Trellix

TLP:GREEN

Threat Landscape Report

Threats to Canadian Elections

UNCLASSIFIED

Threat Intelligence Group
threatintelligenceservices@trellix.com

"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."[1]

The above quote comes from the Communications Security Establishment's publication on the 'Cyber Threats to Canada's Democratic Process' and highlights the real and imminent threats we face going to the polls this year. The US had similar concerns for the 2024 Presidential election and we can learn a lot from studying what happened to them.

2024 US Elections

The 2024 US elections faced significant cybersecurity and information threats, particularly from state-sponsored actors like Russia, China, and Iran, who targeted vulnerabilities in voting infrastructure to disrupt processes and erode trust. Foreign influence networks, including China's *Spamouflage Dragon*, were deploying disinformation campaigns on social media to mislead voters. Foreign campaigns, such as Russia's *Good Old USA Project* and *Operation Overload* and Iran's *Storm-2035*, employed AI-driven narratives and fake news sites to target specific US voter groups with polarizing content on social and political issues.

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

Spamouflage Dragon

This influence operation, linked to China's Ministry of Public Security, intensified its efforts last fall, targeting US elections. They employed fake social media accounts impersonating Americans and used them to spread divisive content and attack US candidates. These efforts aimed to undermine confidence in democratic institutions, polarize the electorate, and manipulate narratives that increase societal divisions.

US company Graphika has monitored 'Spamouflage' since 2019 and has seen it active across more than 40 online platforms, using accounts to promote pro-China and anti-Western narratives.[2]

Image 1, Album cover of Good Old US song
Source: https://digital.library.illinois.edu

GoodOld USA Project

The Russian Social Design Agency ran a campaign to sway the 2024 US presidential election in Donald Trump's favor, targeting minorities, swing-state residents, online gamers, Reddit users, and image board communities like 4chan. Key tactics included creating fake websites that impersonate major media outlets, using AI-generated content to spread pro-Russian narratives, and establishing supportive community groups on social media. The campaign also mixes pro-Trump messaging with viral videos on YouTube to increase visibility. Its narratives exploit societal divisions, employing racist stereotypes and far-right conspiracies, and promote "traditional values" to resonate with specific voter groups.[3]

Operation Overload

Operation Overload, also known as Matryoshka and Storm-1679, is a Russia-aligned influence campaign targeting the 2024 US presidential election to manipulate public opinion and incite discord. It focuses on media organizations, fact-checkers, and researchers, using tactics such as impersonating trusted news outlets to create seemingly legitimate content, generating AI-driven voiceovers, and overwhelming media resources with spam and fake fact-checking leads. This campaign spreads divisive narratives about Ukrainian refugees, political violence, and election integrity, including discrediting mail-in voting, through coordinated social media activity and automated bots. By amplifying false narratives and laundering

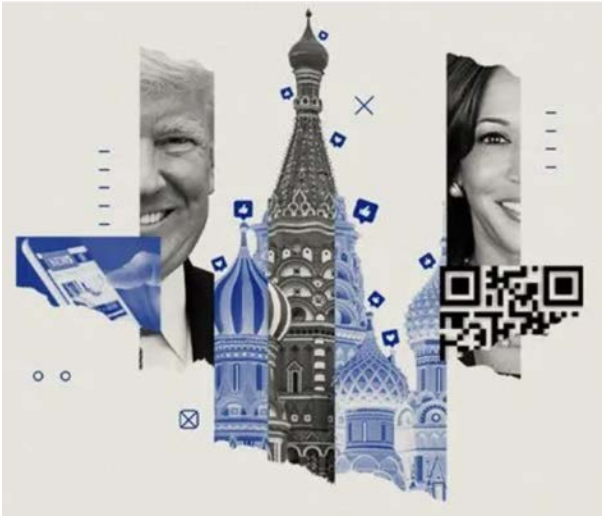

Image 2, Cover page of Operation Overload Impersonates Media to Influence 2024 US Election
Source: recordedfuture.com

[2] https://www.institut-ega.org/l/china-linked-spamouflage-network-and-the-us-november-election/
[3] https://www.justice.gov/opa/media/1366201/dl

disinformation, Operation Overload seeks to exploit societal divisions, disrupt the electoral process, and erode trust in democratic institutions.[4]

Storm-2035 (Iran)

The Iranian network Storm-2035 operates four websites posing as news outlets to engage US voters with polarizing content on issues such as the presidential candidates, LGBTQ rights, and the Israel-Hamas conflict. Part of a broader campaign dating back to 2020, this network includes over a dozen covert sites targeting audiences in multiple languages, including English, French, Spanish, and Arabic. Storm-2035 directs its messaging to both ends of the US political spectrum, particularly liberal audiences, using tactics like plagiarizing content from US sources with AI-enabled tools and SEO plugins to obscure sources and boost site traffic. The campaign aims to amplify social division on key political and social issues.[5]

Image 3, image from 'Iran steps into US election 2024 with cyber-enabled influence operations' Source: Microsoft.com

While Russia, China, and Iran are recognized as key adversaries actively involved in cyber operations targeting elections globally, the majority of this cyber threat activity is unattributed. The '*Cyber Threats to Canada's Democratic Process: July 2021 update*', noted that 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. They 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.

2025 Canadian Federal and Provincial Elections

Same Techniques, Different Country

The Canadian Centre for Cyber Security (CCCS)'s National Cyber Threat Assessment 2023-2024 identifies cyber threat actors' attempts to influence Canadians and diminish trust in online spaces as a primary concern for the country.[6] They note that misinformation, disinformation, and malinformation (MDM) is used to pollute the online information space by spreading false and potentially harmful information, making it difficult for Canadians to separate truth from falsehoods and that these activities are often centred around events such as elections.

[4] https://www.recordedfuture.com/research/operation-overload-impersonates-media-influence-2024-us-election

[5] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf

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

Figure 1, Image of definitions of misinformation, disinformation, and malinformation
Source: National Cyber Threat Assessment 2023-2024, cyber.gc.ca

CCCS also noted that they see an increased willingness of nation states to use MDM to advance their geopolitical interests. This, along with advancements in AI tooling, is making it easier for malicious actors to create convincing disinformation, and automate influence operations, further complicating the electoral landscape.

Indeed, the Security Intelligence Threats to Elections Task Force, a working group with members from the Canadian Security Intelligence Service, The Communications Security Establishment, Global Affairs Canada and The Royal Canadian Mounted Police, has already found evidence of MDM directed at current Liberal leadership candidate Chrystia Freeland via the WeChat social media platform and believed to be Chinese state sponsored.[7]

Image 4, Source: Chrystia Freeland THE CANADIAN PRESS/Frank Gunn, WeChat - iphoneincanada.ca

While we have focused on threats related to geopolitical motivations we shouldn't overlook the financial ones.

Cybercriminal Activity

At the end of last year, while threat hunting post US election, analysts in Trellix's Advanced Research Group found evidence of cybercriminals using election related typosquatted domains in crypto currency scams.[8]

7 https://www.thecanadianpressnews.ca/national/federal-unit-uncovers-malicious-effort-tied-to-china-aimed-at-chrystia-freeland/article_21267d8d-0d50-54d5-ae54-b5da02f4bed9.html

8 https://www.trellix.com/blogs/research/safeguarding-election-integrity-threat-hunting-for-the-us-elections/

The first domain, trrump[.]com, loaded a single image showing a website with a Bitcoin QR code and had an on-click event connected to it, where it would prompt the user to share it on Twitter. With the help of Mandiant, additional insight was gained into this campaign, as it was spread via multiple social media platforms, including YouTube.

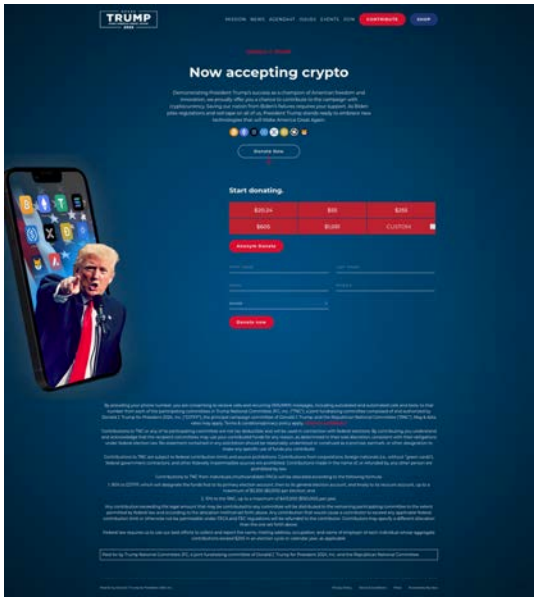

Image 5, screenshot of the doonaldjtrump[.]com webpage

The second site (doonaldjtrump[.]com, note the “oo” in the beginning) was set up as a donation portal for the Trump campaign.

We should expect the same behaviour from cybercriminals for the upcoming elections in Canada and educate users on how to protect themselves against such scams. It is interesting to note that Elections Canada themselves recommend prohibiting contributions in cryptocurrency or untraceable instruments, in ‘Key Recommendations Protecting Against Threats to the Electoral Process’ published in Nov 2024.[9] Such a move would likely impact the cybercriminal’s motivation to implement these scams as traceable forms of currency complicate these campaigns and raise the risk of getting caught or not getting paid.

Moving Forward

The Canadian elections scheduled this year will face multifaceted cyber threats. This includes disinformation campaigns from foreign influence networks, misinformation tactics to manipulate public perception and behavior, and cybercriminal campaigns leveraging the event for their purposes. A coordinated response involving government, social media platforms, and public awareness initiatives is essential to mitigate these threats and protect the integrity of the electoral process.

Image 6, Credit: https://capacoa.ca/en/healthy-sector/arts-promotion/federal-election/