepfakes is further complicated by considerations about creativity and freedom of speech. Political parties are themselves using generative AI capabilities as part of their campaigns, for example, to create videos depicting "future scenarios" if a political rival is elected.[40] While disclaimers are used to identify the video as a deepfake, very little regulation currently exists in Canada and the US on the extent to which generative AI can be used in political advertising.[41]

Social botnets augmented by AI capabilities

Cyber threat actors use fake social media profiles to disseminate or amplify disinformation ahead of elections.[42] A cluster of fake profiles operated by software robots, or "social botnets", can "control online social network accounts and mimic the actions of real users".[43] Social botnets can influence and/or misrepresent popular opinion and researchers have found that bots accounted for as much as 10% of accounts participating in conversations on certain topics, such as crisis events.[44] Social botnets have also been known to amplify domestic narratives or disinformation to contribute to a country's political polarization. As such, they are often part of larger influence campaigns and several "influence-for-hire" firms list this as one of their offered services.[45]

We assess that generative AI will almost certainly be increasingly used to further automate and augment social botnet functions in the next two years. AI text generators, like ChatGPT and Bard, are capable of generating paragraphs of coherent text that are virtually impossible to tell apart from human writing.[46] These generative AI capabilities can be applied to social botnets to improve their posts and make them sound more believably human.[47] Moreover, AI image generators, like GAN Lab, Midjourney or DALL-E, can fabricate fake images that are in some cases almost impossible to tell apart from real ones.[48] These capabilities can be used to generate fake profile pictures for botnet social media accounts, or to generate misleading content for posts. For example, in March 2023 a pro-Chinese government influence campaign used several AI-generated images to support narratives negatively portraying US leaders.[49] Differentiating between what is real and what is AI-generated will become more difficult for voters as social botnets continue to evolve and as generative AI capabilities become increasingly available.

We assess it very likely that the capacity to generate deepfakes exceeds our ability to detect them. Current publicly available detection models struggle to reliably distinguish between deepfakes and real content. Given the ineffectiveness of deepfake detection models, and the increasing availability of generative AI, it is likely that influence campaigns using generative AI that target voters will increasingly go undetected by the general public. We also assess that it is very likely that as technology develops, it will become better at fooling detection models, which will make it more difficult for social media companies to detect and automatically remove synthetic content before it reaches voters.

IMPLICATIONS FOR CANADA

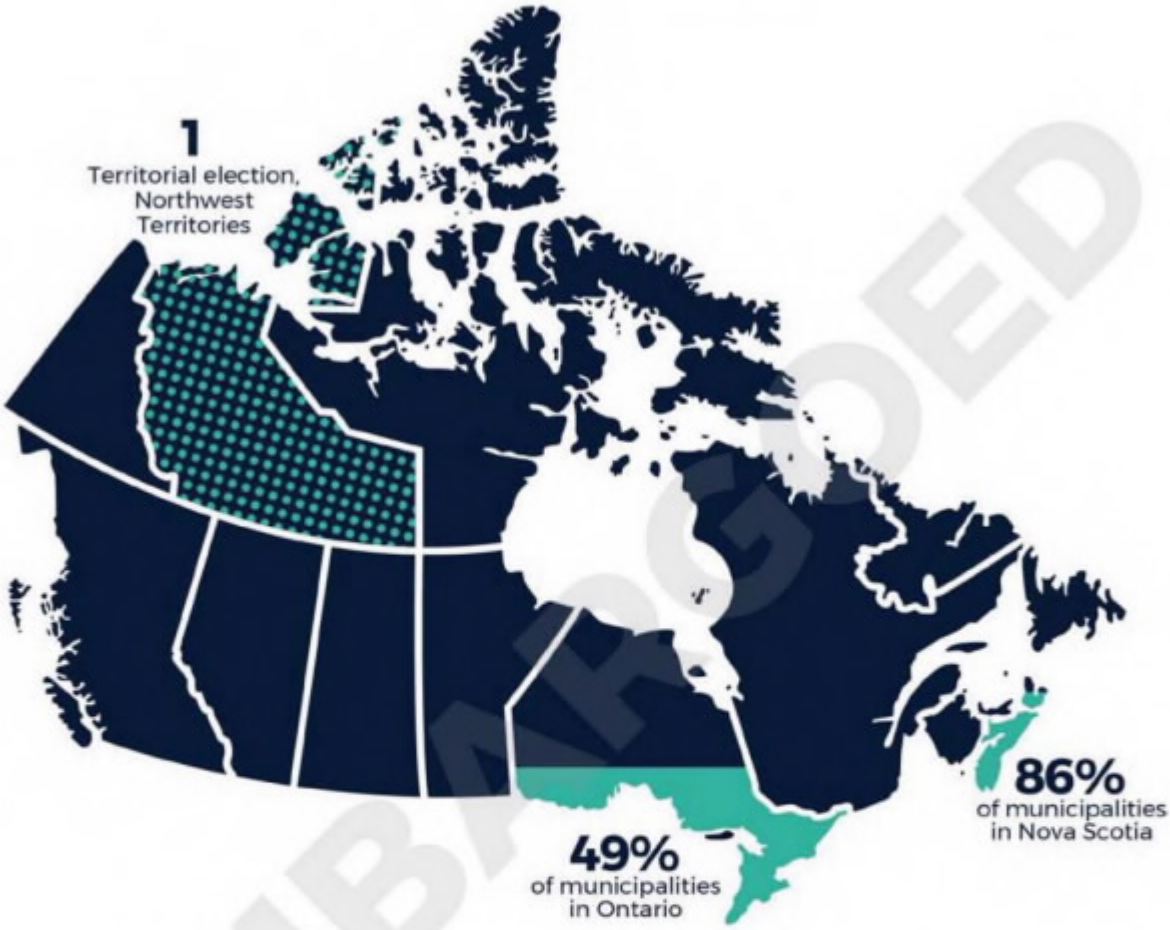
Based on our findings, we assess that disinformation about the next federal election will almost certainly be found online and that foreign adversaries will likely use generative AI to target Canada's federal election in the next two years. We assess that, overall, Canada is a lower priority target for cyber threat activity than some of its allies, such as the US and UK. However, Canada does not exist in a vacuum and cyber activity affecting our allies' democratic processes will likely have an impact on Canada as well. For example, a high percentage of Canadians use US social media platforms and are often exposed to the same deepfakes and foreign influence campaigns targeting US citizens.[50]

We also note that the four global trends we identified have implications for Canada. The percentage of elections targeted by cyber threat activity has increased globally and, based on this trend, we assess cyber incidents are also more likely to happen in Canada's next federal election than they have been in the past. As stated in the National Cyber Threat Assessment 2023-2024,[51] cyber threat activity has become an important tool for states to influence events without reaching the threshold of conflict. We judge that cyber threat activity targeting democratic processes are likely viewed by foreign adversaries such as China and Russia as an obscure and risk-averse way of impacting Canada's policy outcomes. We also note that identifying the perpetrators of cyber threat activity targeting elections is becoming increasingly difficult as obfuscation techniques and third-party contracting become widespread. We judge it likely that this will also mean that it will become increasingly difficult for Canada to attribute cyber threat activity targeting its democratic processes.

In Canada, technology is used throughout the national election process and can be an important part of making elections efficient and accurate, however, not having physical paper ballots presents some risks. Relying on digital forensic teams to assess election interference presents challenges including flagging non-fraudulent voting abnormalities as fraud and not being able to distinguish cyber compromises from system malfunctions. Currently, Canada's national elections are paper based, however, some provincial, territorial, Indigenous and municipal governments are deliberating the benefits and drawbacks of online voting.[52] The Northwest Territories conducted its 2019 territorial elections using online voting and a large percentage of municipalities in Ontario and Nova Scotia are adopting online voting practices. As of September 15, 2023, we found that 217 of Ontario's 444 municipalities (49%) and 42 of Nova Scotia's 49 municipalities (86%) used online voting in at least one of their past elections. (Figure 6)

Implications for Canada

Figure 6: Map of electronic voting in Canada



Potential election interference and suspected election result tampering can put into question the legitimacy of an election and result in investigations into the election process. Disproving false narratives relating to election interference can be difficult: the technical components of cyber threat activity are not always easily understood by voters and the extent of cyber compromises can be misunderstood or misinterpreted.

LOOKING AHEAD

Cyber threat activity continues to be used to target democratic processes globally, and the Government of Canada, CSE, and the Cyber Centre produce advice and guidance to help inform Canadians about the cyber threats to Canada's elections.

The Cyber Centre provides cyber security advice and guidance to all major political parties, in part through publications such as the Cyber Security Guide for Campaign Teams[53] and Cyber Security Advice for Political Candidates.[54]

The Cyber Centre has also published the following:

- Cyber Security Guidance for Elections Authorities[55]
- Cyber Security Guidance on Generative Artificial Intelligence (AI)[56]
- Guide on Security Considerations When Using Social Media in Your Organization[57]

The Cyber Centre also works closely with Elections Canada to protect its infrastructure, including publishing a report on Security Considerations for Electronic Poll Book Systems.[58]

We encourage Canadians to consult the Cyber Centre's resources including the National Cyber Threat Assessment 2023-2024,[59] and the How to Identify Misinformation, Disinformation, and Malinformation[60] publication, as well as the Fact Sheet for Canadian Voters.[61] CSE's Get Cyber Safe[62] 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

ENDNOTES

1 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

2 These numbers exclude instances of Online Foreign Influence Activity (OFIA) and focus solely on cyber threat activity.

3 Cyber threat actors can conduct Network Denial of Service (DoS) attacks to restrict or block users' ability to access a targeted resource, such as a website. "A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS)." See MITRE ATT&CK. "Network Denial of Service." October 2023. https://attack.mitre.org/techniques/T1498/

4 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

5 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

6 https://www.cyber.gc.ca/en/guidance

7 https://www.getcybersafe.gc.ca/en/home

8 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

9 https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

10 https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300

11 The vast majority of Canadians use social media platforms to get and share information related to politicians, political parties, and elections. In 2022, approximately 74% of Canadians over 15 years old used social media and approximately 77% accessed online news. In 2019, almost 50% of Canadians between the ages of 18 and 24 relied on social media as their main source of news, and today the number is likely even higher.

12 Stephanie Kirchgaessner, Manisha Ganguly, David Pegg, Carole Cadwalladr and Jason Burke "Revealed: the hacking and disinformation team meddling in elections." The Guardian. February 15, 2023. https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan

13 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

14 These numbers exclude instance of Online Foreign Influence Activity (OFIA) and focuses solely on cyber threat activity.

15 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

16 Craig Silverman, Jane Lytvynenko and William Kung. "Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online." Buzz Feed News. January 6, 2020. https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms

17 Jacob Wallis, Ariel Bogle, Albert Zhang, Hillary Mansour, Tim Niven, Elena Yi-Ching Ho, Jason Liu, Jonathan Corpus Ong and Ross Tapsell. "Influence for hire: The Asia-Pacific's online shadow economy." Australian Strategic Policy Institute - International Cyber Policy Centre. August 2021. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-08/Influence for hire_0.pdf

18 Recorded Future. "The Business of Fraud: Deepfakes, Fraud's Next Frontier." April 29, 2021; Shamani Joshi. "They Follow You on Instagram, Then Use Your Face to Make Deepfake Porn in This Sex Extortion Scam." Vice News. September 7, 2021. https://www.recordedfuture.com/deepfakes-frauds-next-frontier https://www.vice.com/en/article/z3x9yj/india-instagram-sextortion-phishing-deepfake-porn-scam

19 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update

20 United Nations, "Women and Elections: Basic elements of voter registration." March 2005; Elections Canada. "The Electoral System of Canada." October 17, 2022. https://www.un.org/womenwatch/osagi/wps/publication/Chapter4.htm https://www.elections.ca/content.aspx?section=res&dir=ces&document=part5&lang=e

21 Federal Bureau of Investigations Most Wanted. "Iranian Interference in 2020 US Elections." October 20, 2021. https://www.fbi.gov/wanted/cyber/iranian-interference-in-2020-us-elections

22 International Institute for Democracy and Electoral Assistance. "Use of E-Voting Around the World." February 6, 2023. https://www.idea.int/news-media/media/use-e-voting-around-world

Endnotes

23 Sue Halpern. "Election-Hacking Lessons from the 2018 Def Con Hackers Conference." The New Yorker. August 23, 2018; Shaun Nichols. "Expert gives Congress solution to vote machine cyber-security fears: Keep a paper backup." The Register. December 1, 2017; Shaun Nichols. "US voting hardware maker's shock discovery: Security improves when you actually work with the community." The Register. August 6, 2020; Cyberscoop. "DEF CON Voting Village takes on election conspiracies, disinformation." August 17, 2022.
https://www.newyorker.com/news/dispatch/election-hacking-lessons-from-the-2018-def-con-hackers-conference
https://www.theregister.com/2017/12/01/us_voting_machine_security_hearing/
https://www.theregister.com/2020/08/06/black_hat_ess_bugs/
https://cyberscoop.com/defcon-voting-village-harri-hursti-election-fraud/

24 International Institute for Democracy and Electoral Assistance. "Use of E-Voting Around the World, International Institute for Democracy and Electoral Assistance." February 6, 2023.
https://www.idea.int/news-media/media/use-e-voting-around-world

25 Some DRE machines are able to create paper trail called a voter-verified paper audit trail (VVPAT) by recording the vote on paper, however, many voting machines do not. See Raj Karan Gambhir and Jack Karsten. "Why paper is considered state-of-the-art voting technology." The Brookings Institution. August 14, 2019.
https://www.brookings.edu/articles/why-paper-is-considered-state-of-the-art-voting-technology/

26 International Institute for Democracy and Electoral Assistance. "ICTs in Elections Database." April 29, 2019; Paul Laronde. "Technologies in the Voting process: An Overview of Emerging Trends and Initiatives (Research Note)." Elections Canada. May 2012; Elections Canada. "Safeguards for Counting Votes and Reporting on Results." May 13, 2023.
https://www.idea.int/news-media/media/use-e-voting-around-world
https://www.idea.int/news-media/media/use-e-voting-around-world
https://www.elections.ca/content.aspx?section=vot&dir=int/cou&document=index&lang=e

27 In September 2007, Secretary of State Debra Bowen conducted a review of many of the voting systems certified for use in California. See California Secretary of State. "Top-to-Bottom Review." July 20, 2007.
https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review

28 IBM. "What is social engineering?" November 20, 2020.
https://www.ibm.com/topics/social-engineering

29 Geo-spoofing is the process of changing or hiding the location of a device on the internet by making the device look like it is somewhere else. See Justin Schamotta. "How to change your location online using geo-spoofing." Bleeping Computers. June 20, 2023.
https://www.bleepingcomputer.com/vpn/guides/location-geo-spoofing/

30 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard. "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." Oxford Internet Institute. January 13, 2022.
https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf

31 Emilio Ferrara, Herbert Chang, Emily Chen, Goran Muric, and Jaimin Patel. "Characterizing social media manipulation in the 2020 U.S. presidential election." First Monday. November 2020.
https://doi.org/10.5210/fm.v25i11.11431

32 Sebastien Charlton and Kamille Leclair. "Digital News Report: Canada 2019 Data Overview." Centre d'études des médias - Université Laval. February 2019.
https://www.cem.ulaval.ca/wp-content/uploads/2019/06/dnr19_can_eng.pdf

33 Thanh Thi Nguyena, Quoc Viet Hung Nguyenb, Dung Tien Nguyena, Duc Thanh Nguyena, Thien Huynh-Thec, Saeid Nahavandid, Thanh Tam Nguyene, Quoc-Viet Phamf, and Cuong M. Nguyen. "Deep Learning for Deepfakes Creation and Detection: A Survey." April 26, 2021; Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville and Yoshua Bengio. "Generative Adversarial Nets." Université de Montréal. June 10, 2014.
https://arxiv.org/pdf/1909.11573.pdf
https://arxiv.org/pdf/1406.2661.pdf

34 Recorded Future. "The Business of Fraud: Deepfakes, Fraud's Next Frontier." April 29, 2021; Shamani Joshi, "They Follow You on Instagram, Then Use Your Face to Make Deepfake Porn in This Sex Extortion Scam." Vice News. September 7, 2021.
https://www.recordedfuture.com/deepfakes-frauds-next-frontier
https://www.vice.com/en/article/z3x9yj/india-instagram-sextortion-phishing-deepfake-porn-scam

35 Bobby Allyn. "Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn." NPR. March 16, 2022.
https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

Endnotes

36 Adrian Tijie Xu. "AI, Truth, and Society: Deepfakes at the front of the Technological Cold War." Medium. July 2, 2019; Christian Vaccari and Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception." SAGE Journals. February 2020.
https://medium.com/gradientcrescent/ai-truth-and-society-deepfakes-at-the-front-of-the-technological-cold-war-86c3b5103ce6
https://journals.sagepub.com/doi/full/10.1177/2056305120903408

37 Reuters. "Fact Check-Video does not show Joe Biden making transphobic remarks." February 10, 2023.
https://www.reuters.com/article/factcheck-biden-transphobic-remarks-idUSL1N34Q1IW

38 Alexandra Ulmer and Anna Tong. "Deepfaking it: America's 2024 election collides with AI boom." Reuters. March 30, 2023
https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30/

39 John G Geer. "The effects of Presidential debates on the electorate's preferences for candidates." American Politics Quarterly. October 1988.
https://journals.sagepub.com/doi/10.1177/004478088016004005

40 Ali Swenson. "FEC moves toward potentially regulating AI deepfakes in campaign ads." PBS. August 10, 2023.
https://www.pbs.org/newshour/politics/fec-moves-toward-potentially-regulating-ai-deepfakes-in-campaign-ads

41 Fredreka Schouten. "Federal regulators inch a bit closer to regulating AI in political ads." CNN. August 10, 2023; Paola Ramirez and Pablo Tseng. "What Has the Law Done About "Deepfake"?" May 10, 2023.
https://www.cnn.com/2023/08/10/politics/fec-deepfakes-political-ads-regulation/index.html
https://mcmillan.ca/insights/what-has-the-law-done-about-deepfake/

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

43 Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. "Design and analysis of a social botnet." Computer Networks. June 27, 2012.
https://doi.org/10.1016/j.comnet.2012.06.006

44 Shashank Yadav. "Political Propagation of Social Botnets: Policy Consequences." Cornell University, May 10, 2022; Conrad Nied, Leo Stewart, Emma Spiro, and Kate Starbird. "Alternative Narratives of Crisis Events: Communities and Social Botnets Engaged on Social Media." Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. February 2017.
https://arxiv.org/ftp/arxiv/papers/2205/2205.04830.pdf
https://dl.acm.org/doi/10.1145/3022198.3026307

45 Lena Frischlich, Niels Göran Mede, and Thorsten Quandt. "The Markets of Manipulation: The Trading of Social Bots on Clearnet and Darknet Markets." Disinformation in Open Online Media. January 29, 2020.
https://link.springer.com/chapter/10.1007/978-3-030-39627-5_8

46 OpenAI. "Better Language Models and Their Implications." February 14, 2019.
https://openai.com/research/better-language-models

47 Alex Newhouse, Jason Blazakis and Kris McGuffie. "The industrialization of Terrorist Propaganda; Neural Language Models and the Threat of Fake Content Generation." Middlebury Institute of International Studies Center on Terrorism, Extremism and Counterterrorism." October 2019.
https://www.middlebury.edu/institute/sites/www.middlebury.edu.institute/files/2019-11/The Industrialization of Terrorist Propaganda - CTEC.pdf

48 Ian, J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville and Yoshua Bengio. "Generative Adversarial Nets." Université de Montréal. June 10, 2014.
https://arxiv.org/pdf/1406.2661.pdf

49 Michelle Cantos, Sam Riddell and Alice Revelli. "Threat Actors are Interested in Generative AI, but Use Remains Limited." Mandiant. August 17, 2023.
https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited

Endnotes

50 Most Canadians have viewed some form of synthetic content on social media due to 1) the large amounts of synthetic content circulating on social media and 2) Canadians' high intake of social media content. Researchers at the Queensland University of Technology found that, on average, over 3.2. billion photos and 720,000 hours of video are created daily and available online. They note that plenty of this online content consists of synthetic media shared on social media. In 2018, 78% of Canadians used at least one social networking account and as of January 2021, the estimated number of Canadian users on social media platforms Facebook, Instagram, Twitter, TikTok, WeChat, and Youtube totalled 67.1 million. See Sebastien Charlton and Kamille Leclair, "Digital News Report: Canada, 2019 Data Overview." Université Laval. June 11, 2019; Christoph Schimmele, Jonathan Fonberg and Grant Schellenberg, "Canadians' assessments of social media in their lives." Statistics Canada. March 24, 2021; T.J. Thompson, Daniel Angus, Paula Dootson, Edward Hurcombe and Adam Smith. "Visual Mis/disinformation in Journalism and Public Communications: Current Verification Practices, Challenges, and Future Opportunities." Journalism Practice. October 2020.
https://www.cem.ulaval.ca/wp-content/uploads/2019/06/dnr19_can_eng.pdf
https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm
https://www.researchgate.net/publication/344778089_Visual_Misdisinformation_in_Journalism_and_Public_Communications_Current_Verification_Practices_Challenges_and_Future_Opportunities

51 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

52 Chelsea Gabel and Nicole Goodman. "Indigenous Experiences with Online Voting." First Nation Digital Democracy. May 2021; Nicole Goodman, Jon H. Pammett and Joan DeBardeleben. "A Comparative Assessment of Electronic Voting." Elections Canada. February 2010; Paul Laronde. "Technologies in the Voting process: An Overview of Emerging Trends and Initiatives (Research Note)." Elections Canada. May 2012;
http://www.digitalimpactfn.com/wp-content/uploads/2021/05/FN_DIGITAL_REPORT_DIGITAL_FNL6.pdf
https://www.elections.ca/res/rec/tech/ivote/comp/ivote_e.pdf
https://www.elections.ca/content.aspx?section=res&dir=rec/tech/note&document=index&lang=e

53 https://cyber.gc.ca/en/guidance/cyber-security-guide-campaign-teams

54 https://www.cyber.gc.ca/en/guidance/cyber-security-advice-political-candidates

55 https://www.cyber.gc.ca/en/guidance/cyber-security-guidance-elections-authorities-itsm10020

56 https://www.cyber.gc.ca/en/guidance/generative-artificial-intelligence-ai-itsap00041

57 https://www.cyber.gc.ca/en/guidance/security-considerations-when-using-social-media-your-organization-itsm10066

58 https://www.cyber.gc.ca/en/guidance/security-considerations-electronic-poll-book-systems-itsm10101

59 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

60 https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300

61 https://www.cyber.gc.ca/en/guidance/fact-sheet-canadian-voters-online-influence-activities

62 https://getcybersafe.gc.ca/