ISSN 2563-8165
CAT D95-10E-PDF

Cyber Threats to CANADA'S Democratic Process | 2025 Update

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Canada

Communications Security Establishment Canada
1929 Ogilvie Road,
Ottawa (Ontario) K1J 8K6
cse-cst.gc.ca

ISSN 2563-8165
CAT D95-10E-PDF

TABLE OF CONTENTS

ABOUT US

The Communications Security Establishment Canada (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 our 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, 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 threats, helping to ensure our nation's security, stability, and prosperity. Threats include foreign-based terrorism, foreign espionage, cyber threat activity, kidnapping of Canadians abroad and attacks on our embassies, among others.

EXECUTIVE SUMMARY

Hostile actors are increasingly leveraging artificial intelligence (AI) tools in attempts to interfere in democratic processes, including elections, around the globe. Over the past two years, these tools have become more powerful and easier to use. They now play a pervasive role in political disinformation, as well as the harassment of political figures. They can also be used to enhance hostile actors' capacity to carry out cyber espionage and malicious cyber activities.

This report is an update to the Cyber Threats to Canada's Democratic Process: 2023 Update[1] (TDP 2023). Although the assessments contained in that report remain relevant, the rapid technological advances over the past two years in AI pose a new challenge. Accordingly, this update addresses exclusively threat actors and their use of AI to target democratic processes globally and in Canada. While it is difficult to predict what disinformation or influence campaigns will gain traction, we assess that it is very unlikely (i.e. roughly 10-30% chance) that disinformation, or any AI-enabled cyber activity, would fundamentally undermine the integrity of Canada's democratic processes in the next Canadian general election. As AI technologies continue to advance and cyber adversaries improve their proficiency in using AI, the threat against future Canadian general elections is likely to increase.

Key findings and global trends

- In the last two years, hostile actors have increasingly used generative AI to target global elections, including in Europe, Asia, and in the Americas. While TDP 2023 counted only one case of generative AI being used to target an election between 2021 and 2023, we observed 102 reported cases of generative AI being used to interfere with or influence 41 elections, or 27%, of elections held between 2023 and 2024. These cases involved the use of AI to create disinformation, actively spread disinformation online, and harass politicians. These new developments are driven by improvements in the quality, cost, efficiency, and accessibility of AI technology.

- While we were unable to attribute the majority of the AI-enabled campaigns against global elections to specific actors, our research did identify a high number of threat activities attributed to Russia and the People's Republic of China (PRC). We assess it almost certain that these states, as well as a range of non-state actors, leverage generative AI to spread disinformation narratives, in particular to sow division and distrust within democratic societies. We assess it very likely that Russia and the PRC will continue to be responsible for most of the attributable nation state AI-enabled cyber threat and disinformation activity targeting democratic processes.

- A range of threat actors are using generative AI to pollute the information environment. Of 151 global elections between 2023 and 2024, there were 60 reported AI-generated synthetic disinformation campaigns and 34 known and likely cases of AI-enabled social botnets. The increased use of generative AI marks a change in how disinformation is created and spread but not in the underlying motives and intended effects of disinformation campaigns. We assess it likely that such campaigns will continue to grow in scale as AI technology enabling synthetic disinformation becomes increasingly available.

- We assess it likely that, consistent with non-AI-enabled forms of disinformation, most foreign created AI-generated content does not gain significant visibility in democratic societies. However, information that does gain visibility is usually wittingly or unwittingly amplified by popular domestic and transnational commentators. In addition, foreign actors have displayed an ability to create and spread viral disinformation using generative AI. We assess it likely that, as foreign actors refine their AI-enabled methods, their disinformation will gain greater exposure online. Nonetheless, it remains difficult to predict which piece of disinformation will gain exposure or find resonance online.
- The National Cyber Threat Assessment 2025-2026[2] (NCTA 2025-2026) documented that cybercriminals and state-sponsored actors are using generative AI to make social engineering attacks more personal and persuasive. We assess it likely that over the next two years, threat actors will integrate generative AI into social engineering attacks against political and public figures, as well as election management bodies. Although we have not yet observed an actor using generative AI to target elections in this way, we cannot rule out the possibility it has already happened.
- We further assess it likely that, over the next two years, actors targeting Canada will use a range of AI technologies to improve the stealth and efficacy of malware they seek to deploy against target voters, politicians, public figures, and electoral institutions.
- Nation states, in particular the PRC, are undertaking massive data collection campaigns, collecting billions of data points on democratic politicians, public figures, and citizens around the world. Advances in predictive AI allow human analysts to quickly query and analyze these data. We assess it likely that such states are gaining an improved understanding of democratic political environments as a result. By possessing detailed profiles of key targets, social networks, and voter psychographics, threat actors are almost certainly enhancing their capabilities to conduct targeted influence and espionage campaigns.
- Cybercriminals and non-state actors are using generative AI to create deepfake pornography of politicians and public figures—almost all the targets were women. While most cases do not appear to have been part of a deliberate influence campaign, deepfake pornography deters participation in democracy for those targeted. Further, we assess it likely that, on at least one occasion, that content was seeded to deliberately sabotage the campaign of a candidate running for office. We assess that these AI-enabled personal attacks will almost certainly increase given the wide availability of these models.

Key terms

Machine learning: Methods or models that enable machines to learn how to complete a task from given data without explicitly programing a step-by-step solution.

Generative AI: A subset of machine learning that generates new content based on patterns extracted from large volumes of training data. Generative AI can create many forms of content including text, images, audio, video, or software code.

Predictive AI: A subset of machine learning that consumes input data but, rather than producing an image or a text, it discovers patterns in data to classify new data, like object recognition in images or words in speech recognition.

ABOUT THIS REPORT

This report provides an update to TDP 2023, published in December 2023. Given the changes in AI and machine learning technology since then, the report focuses on the threat posed by hostile actors using these technologies to target Canada's democratic process in 2025. The key findings stated in TDP 2023 remain relevant to the present threat environment.

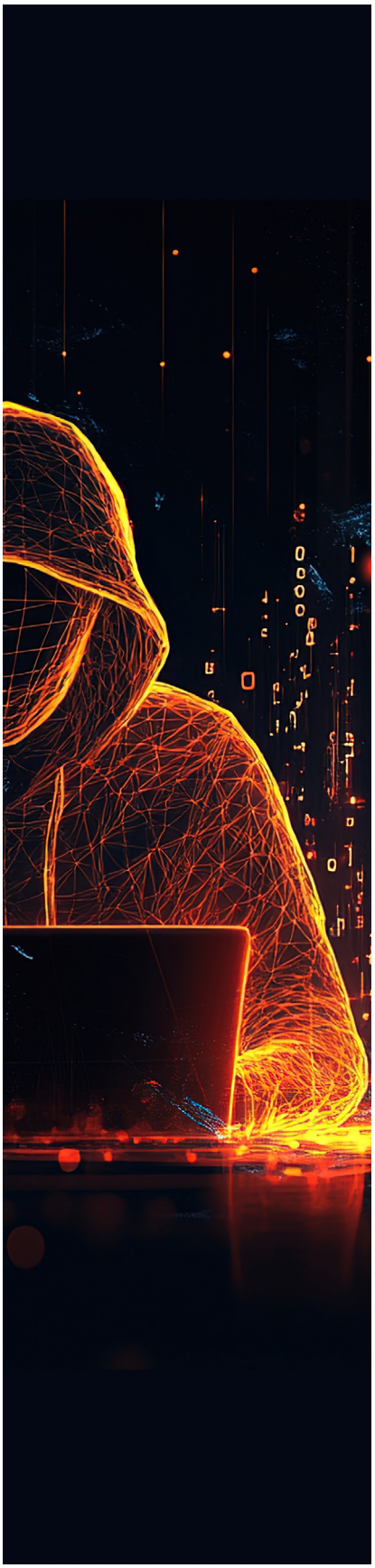
Scope

This report considers AI-enabled cyber threat activity that affects democratic processes globally. Cyber threat activity (e.g. spear phishing, malware) is AI-enabled when it integrates AI components (generative or other machine learning methods) to compromise the security of an information system by altering the confidentiality, integrity, or availability of a system or the information it contains. This assessment also considers AI-enabled influence campaigns, which occur when cyber threat actors use generative AI and predictive AI to research intelligence targets and to covertly manipulate online information.

We discuss a wide range of cyber threats to global and Canadian political and electoral activities, particularly in the context of Canada's next general election, currently set for 2025. Providing threat mitigation advice is outside the scope of this report.

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



More information

Further resources can be found on the Cyber Centre's cyber security guidance page[3] and on the Get Cyber Safe[4] website.

For more information about cyber tools and the evolving cyber threat landscape, consult the following publications:

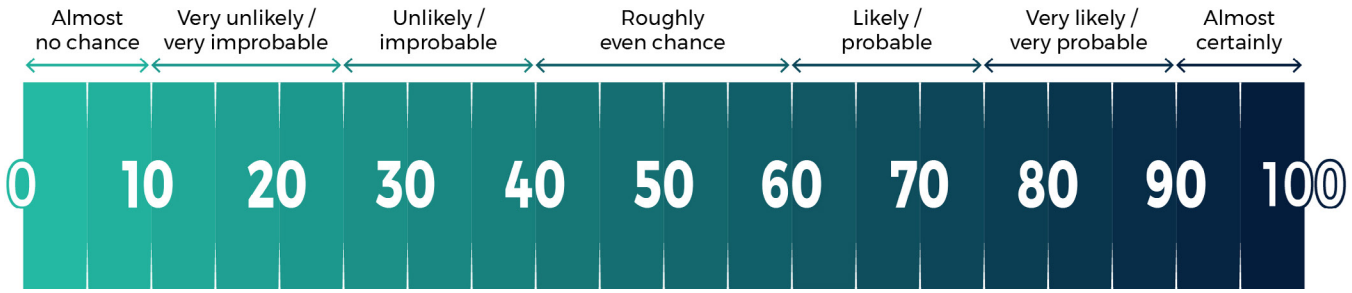
- National Cyber Threat Assessment 2025-2026[5]
- An Introduction to the Cyber Threat Environment[6]
- How to identify misinformation, disinformation, and malinformation[7]

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 **January 27, 2025**.

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

Compared with earlier versions of Cyber Threats to Canada's Democratic Process, which focused on the broad cyber threat to national elections, this update focuses exclusively on the threat posed by AI. It provides information on how cyber threat actors are using powerful developments in AI, specifically generative AI and predictive AI, to target the electoral process, harm democratic actors, and mislead and disinform voters.

Canadian elections: An attractive target for foreign actors

Foreign threat actors are interested in targeting Canadian elections for a multitude of reasons. Canada is a member of the North Atlantic Treaty Organization (NATO), the Five Eyes (FVEY) intelligence alliance, and is economically and culturally integrated with the United States (US).

As an active player in the international community, Canada participates in key institutions such as the United Nations (UN), Organization for Economic Cooperation and Development (OECD), the World Trade Organization (WTO), the International Monetary Fund (IMF), and the World Bank. As a major economy, Canada is a member of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), as well as multilateral forums such as the Group of 20 (G20) and the Group of 7 (G7). Government of Canada decisions on matters of military, trade, investment, and migration all affect the global community, as do the products of Canadian culture and science. We assess it almost certain that foreign actors target Canadian elections to influence how these decisions are made, as well to weaken our capacity for decision-making entirely.

AI-enabled cyber threats to Canada's democratic process

The malicious use of AI is a growing threat to Canadian elections, a point first noted in the Cyber Centre's 2019 Update: Cyber Threats to Canada's Democratic Process.[8] Generative AI at that time was expensive and required technical knowledge to use but has since become less costly and more accessible to non-technical users. User-friendly web interfaces, easy prompts, and few regulations or guardrails make it easier for more threat actors to engage in malicious cyber activity.[9] The speed and quality of output from generative AI models has also markedly improved, for instance from the first Generative Pre-Trained Transformer 1 (GPT-1) to GPT-4 now used for high-quality synthetic content generation.[10] These and related technologies have enabled adversarial actors to generate persuasive deepfakes and design convincing chatbots capable of spreading disinformation personalized to their target audience. The customization of content to specific targets with generative AI has also been used to enhance phishing attacks and enable new forms of digital harassment, cybercrime, and espionage. Predictive analytics allow data processing at a sophistication and volume unachievable by non-AI enabled methods, allowing human analysts to swiftly identify targets for potential hacking operations or populations to be flooded with targeted propaganda.[11]

The increased accessibility of generative AI compounds the risk to countries like Canada, whose citizens and infrastructure are highly connected. According to DataReportal, 94.3% of Canadians are registered Internet users while 80% of Canadians are active users of social media.[12] Survey data from Statistics Canada indicate that the majority of Canadians receive their news and information from the Internet or social media, increasing Canadians' exposure to AI-enabled malign influence campaigns.[13]

Although Canada's general elections are conducted by paper ballot, much of the surrounding electoral infrastructure is digitized, including voter registration systems, election websites, and communications between election management bodies and their employees. This creates a threat surface vulnerable to malicious cyber activity aimed at compromising the confidentiality, integrity, or availability of the underlying system before or during an election period. Cyber actors can use generative AI to quickly create targeted and convincing phishing emails, potentially allowing them illicit entry to this infrastructure, where they can install malware or exfiltrate and expose sensitive information.[14]

Canadians, their data, and public and political organizations are all potential targets of AI-enabled influence operations. Virtually every politician, candidate, and media personality has an online presence from which data can be mined and used to create fake content. Canadian political parties hold terabytes* of politically relevant data about Canadian voters as do commercial data brokers.[15]

PRC state-affiliated actors steal United Kingdom voter registry data

In July 2024, the United Kingdom (UK) government attributed a hack of the UK Electoral Commission to PRC state-affiliated actors. In addition to commission emails, hackers gained access to copies of electoral registries with the names and addresses of anyone registered to vote between 2014 and 2021.[16] AI-enabled cyber actors can use data such as this to develop propaganda campaigns tailored to specific audiences.

We assess foreign actors are almost certainly attempting to acquire this data, which they can then weaponize against Canadian democratic processes. Cyber actors can combine purchased or stolen data with public data about Canadians to create targeted propaganda campaigns, built on predictive analytics and using AI-generated content.[17] Malicious cyber actors have also used social botnets to take advantage of social media recommendation algorithms, amplify disinformation narratives, and even engage directly with voters in other countries.[18] Based on this capacity, we assess that cyber actors can almost certainly target Canadian voters in the same manner.

We assess that countries pursuing adversarial strategies against Canada and our allies almost certainly possess the capabilities illustrated above. We assess that the PRC is likely to employ these capabilities to push narratives favourable to its interests and spread disinformation among Canadian voters. For Russia and Iran, we assess that Canadian elections are almost certainly lower priority targets compared to the US or the UK. We also assess that, if these states do target Canada, they are more likely to use low-effort cyber or influence operations.

Domestic actors, as well as activists and thrill-seekers based abroad, also possess access to off-the-shelf generative AI tools. We assess such actors will almost certainly use these tools to spread disinformation ahead of a national election. We assess that increased geopolitical tensions between Canada and other states are likely to result in cyber threat actors, including non-state actors, using AI-enabled tools to target Canada's democratic process. Ahead of the 2021 general election, for example, known or likely PRC affiliated actors spread non-AI enabled disinformation about politicians running for office, whom they assessed to be anti-PRC.[19]

* A single terabyte is the equivalent of approximately 500 hours of HD video or 6.5-million document pages stored in PDF form.

CHANGES IN AI TECHNOLOGY

Generative AI is a type of artificial intelligence that generates new content by modelling features of data from large datasets. Generative AI can create new content in many forms, including text, image, audio, or computer code. Similar to generative AI, predictive AI consumes input data but, rather than producing an image or a text, it applies the patterns it has discovered to make an informed prediction to classify new data. As a result, software can quickly assess large pools of data to identify patterns and perform analysis that would otherwise require time consuming and costly manual annotation by a team of humans. Both types of AI rely on machine learning, which is the process by which machines learn how to complete a task from given data without explicitly programing a step-by-step solution.

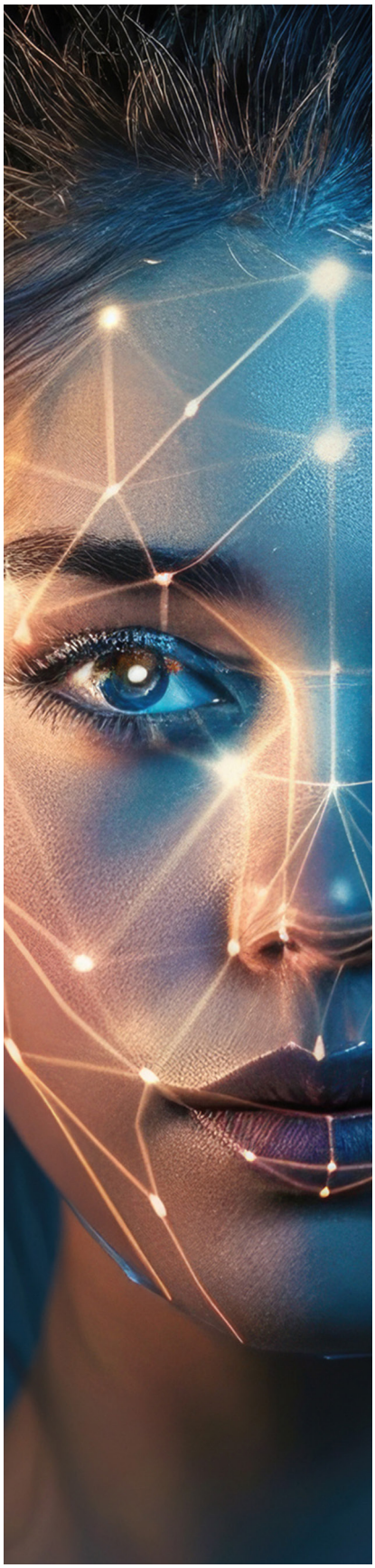
Large language models

Large language models (LLMs) are machine learning models that are trained on very large sets of language data using self- and semi-supervised learning. Early language models generated text via next word prediction, but more recent LLMs have significantly built on this function—learning from very large text datasets and sophisticated modelling—so that users can enter prompts on applications such as Chat GPT to output complete sentences or generate entire documents on a given topic, in a given style.[20]

The growing accessibility and diminishing cost of these technologies has enabled their use in cybercrime and in spreading disinformation and attacking democratic infrastructure.[21] Through either a fake or compromised account, a threat actor can use an LLM to write plausible communication that persuades the target to click a malicious link or inadvertently share their credentials or sensitive information.

LLMs can quickly produce tailored phishing products

To demonstrate the potential threat a researcher at the University of Oxford used ChatGPT and other LLMs to draft (but not send) personalized spear phishing emails to over 600 members of British Parliament.[22] Research has shown that LLMs can produce these emails at much faster rates than human researchers and are able to persuade targets to click on malicious links at rates comparable to phishing emails created by humans.[23]



The rise of deepfakes

Deepfakes refer to pictographic, video, and audio content that has been altered or created by a machine learning model. They can be distinguished from "cheap fakes", which are also designed to deceive, but, because they are created with less sophisticated software, are of lower quality and easier to identify.[24]

Although deepfake technology has existed since 2014, it was difficult to use and computationally intensive until the 2021-2022 release of image generation models such as GPT, DALL-E, and Midjourney.[25] Today, a convincing deepfake can be made from only a few seconds of video or audio, requiring little technical expertise from the user.[26] Deepfakes are being used against elections globally, primarily to spread disinformation.[27]

A deepfaked voice or video call can also be used by a malicious actor to trick a target into sharing sensitive information. Although we have not yet observed this in the context of an election, cyber criminals have successfully used generative AI in this manner to carry out billions of dollars' worth in fraud.[28]

AI-enabled scammers steal $35 million

In 2024, hackers used a deepfake to impersonate the Chief Financial Officer (CFO) of a company based in Hong Kong. During a video call with a financial worker, they tricked the worker into transferring nearly $35 million (CAD) to the hacker's bank accounts.[29]

Machine learning analytics and the exploitation of big data

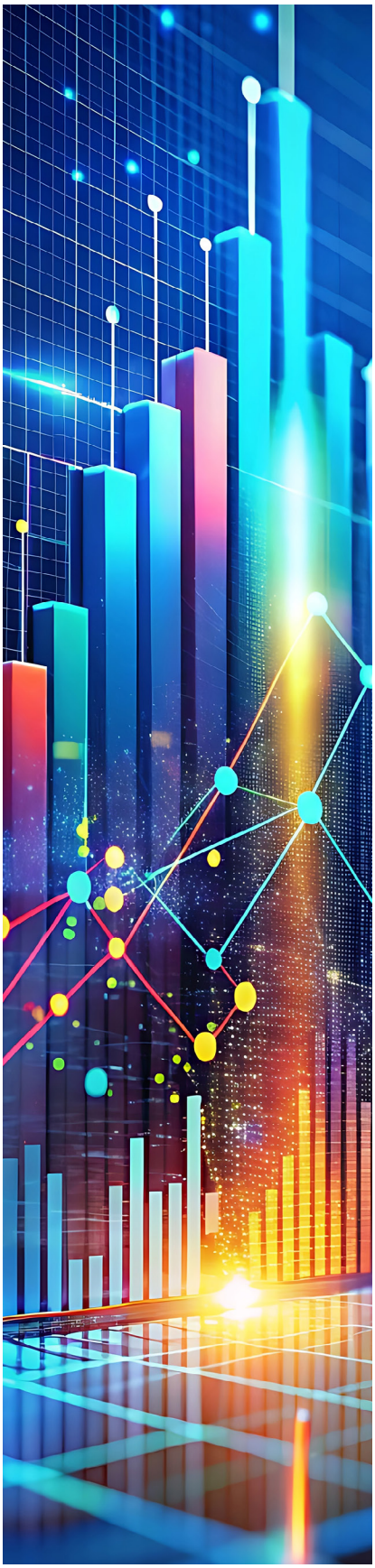
Machine learning models are powerful tools for analyzing big data. Master datasets are created by collecting, purchasing, or acquiring huge amounts of data, measured in peta- or exabytes,* and require powerful computers to store, query, and analyze. Advances in chip design, software architecture, and computing power have enabled advanced analytics, vastly increasing the speed and accuracy with which big data can be processed.[30]

Machine learning analytics are used by social media companies to identify and promote content assessed as most likely to sustain and generate engagement from a user. Social media platforms have designed their machine learning recommendation algorithms to favour emotionally charged and polarizing content, which can be used to misinform, radicalize, and divide users.[31] Malicious actors may take advantage of these algorithms to promote their favoured political narratives ahead of elections, while certain platforms themselves have been noted to amplify biased content.[32]

In the hands of adversarial actors, big data can be exploited by machine learning to provide intelligence that enables threat actors to influence targets, including through both human operations and targeted propaganda.[33] The collation of data, for example, can produce profiles of users—or psychographic information individualized to each voter or voter group, reflecting their attitudes, aspirations, values, and fears.[34] Likewise, real-time data analytics, capable of collecting and processing data as it is created, enable instantaneous feedback responses and on-demand intelligence reporting.[35]

Russian propaganda agencies purchase targeted advertising to target US federal elections

According to the US Federal Bureau of Investigation (FBI), in fall 2023, Russian propaganda agencies purchased Meta's advertising services, which rely on predictive AI, to direct propaganda towards groups that Russian agencies had assessed as receptive towards given propaganda narratives.[36]



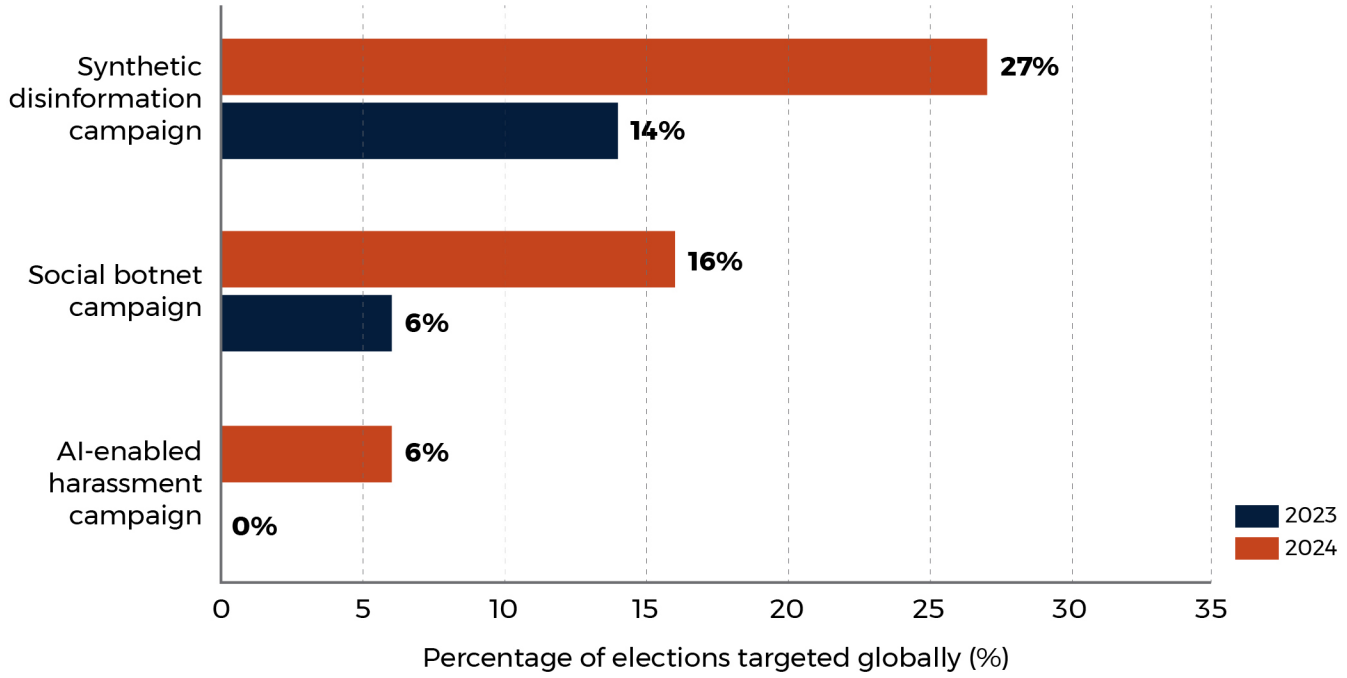
* A petabyte is 1,000 terabytes, or the equivalent of 11,000 HD movies. An exabyte is 1,000 petabytes.

GLOBAL TRENDS

The Cyber Centre has analyzed cyber threat activity targeting national level elections since 2015. This update focuses on AI-enabled threats, with data starting from 2023, the year in which our research first indicated that threat actors used generative AI to target a democratic process.

Since 2023, we have observed an increase in the amount of AI-enabled cyber threat activity targeting elections worldwide. We assess that the data almost certainly underestimates the total amount of events targeting global democratic processes, as not all cyber activity is reported or detected. Similarly, deepfakes and LLM-generated texts can be difficult to identify or distinguish from human-generated content. Based on our observations from 2023 and 2024, we identified four global trends.

Figure 1: Growth in AI-enabled threats to democratic processes from 2023 to 2024



Types of AI-enabled threats

Synthetic disinformation campaign: The use of AI to create disinformation to be spread online, pushing a consistent message or theme, or as part of a sporadic and uncoordinated effort to create disinformation about candidates running for office.

Social botnet campaign: Automated botnets, characterized by the use of LLMs to generate content or AI-generated profiles.

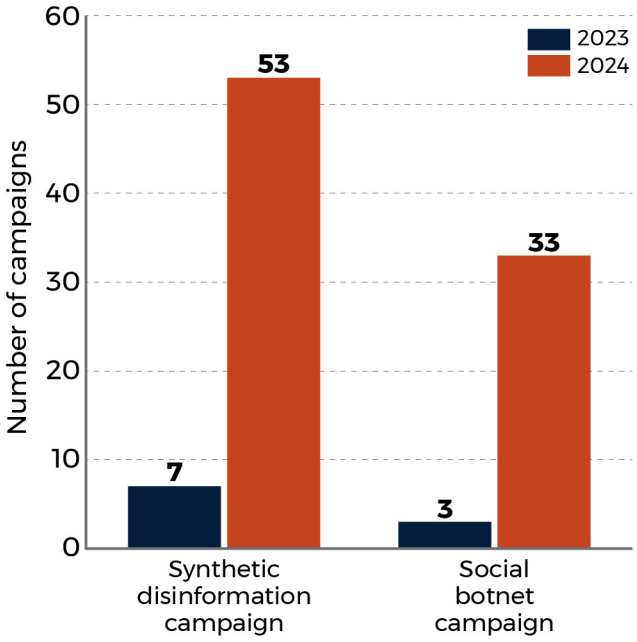
AI-enabled harassment campaign: The use of AI to aggressively pressure or intimidate a democratic politician.

Trend 1: Generative AI is polluting the information ecosystem

Between 2023 and 2024, there were 124 national level elections around the globe, as well as the European Union (EU) parliamentary elections in 2024, which took place across the EU's 27 member states. Of these 151 total elections, Cyber Centre research indicates that 40 were targeted by actors using generative AI to **create** or **spread** disinformation at least once during the 12 months leading up to the election. Since some countries were targeted multiple times, we identified 60 unique synthetic disinformation campaigns, meaning hostile actors used generative AI to create disinformation to be spread online. These campaigns either pushed a consistent message or theme or were part of a sporadic and uncoordinated effort to create disinformation about candidates running for office. These include cases where AI-imagery, audio, or text was used to confuse or disinform voters.

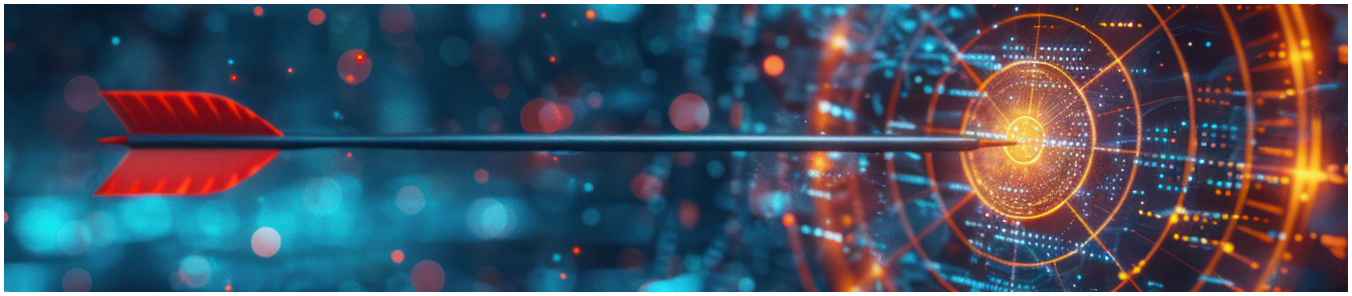
We also detected 36 known or likely cases where automated botnets were used to spread disinformation. These social botnets were often characterized by their use of AI-generated profile pictures, while the bots themselves proved capable of posting links, amplifying content, and interacting with authentic users. On several occasions, researchers and independent watchdogs observed social botnets attempting to manipulate social media recommendation algorithms. Affected platforms included X, Facebook, TikTok, WeChat, Telegram, and country specific platforms such as Taiwan's PTT.[37]

Figure 2: AI-enabled disinformation campaigns targeting democratic processes



Trend 2: AI involvement uncertain in phishing against electoral institutions

Between 2023 and 2024, we observed three reported cases where threat actors launched phishing campaigns in attempts to harvest credentials or engage in hack-and-leak operations against political and government organizations.[38] While we cannot confirm whether or not generative AI was used in these cases, the frequency with which threat actors have used LLMs to enhance phishing attacks in other contexts has rapidly increased over the past two years.[39] Likewise, over the same period, AI technology to improve and speed up phishing campaigns has proliferated on the dark web, along with the discovery of new techniques to circumvent anti-phishing controls on legitimate technology.[40] LLMs additionally allow non-native language actors to rapidly create content—not only in the target language but to also reflect the "voice" and idiosyncrasies specific to the user group or platform. We assess that AI-enabled phishing attacks against democratic targets will almost certainly increase over the next two years.



Trend 3: Advanced targeting based on machine learning analytics

It is difficult to observe in every case how nation states are using machine learning to analyze big data. However, we have observed the PRC and, to a lesser extent, Russia engaging in massive data collection campaigns, typically accomplished through open source acquisition, covert purchase, and theft.[41] Datasets of interest include information that is expressly political, such as voter registries or campaign data, or specific information that reveals, for example, an individual's shopping habits, health records, and browsing and social media activity.[42]

As assessed in NCTA 2025-2026, well-resourced nation states are very likely relying on AI to process and analyze these datasets, producing information for follow-on intelligence operations, including against elections.[43] Hostile actors are also using this data to enhance surveillance of, or online operations against, diaspora groups and their political representatives.[44] Separately, according to an FBI affidavit, Russia covertly used targeted advertising products sold by social media companies and search engines to conduct their propaganda efforts.[45]

Trend 4: Threat actors are using generative AI to harass public figures

Of the 151 elections we assessed from 2023 to 2024, at least 6 had instances where deepfakes were used to harass or intimidate politicians. The deepfakes used in this manner are of an exclusively sexual nature and have primarily targeted women politicians or 2SLGBTQI+ identifying persons in politics. This is consistent with a broader trend concerning AI: deepfake pornography makes up 98% of all deepfake videos online and 99% of those deepfakes target women.[46]

AI is being used in this way to humiliate, intimidate, and exclude targeted persons from political participation. While most efforts do not appear to have been part of deliberate influence campaigns, we assess it likely that, on at least one occasion, content was seeded to deliberately sabotage the campaign of a candidate running for office.[47]

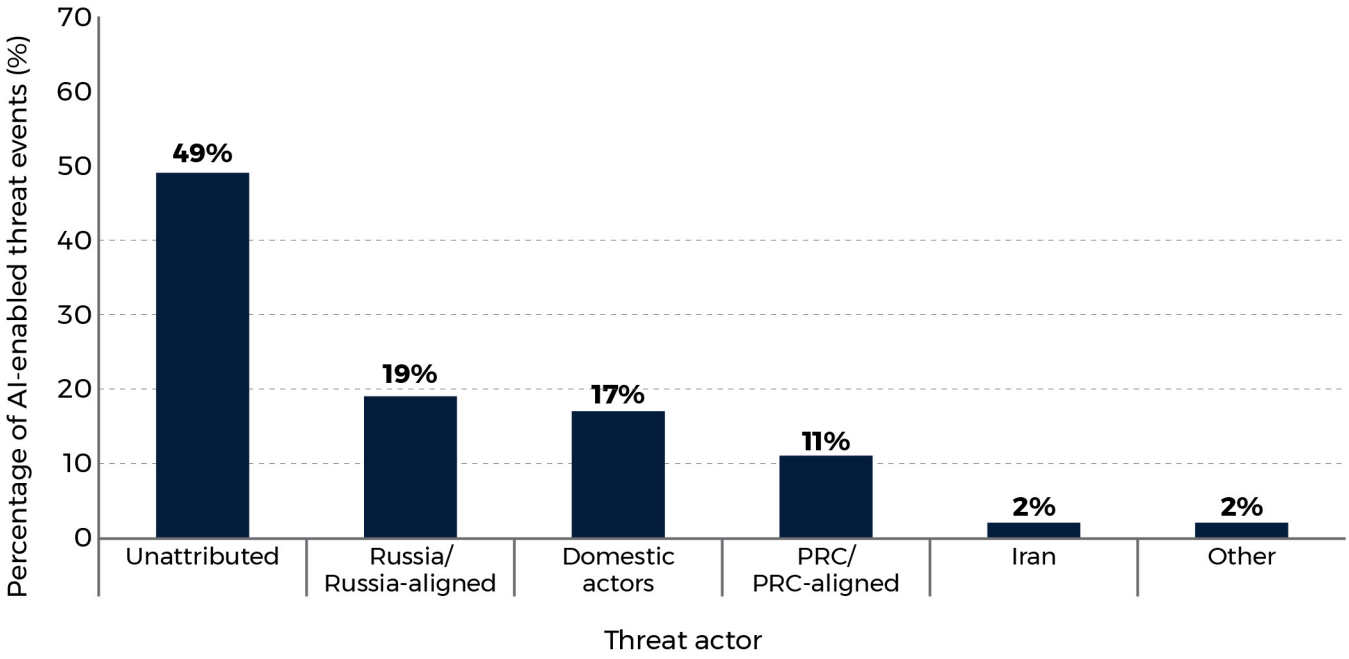
Women disproportionately targeted

In June 2024, British media reported that 400 digitally altered pornographic pictures of more than 30 high-profile women politicians had been found online.[48] In Greece, AI was used to create a nude image of a party leader, sparking derogatory homophobic comments.[49] Ahead of Bangladesh's 2024 elections, photographs were shared online falsely depicting a women politician in a bikini.[50]

MAIN THREAT ACTORS USING AI TO TARGET DEMOCRATIC PROCESSES

Around 49% of the AI-enabled activity that we observed—all of which involved the spread of disinformation or the harassment of politicians—could not be credibly attributed to a specific actor. From our research, the majority of **attributed** AI-enabled cyber threat activity emanates from state-sponsored actors with links to Russia, the PRC, and Iran. We assess their goal is almost certainly to break democratic alliances and entrench divisions within and between democratic states while also advancing their geopolitical goals.[51] We also note that political parties have maliciously used AI within their own countries, typically through the spread of disinformation.

Figure 3: Attributions of threats to democratic processes



Russia

Consistent with statistics we gathered in TDP 2023, Russia and pro-Russia non-state actors remain the most aggressive among attributed actors targeting global elections. We assess Russia's cyber threat activity is almost certainly aimed at harming the electoral prospects of parties or candidates that Russia perceives as pro-West in ideology and foreign policy orientation. Over the past two years, at least four prominent Russian networks have used AI to spread disinformation in distinctive ways.

Although we have not definitively observed Russian actors using AI to enhance their phishing or hack-and-leak efforts against elections, we assess it almost certain that they possess this capability. This assessment is based on similar activity undertaken by criminal groups and other nation states.[52] Likewise, we assess it very likely that Russia has the capability to use AI to improve the efficacy and stealth of malware to deploy against target assets.[53]

With regard to AI-enabled disinformation, a network known as Doppelganger (founded in April 2022) is operated by two Russia-based companies with known links to the Russian state.[54] Doppelganger relies on AI to spoof legitimate news websites, such as *Der Spiegel* or *The Guardian*, while using LLMs to generate articles containing disinformation.[55] A similar network known as CopyCop uses LLMs to create disinformation articles and deliver them via websites that purport to be news organizations based in western states.[56]

Storm-1679, a third network active since 2023, relies on generative AI to spam media organizations, researchers, and fact checkers with requests for story verification, in an effort to overwhelm their anti-disinformation resources.[57] Each of these networks has leveraged generative AI to create content as well as social botnets to amplify disinformation across various online mediums.

US vice-presidential candidate Tim Walz deepfake

The deepfake claimed to have been abused by Walz, during Walz's former job as a high school teacher. Although the video was fake, the person in the video appeared to have been an actual student at Walz's school. To create the deepfake, Storm-1516 had likely researched students at Walz's former school, used AI to create a fake video based on their likeness, and then deployed it against Walz.[58]

While the quality of Russian disinformation has varied, Russia and pro-Russia non-state actors have displayed an ability to create bespoke propaganda, designed to enhance its virality and political impact on the target state. In October 2024, Storm-1516 released a tailored deepfake of an individual claiming to have been abused by US vice-presidential candidate Tim Walz.[59] The attack was a blend of methods, combining disinformation with sexual degradation without concern for the intermediary victim.

Despite these efforts, we assess it likely that Russia's campaigns generally do not gain significant visibility without the amplification of witting or unwitting actors from within the targeted state.[60] According to German intelligence, Russia's Doppelganger campaigns garnered only 800,000 views* of its 700 fake websites across all its campaigns between November 2023 and August 2024.[61] Another researcher noted that most of the links shared by Doppelganger received little to zero engagement.[62] The Tim Walz abuse claim only gained significant attention after it was covered by influential American commentators.[63] Responsive efforts by the targeted states to remove the online infrastructure supporting these websites as well as deplatforming operations carried out by social media companies have blunted their overall visibility.[64]

Nonetheless, we assess that Russia almost certainly retains the intent and capability to continue using generative AI to pollute the democratic information environment. Recent trends among social media companies to move away from professional fact checking will likely increase user engagement with misleading content.[65]

* For contrast, the *Frankfurter Allgemeine Zeitung*, a popular German newspaper, typically receives over nine million views per month.

The People's Republic of China

The PRC poses a sophisticated and pervasive threat in the cyber domain. Using cyber and non-cyber means, the PRC carried out an aggressive malign influence campaign around Taiwan's 2024 presidential election.[66] With regard to AI, Taiwanese-based researchers identified a likely social botnet composed of over 14,000 accounts across Facebook, X, YouTube, TikTok, and PTT, a Taiwanese social media platform. The profile avatars for the bots were in some instances created by generative AI, while the bots themselves exhibited coordinated behaviour and similarity in commenting patterns. The accounts echoed narratives pushed by PRC state media and often sought to denigrate the US-Taiwanese relationship and harm the electoral candidacy of Lai Ching-Te, the leader of the Democratic People's Party.[67] The botnet also shared and amplified content that disparaged the character of various Taiwanese politicians, including the leak of an alleged deepfake sex tape posted to a pornographic website.[68]

Similarly, Spamouflage Dragon, a probable PRC-driven propaganda campaign that has targeted Canada in the past, has used generative AI to create disinformation to influence foreign voters ahead of democratic elections internationally.[69] Although these efforts did not garner much attention, independent research organizations have noted that the PRC is refining its propaganda efforts, which are starting to gain more engagement from authentic citizens in the targeted electorate.[70]

As stated earlier, the PRC conducts massive data collection operations against Western populations. Although these data serve various purposes, we assess it likely that the PRC has both the ability and intent to use machine learning to analyze these data to produce detailed intelligence profiles of potential targets connected to democratic processes.[71] These include voters, politicians, members of the media, public servants, and activists.[72] Working in cooperation with PRC-based technology companies, the PRC uses this data to aid intelligence work, including to:

- inform decision-making
- identify recruitment opportunities
- enhance influence operations[73]

We assess it almost certain that the PRC will continue to harvest politically relevant information from Western societies.

We assess it likely that the PRC has leveraged TikTok, a social media platform owned by the PRC-based company ByteDance, to promote pro-PRC narratives in democratic states and to censor anti-PRC narratives.[74] According to the Network Contagion Research Institute, the PRC "is deploying algorithmic manipulation in combination with prolific information operations to impact user beliefs and behaviours on a massive scale."[75] We assess it likely that these operations have, on at least one occasion, targeted voters ahead of an election.[76]

Spamouflage Dragon

In 2023, the Spamouflage network spread disinformation targeting dozens of MPs, including the Prime Minister, the leader of the opposition, and several members of Cabinet. The network has also used generative AI to target Mandarin-speaking figures in Canada.[77]

Iran

According to the FBI, in 2024, the Islamic Revolutionary Guard Corps (IRGC) used spear phishing to hack into one US presidential campaign and attempt to hack into the campaign of a second candidate.[78] It remains unclear whether the IRGC used AI in this case. However, the IRGC has been observed in other cases using LLMs to generate targeted and convincing emails inciting their target to click a link (or open an attachment) to navigate to a malicious webpage or download malware.[79]

We assess it very likely that a hostile actor like the IRGC could integrate AI into a similar cyber attack against election infrastructure. The IRGC also has spoofed login pages to harvest the credentials of their victims, a task which, like phishing, can be enhanced by AI technologies.[80] It is also likely that the IRGC has used LLMs to improve their malware code, disable antivirus software, and evade detection.[81]

IRGC hack of US presidential campaign

During a 2024 hack of a US presidential campaign, the IRGC exfiltrated sensitive information and attempted to share it with the media and individuals that IRGC believed to be associated with rival campaigns. The media and rival campaigns rebuffed these efforts, reporting them to law enforcement, which minimized the effects of the operation.[82] Although it is unclear if AI was used by the IRGC in this case, the IRGC has been known to use LLMs in similar activities.

Cybercriminals and non-state actors

Cybercriminals and non-state actors are almost certainly responsible for the vast majority of non-consensual deepfake pornography targeting politicians, public figures, and people in the media. Cybercriminals also prolifically conduct hack-and-leak operations against commercial and public databases, including in democratic states.[83] While the Cyber Centre defines cybercrime as financially motivated cyber threat activity, nation states are known buyers of stolen data.[84] Stolen data can be used for various purposes, and we assess it likely that some of this data is used by nation states to enhance their AI- and machine learning-enabled operations against democratic processes.

Cybercriminals are also known to take advantage of events with high media coverage, such as an election, as an opportunity to commit scams and fraud against voters.[85] We assess it very likely that, over the next two years, cybercriminals will use deepfakes and AI-enabled phishing to deploy a range of cyber attacks against democratic processes. These include more disruptive forms of cybercrime like ransomware.[86]

Non-state actors or domestic influencers may wittingly or unwittingly amplify AI-enabled foreign disinformation. Given that such actors typically form more connected and trusted links within domestic social networks, their impact on the amplification of disinformation is larger than that of regular users. As noted earlier, attempts by Russia-linked actors to seed salacious stories about Tim Walz failed to generate much attention until key American influencers engaged with and amplified the content from their platforms.[87]

IMPLICATIONS FOR CANADIAN ELECTIONS

We assess that the PRC, Russia, and Iran will very likely use AI-enabled tools to attempt to interfere with Canada's democratic process before and during the 2025 election. We assess it likely that cybercriminals will take advantage of election-related opportunities in Canada to conduct scams and fraud, without being uniquely focused on exploiting Canadian elections.

When targeting Canadian elections, threat actors are most likely to use generative AI as a means of creating and spreading disinformation, designed to sow division among Canadians and push narratives conducive to the interests of foreign states. We assess it very likely that PRC-affiliated actors will continue to specifically target Chinese-diaspora communities in Canada, pushing narratives favourable to PRC interests on social media platforms.[88] Since Canadians share a common information ecosystem with the US, Canadians have already been exposed to AI-enabled disinformation targeting US citizens.[89] It is almost certain that this trend will continue. However, the extent to which any given piece of disinformation will gain visibility or resonance among Canadians is unpredictable.

Canadian politicians and political parties are likely to be targeted by threat actors seeking to conduct hack-and-leak operations. As we have observed in other contexts, we assess it likely that threat actors will leverage LLMs to engage with targets as part of an extended phishing operation. However, we assess it very unlikely that hostile actors will carry out a destructive cyber attack against election infrastructure, such as attempting to paralyze telecommunications systems on election day, outside of imminent or direct armed conflict.

Finally, Canadian public figures, especially women and members of the 2SLGBTQI+ community, are at heightened risk of being targeted by deepfake pornography. Without updated legal and regulatory guidelines, we assess it very likely that the spread of this content will continue unabated.

LOOKING AHEAD

Cyber threat activity continues to be used to target democratic processes globally. The Cyber Centre, as part of CSE, produces advice and guidance to help inform Canadians about the cyber threats to Canada's elections.[90]

We provide cyber security advice and guidance to all major political parties, in part through publications such as the Cyber Security Guide for Campaign Teams[91] and Cyber Security Advice for Political Candidates.[92] Representatives from CSE form part of Canada's Security and Intelligence Threats to Elections (SITE) task force.[93]

We work closely with Elections Canada to protect its infrastructure and defend our elections from cyber threats. CSE is authorized by the Minister of National Defence to conduct defensive cyber operations (DCO) to protect the Government of Canada, including Elections Canada. This authorization allows CSE to disrupt malicious cyber activities against those systems. CSE is also authorized to protect systems of importance to the government, such as those related to a general election.

Additionally, the Cyber Centre's sensors program[94] helps defend Elections Canada's infrastructure by monitoring and mitigating potential cyber threats. We also provide expert advice through publications like Security Considerations for Electronic Poll Book Systems[95] and Cyber Security Guidance for Elections Authorities[96] to help electoral bodies enhance their cyber security measures.

To further protect our democratic institutions, the Privy Council Office has published resources for how to combat disinformation and foreign interference.[97] These include toolkits for community leaders, elected officials, public office holders, and public servants.

We encourage Canadians to consult the following resources related to the themes in this assessment:

- Cyber Security Guidance on Generative Artificial Intelligence (AI)[98]
- Guide on Security Considerations When Using Social Media in Your Organization[99]
- Cyber Security Guidance on Identifying and Countering Online Disinformation[100]
- Guidance on Using Social Media Safely[101]
- National Cyber Threat Assessment 2025-2026[102]
- How to Identify Misinformation, Disinformation, and Malinformation[103]
- Fact Sheet for Canadian Voters[104]

CSE's Get Cyber Safe[105] campaign continues to publish relevant advice and guidance throughout the year to inform Canadians about cyber security and the steps they can take to protect themselves online.

ENDNOTES

1 https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

2 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

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

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

5 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

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

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

8 https://www.cyber.gc.ca/sites/default/files/cyber/publications/tdp-2019-report_e.pdf

9 Jack Nicas and Lucía Cholakian Herrera, "Is Argentina the First A.I. Election?," *The New York Times*, November 15, 2023, https://www.nytimes.com/2023/11/15/world/americas/argentina-election-ai-milei-massa.html.

10 "History of Generative AI," Toloka, August 22, 2023, https://toloka.ai/blog/history-of-generative-ai/.

11 Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York: W.W. Norton and Company, 2023); "UAE : UAE's Edge Group and G42 Get into Natural Language Processing - 22/03/2023," Intelligence Online, December 17, 2024, https://www.intelligenceonline.com/surveillance--interception/2023/03/22/uae-s-edge-group-and-g42-get-into-natural-language-processing,109926405-art.

12 "Digital 2024: Canada," DataReportal – Global Digital Insights, February 22, 2024, https://datareportal.com/reports/digital-2024-canada.

13 Statistics Canada, "Canadian Social Survey - Quality of Life, Virtual Health Care and Trust, 2023," November 10, 2023, https://www150.statcan.gc.ca/n1/daily-quotidien/231110/dq231110b-eng.htm.

14 Belle Lin, "Welcome to the Era of BadGPTs," *The Wall Street Journal*, February 28, 2024, https://www.wsj.com/articles/welcome-to-the-era-of-badgpts-a104afa8; "The Near-Term Impact of AI on the Cyber Threat," National Cyber Security Centre, January 24, 2024, https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

15 Elizabeth Judge and Michael Pal, "Voter Privacy and Big-Data Elections," *Osgoode Hall Law Journal* 58, no. 1 (March 9, 2021): 1–55.

16 "UK Calls out China State-Affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians," March 25, 2024, https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians.

17 Dan Milmo, "Hacked UK Voter Data Could Be Used to Target Disinformation, Warn Experts," *The Guardian*, August 9, 2023, https://www.theguardian.com/politics/2023/aug/09/hacked-uk-electoral-commission-data-target-voter-disinformation-warn-expert.

18 Darren Linvill and Patrick Warren, "Digital Yard Signs: Analysis of an AI Bot Political Influence Campaign on X", Clemson University Media Forensics Hub, September 30, 2024, https://open.clemson.edu/mfh_reports/7/; Kai-Cheng Yang and Filippo Menczer, "Anatomy of an AI-Powered Malicious Social Botnet," *Journal of Quantitative Description: Digital Media* 4 (May 29, 2024).

19 "Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions," Government of Canada, May 3, 2024, 128–35, https://foreigninterferencecommission.ca/fileadmin/user_upload/Foreign_Interference_Commission_-_Initial_Report__May_2024__-_Digital.pdf.

20 "Better Language Models and Their Implications," Open AI, February 14, 2019, https://openai.com/index/better-language-models/.

21 Belle Lin, "Welcome to the Era of BadGPTs," *The Wall Street Journal*, February 28, 2024, https://www.wsj.com/articles/welcome-to-the-era-of-badgpts-a104afa8.

22 Julian Hazell, "Spear Phishing with Large Language Models," Oxford Internet Institute, December 14, 2023, https://cdn.governance.ai/Spear_Phishing_with_Large_Language_Models.pdf.

23 Fredrik Heiding, Bruce Schneier, and Arun Vishwanath, "AI Will Increase the Quantity — and Quality — of Phishing Scams," *Harvard Business Review*, May 30, 2024, https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams.

24 A summary of deepfake technology and the threat it could pose to Canada can be found here: "The Evolution of Disinformation: A Deepfake Future," Canadian Security Intelligence Service, October 2023, https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future.html.

25 "The Evolution of Disinformation: A Deepfake Future," Canadian Security Intelligence Service, October 2023, https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future.html.

26 Nate Nelson, "Deepfake-Generating Apps Explode, Allowing Multimillion-Dollar Corporate Heists," February 5, 2024, https://www.darkreading.com/threat-intelligence/deepfake-apps-explode-multimillion-dollar-corporate-heists.

27 "AI Deepfakes Can Sway Voters and Disrupt Elections," *Financial Times*, July 7, 2024, https://www.ft.com/video/4f473456-ca0e-4f0b-a9aa-9bac1e3220a6.

28 Satish Lalchand et al., "Generative AI Is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking", Deloitte, May 29, 2024, https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html.

29 Kathryn Mannie, "Company out $35M after Scammers Stage Video Call with Deepfake CFO, Coworkers," *Global News*, February 5, 2024, https://globalnews.ca/news/10273167/deepfake-scam-cfo-coworkers-video-call-hong-kong-ai/.

30 "Top Trends in Big Data for 2024 and Beyond," TechTarget, January 12, 2024, https://www.techtarget.com/searchdatamanagement/feature/Top-trends-in-big-data-for-2021-and-beyond; Our World Data, "Computation Used to Train Notable Artificial Intelligence Systems, by Domain," 2023, https://ourworldindata.org/grapher/artificial-intelligence-training-computation.

31 William J. Brady et al., "Algorithm-Mediated Social Learning in Online Social Networks," *Trends in Cognitive Sciences* 27, no. 10 (October 1, 2023): 947–60.

32 Smitha Milli et al., "Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media," Columbia University, January 3, 2024), http://knightcolumbia.org/content/engagement-user-satisfaction-and-the-amplification-of-divisive-content-on-social-media; Dominik Bär et al., "Systematic Discrepancies in the Delivery of Political Ads on Facebook and Instagram," *PNAS Nexus* 3, no. 7 (July 1, 2024), https://doi.org/10.1093/pnasnexus/pgae247; Joel Finkelstein et al., "The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States," Network Contagion Research Institute, August 2024, https://networkcontagion.us/reports/the-ccps-digital-charm-offensive/; Karen Hao, "Troll Farms Reached 140 Million Americans a Month on Facebook before 2020 Election, Internal Report Shows," *MIT Technology Review*, September 16, 2021, https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election/.

33 Robert McMillan, Dustin Volz, and Aruna Viswanatha, "China Is Stealing AI Secrets to Turbocharge Spying, U.S. Says," *The Wall Street Journal*, December 25, 2023, https://www.wsj.com/tech/ai/china-is-stealing-ai-secrets-to-turbocharge-spying-u-s-says-00413594.

34 Mohar Chatterjee, "What AI Is Doing to Campaigns," Politico, August 15, 2024, https://www.politico.com/news/2024/08/15/what-ai-is-doing-to-campaigns-00174285.

35 Sandro Shubladze, "Empowering Decision-Making With Real-Time Data Analytics," *Forbes*, April 30, 2024, https://www.*forbes*.com/councils/*forbes*techcouncil/2024/04/30/empowering-decision-making-with-real-time-data-analytics/.

36 "US FBI Affidavit in Support of Seizure Warrant," United States District Court for the Eastern District of Pennsylvania, September 9, 2024, 30–31, 219, https://www.justice.gov/opa/media/1366261/dl.

37 See, for example: "AI and Covert Influence Operations: Latest Trends," Open AI, May 30, 2024, https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/; "2024 Taiwan Presidential Election Information Manipulation AI Observation Report," AI Labs, 2024, https://ailabs.tw/wp-content/uploads/2024/01/2024-Taiwan-Presidential-Election-Information-Manipulation-AI-Observation-Report-2.pdf; Morgan Wack, Darren Linvill, and Patrick Warren, "Old Despots, New Tricks - An AI-Empowered Pro-Kagame/RPF Coordinated Influence Network on X," Media Forensics Hub Reports, June 2024, https://open.clemson.edu/mfh_reports/5.

38 The three observed cases were phishing campaigns against the Trump and Harris presidential campaigns, and against Moldovan officials during the Moldovan election in fall 2024. Daryna Antoniuk, "Google: Iranian Hackers Targeting Affiliates of Both US Presidential Campaigns," August 15, 2024, https://therecord.media/iran-targets-us-election; "Operation MiddleFloor: Disinformation Campaign Targets Moldova Ahead of Presidential Elections and EU Membership Referendum," Check Point Research, October 9, 2024, https://research.checkpoint.com/2024/disinformation-campaign-moldova/.

39 "ThreatLabz 2024 Phishing Report," ZScaler, April 2024, https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report.

40 Lin, "Welcome to the Era of BadGPTs"; Kevin Poireault, "The Dark Side of Generative AI: Five Malicious LLMs Found on the Dark Web," Infosecurity Europe, August 10, 2023, https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/generative-ai-dark-web-bots.html.

41 Cate Cadell, "China Harvests Masses of Data on Western Targets, Documents Show," *Washington Post*, December 31, 2021, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html; Craig Silverman, "Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months," ProPublica, July 1, 2022, https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine.

42 Mark Landler and Stephen Castle, "U.K. Accuses China of Cyberattacks Targeting Voter Data and Lawmakers," *The New York Times*, March 25, 2024, https://www.nytimes.com/2024/03/25/world/europe/uk-china-cyberattack-hacking.html; Christopher Balding, "Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua," *SSRN Scholarly Paper* (Rochester, NY: Social Science Research Network, September 13, 2020), https://doi.org/10.2139/ssrn.3691999.

43 Patrick Tucker, "How China Used TikTok, AI, and Big Data to Target Taiwan's Elections," April 8, 2024, https://www.defenseone.com/technology/2024/04/how-china-used-tiktok-ai-and-big-data-target-taiwans-elections/395569/.

44 See, for example, "Press Release: Eastern District of New York | 34 Officers of People's Republic of China National Police Charged with Perpetrating Transnational Repression Scheme Targeting U.S. Residents," United States Attorney's Office, April 17, 2023, https://www.justice.gov/usao-edny/pr/34-officers-peoples-republic-china-national-police-charged-perpetrating-transnational. The full indictment can be accessed here, see esp. p. 8-9: https://web.archive.org/web/20250204065726/https:/www.justice.gov/d9/2023-04/squad_912_-_23-mj-0334_redacted_complaint_signed.pdf.

45 US FBI Affidavit in Support of Seizure Warrant," United States District Court for the Eastern District of Pennsylvania, September 9, 2024, 30, 216–20, https://www.justice.gov/archives/opa/media/1366261/dl.

46 "2023 State Of Deepfakes: Realities, Threats, And Impact," Security Hero, December 2023, https://www.securityhero.io/state-of-deepfakes/.

47 Chen-Ling Hung et al., "AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election," Thomson Foundation, April 2024, 5, https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf.

48 Kathy Newman, "Exclusive: Top UK Politicians Victims of Deepfake Pornography," *Channel* 4 (July 1, 2024), https://www.channel4.com/news/exclusive-top-uk-politicians-victims-of-deepfake-pornography.

49 (Greek language resource) Thanos Sitistas Epachtitis, "Κατασκευασμένη με λογισμικό AI η φωτογραφία που "δείχνει" τον Σ. Κασσελάκη και τον Τ. Μακμπέθ γυμνούς σε παραλία," Greece Fact Check, April 3, 2024, https://www.factchecker.gr/2024/04/03/ai-generated-image-of-kasselakis-and-tyler-naked-on-a-beach/.

50 The Tribune, "Pakistanis, Bangladeshi Politicians Are New Targets of Deepfake, 90 per Cent of Videos Online Are Pornographic," December 14, 2023, https://www.tribuneindia.com/news/science-technology/from-rashmika-mandanna-to-bangladeshi-politician-filmed-in-a-bikini-90-per-cent-of-deepfake-videos-online-are-pornographic-571782/.

51 Max Seddon, Demetri Sevastopulo, and Joe Leahy, "Vladimir Putin and Xi Jinping Vow to Co-Operate against 'Destructive and Hostile' US," *Financial Times*, May 16, 2024, https://www.ft.com/content/f77028c8-c960-4d10-b0eb-4c511924a4d5; Jonathan Rauch, "Confronting the Axis of Resistance," The Atlantic, July 1, 2024, https://www.theatlantic.com/ideas/archive/2024/07/russia-china-nato-axis-resistance/678831/.

52 James Rundle, "Generative AI Could Revolutionize Email—for Hackers," *The Wall Street Journal*, September 6, 2023, https://www.wsj.com/articles/generative-ai-could-revolutionize-emailfor-hackers-5a8c725c.

53 Other state actors have been observed relying on LLMs to develop code to evade anti-virus protection software. See Microsoft Security, "Staying Ahead of Threat Actors in the Age of AI," February 14, 2024, https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/.

54 "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts," U.S. Department of the Treasury, 20 2024, https://home.treasury.gov/news/press-releases/jy2195; Sarah Thust, "Doppelganger: CORRECTIV Investigations Bring Russian Propaganda Campaign to a Halt," Correctiv, November 15, 2024, https://correctiv.org/en/fact-checking-en/2024/11/15/doppelganger-correctiv-investigations-bring-russian-propaganda-campaign-to-a-halt/.

55 Information about Doppelganger, including on their use of AI, can be found here: "What Is the Doppelganger Operation? List of Resources," EU DisinfoLab, October 30, 2024, https://www.disinfo.eu/doppelganger-operation/.

56 "Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale," Insikt Group, May 9, 2024, https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf.

57 "Operation Overload Impersonates Media to Influence 2024 US Election," Insikt Group, October 23, 2024, https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf.

58 David Gilbert, "Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims," *Wired*, October 21, 2024, https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/.

59 Gilbert, "Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims."

60 Matthew Leake, "Are Fears about Online Misinformation in the US Election Overblown? The Evidence Suggests They Might Be," Reuters Institute for the Study of Journalism, October 24, 2024, https://reutersinstitute.politics.ox.ac.uk/news/are-fears-about-online-misinformation-us-election-overblown-evidence-suggests-they-might-be. For a related study on the visibility of (non-AI related) pro-Russian content, see Jennifer Allen, "Worried about the Russians Dividing America? The Call Is Coming from inside the House," Media Bias Detector, September 28, 2024, https://mediabiasdetector.com/blog.

61 (German language resource) "„Doppelgänger" Interne Details Zu Russicher Desinformationaskampagne," Bayerisches Landesamt für Verfassungsschutz, August 2024, https://www.verfassungsschutz.bayern.de/mam/anlagen/baylfv_vollanalyse_doppelgaenger.pdf.

62 Thomas Rid, "The Lies Russia Tells Itself," *Foreign Affairs*, September 30, 2024, https://www.foreignaffairs.com/united-states/lies-russia-tells-itself.

63 Gilbert, "Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims."

64 See, for example: "TAG Bulletin: Q3 2024," Google Threat Analysis Group, September 12, 2024, https://blog.google/threat-analysis-group/tag-bulletin-q3-2024/; Margarita Franklin et al., "Adversarial Threat Report," Meta, May 2024, https://md.teyit.org/file/meta-threat-report.pdf.

65 Yuwei Chuai et al., "Did the Roll-Out of Community Notes Reduce Engagement With Misinformation on X/Twitter?," *Proceedings of the ACM on Human-Computer Interaction* 8, no. CSCW2 (November 2024), https://doi.org/10.1145/3686967.

66 Stuart Lau, "China Bombards Taiwan with Fake News Ahead of Election," Politico, January 10, 2024, https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election/; Maggie Miller and Joseph Gedeon, "Taiwan Bombarded with Cyberattacks Ahead of Election," Politico, January 11, 2024, https://www.politico.com/news/2024/01/11/taiwan-cyberattacks-election-china-00134841; Alan Yu, Michael Clark, and Megan Shahi, "Taiwan's Election: PRC Interference and Its Implications for the 2024 Election Landscape," Center for American Progress, February 1, 2024, https://www.americanprogress.org/article/taiwans-election-prc-interference-and-its-implications-for-the-2024-election-landscape/.

67 "2024 Taiwan Presidential Election Information Manipulation AI Observation Report."

68 Chen Cheng-yu and Liu Hsin-han, "2024 Elections: Cabinet Supports Probe of Deepfake Video of Legislator," *Taipei Times*, January 10, 2024, https://www.taipeitimes.com/News/taiwan/archives/2024/01/10/2003811892; Hung et al., "AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election."

69 "The #Americans : Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Divisive Narratives Ahead of 2024 Election," Graphika, September 2024, https://public-assets.graphika.com/reports/graphika-report-the-americans.pdf; "Probable PRC 'Spamouflage' Campaign Targets Dozens of Canadian Members of Parliament in Disinformation Campaign."

70 David Gilbert, "Why China Is So Bad at Disinformation," *Wired*, April 29, 2024, https://www.*wired*.com/story/china-bad-at-disinformation/.

71 "National Cyber Threat Assessment 2025-2026," Canadian Centre for Cyber Security, November 2024, https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf; McMillan, Volz, and Viswanatha, "China Is Stealing AI Secrets to Turbocharge Spying, U.S. Says."

72 Christopher Balding, "Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua," in *SSRN Scholarly Paper* (Rochester, NY: Social Science Research Network, 2020), https://doi.org/10.2139/ssrn.3691999.

73 McMillan, Volz, and Viswanatha, "China Is Stealing AI Secrets to Turbocharge Spying, U.S. Says"; Zach Dorfman, "How China's Tech Giants Like Alibaba, Tencent, and Baidu Aid Spy Agencies," Foreign Policy, December 23, 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

74 "TikTok Inc. and Bytedance Ltd. v. Merrick B. Garland, Amended Public Redacted Brief for the Respondent," September 16, 2024, 35–44, https://storage.courtlistener.com/recap/gov.uscourts.cadc.40861/gov.uscourts.cadc.40861.1208648321.0.pdf.

75 Finkelstein et al., "The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States"; see also "A Tik-Tok-Ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives," Network Contagion Research Institute, December 2023, https://networkcontagion.us/reports/12-21-23-a-tik-tok-in-timebomb-how-tiktoks-global-platform-anomalies-align-with-the-chinese-communist-partys-geostrategic-objectives/.

76 Stuart Lau, "China Bombards Taiwan with Fake News Ahead of Election," Politico, January 10, 2024, https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election/.

77 "Probable PRC 'Spamouflage' Campaign Targets Dozens of Canadian Members of Parliament in Disinformation Campaign," Global Affairs Canada, October 23, 2023, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2023-spamouflage.aspx?lang=eng.

78 "Press Release: Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election." The full indictment can be viewed here: https://www.justice.gov/opa/media/1371191/dl.

79 The tactics, techniques, and procedures of the IRGC and other actors affiliated with Iran involving AI are described here: "Staying Ahead of Threat Actors in the Age of AI," Microsoft Security, February 14, 2024, https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/; "Influence and Cyber Operations: An Update," Open AI, October 2024, 14–19, https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf.

80 "How to Protect against Iranian Targeting of Accounts Associated with National Political Organizations," Cybersecurity and Infrastructure Security Agency, October 8, 2024, https://www.cisa.gov/news-events/alerts/2024/10/08/cisa-and-fbi-release-fact-sheet-protecting-against-iranian-targeting-accounts-associated-national.

81 "Staying Ahead of Threat Actors in the Age of AI," Microsoft Security, February 14, 2024, https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

82 "Press Release: Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election," Office of Public Affairs, U.S. Department of Justice, September 27, 2024, https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us.

83 "Global Malicious Activity Targeting Elections Is Skyrocketing," Resecurity, February 12, 2024, https://www.resecurity.com/blog/article/global-malicious-activity-targeting-elections-is-skyrocketing; John Leyden, "Hacked Iraqi Voter Information Found for Sale Online," February 20, 2024, https://www.darkreading.com/endpoint-security/hacked-iraqi-voter-information-found-for-sale-online.

84 Amy Hawkins, "Huge Cybersecurity Leak Lifts Lid on World of China's Hackers for Hire," *The Guardian*, February 23, 2024, https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire.

85 "Cyber Threats to Democracy: A Special Report on Phishing and Online Scams Targeting the 2024 Election," Bolster AI, October 2024, https://bolster.ai/blog/phishing-online-scams-targeting-the-2024-election.

86 Belle Lin and Catherine Stupp, "Cyber Threats and the Election: What You Need to Know," *The Wall Street Journal*, November 1, 2024, https://www.wsj.com/articles/cyber-threats-and-the-election-what-you-need-to-know-c9dcaa7d; Arda Akartuna, "As the US Election Nears, AI Political Deepfake Scams Are Targeting Crypto Users," August 15, 2024, https://www.elliptic.co/blog/as-the-us-election-nears-ai-political-deepfake-scams-are-targeting-crypto-users.

87 Gilbert, "Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims."

88 "Country Summary: People's Republic of China," Canada's Foreign Interference Commission, 2024, https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Exhibits/CAN.SUM.000005.pdf; Aengus Bridgman et al., "Mis- and Disinformation during the 2021 Canadian Federal Election," Media Ecosystem Observatory, June 8, 2022, 60–64, https://osf.io/ubfmx.

89 Non-AI enabled disinformation emanating from the United States was observed in Canadian media ecosystems ahead of the 2021 election. See Bridgman et al., "Mis- and Disinformation during the 2021 Canadian Federal Election", Media Ecosystem Observatory, June 8, 2022, 60–64, https://osf.io/preprints/osf/ubfmx_v1.

90 https://www.cyber.gc.ca/en/guidance/cyber-threats-elections

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

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

93 https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html

94 https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2023-2024#9-1-1

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

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

97 https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions.html

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

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

100 https://www.canada.ca/en/campaign/online-disinformation.html

101 https://www.getcybersafe.gc.ca/en/secure-your-accounts/social-media

102 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

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

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

105 https://www.getcybersafe.gc.ca/en