PROTECTED B

CANADIAN CENTRE FOR CYBER SECURITY

2023 Update: Cyber Threats to Canada's Democratic Process (TDP4)

Overview

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

PROTECTED B

What is TDP4: Cyber Threats to Canada's Democratic Process?

- Fourth iteration of "Cyber Threats to Canada's Democratic Process"
  - Previous versions in 2021, 2019 and 2017
  - Public document
- Dataset that includes all national level elections globally since 2015
  - Open source and classified data
  - Informs Global trends section
- Evaluate the threat to Canada's Democratic Process
  - Implications for Canada section

PROTECTED B

TDP4: Outline

1. **Introduction**
2. **Key Findings:** Global Trends
3. **Cyber Threats to Elections**
4. **Generative AI Tec**
5. **Imp**

2. Key Findings and 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 global national elections has increased from 2015 to 2022.

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

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

- In 2022, 85% of cyber threat activity targeting elections was unattributed

Trend 4: Online disinformation is now ubiquitous in elections globally and generative AI is increasingly used to influence elections

- Between 2021 and spring 2023 all national elections (146 in total) were subject to online disinformation geared towards influencing voters and the election

PROTECTED B

3. Cyber Threats to Elections

- The cyber threat landscape against election infrastructure is growing: Cyber threat activity compromising any of these three stages of the electoral process can jeopardize the integrity of an election
  - Online Voter Registration
  - Casting the Ballot
  - Vote Tally and the Paper Trail

- Foreign adversaries will use cyber threat activity to influence elections by creating, circulating, and/or amplifying disinformation in online public spaces. Types 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
  - Defacing a political party's website with disinformation

PROTECTED B

4. Generative AI threatens democratic processes

- Generative AI can produce various types of content, including:
  - Text, images, audio, and video (sometimes referred to as "deepfakes") can be used in influence campaigns to covertly manipulate information online, and as a result, influence voter opinions and behaviours
  - Deepfake videos of political figures risk deceiving voters and creating further political polarization
  - Generative AI will almost certainly be increasingly used to further automate and augment social botnet functions in the next two years

Deepfake Videos

Generative AI is used to reverse engineer real audio-video of a target person to convincingly mimic their image and auditory style of speech, producing a video of events that never actually occurred

Social Botnet

A cluster of fake profiles operated by software robots that can control online social network accounts and mimic the actions of real users; Social botnets can influence and/or misrepresent popular opinion

PROTECTED B

5. Implications for Canada

- An increase in the use of generative AI to create disinformation
  - **Implications for Canada:** Disinformation about the next federal elections will almost certainly be found online and foreign adversaries will likely use generative AI to target Canada's elections in the next two years (e.g. deepfakes, amplified social botnets)
    - In the long term, we assess that this could lead Canadians to distrust online information about politicians or elections
- Increased targeting of democratic processes using cyber
  - **Implications for Canada:** We assess cyber incidents are also more likely to happen in Canada's next federal elections than they have been in the past
- Heightened bilateral tensions can lead to cyber threat actors targeting elections
  - **Implication for Canada:** We assess that increased tensions or antagonism with countries such as China, Russia, [redacted] are very likely to result in cyber threat actors targeting Canada's democratic processes or disrupting Canada's online information ecosystem ahead of a national election.
- An increase in unattributed cyber threat activity
  - **Implications for Canada:** It will become increasingly difficult for Canada to attribute cyber threat activity targeting its democratic processes
- Election infrastructure, online voting and paper ballots
  - **Implications for Canada:** In Canada, technology is used throughout the election process and can be an important part of making elections efficient and accurate; however, not having physical paper ballots presents some risks

PROTECTED B

CCCS related products

- Cyber threat activity continues to be used to target democratic processes globally and the Government of Canada has put in place several mechanisms and protocols to safeguard the integrity of Canada's elections
- The Cyber Centre provides cyber security advice and guidance to Canadians, please see below some of CCCS products relating to "Cyber Threats to Democratic Processes 4":
  - Cyber Security Guide for Campaign Teams
  - Cyber Security Guidance for Elections Authorities
  - Cyber Security Playbook for Elections Authorities
  - Cyber security advice for political candidates
  - Fact sheet for Canadian voters: Online influence activities
  - 2023-2024 National Cyber Threat Assessment
  - How to identify misinformation, disinformation, and malinformation
  - Security considerations for electronic poll book systems
  - Generative artificial intelligence (AI)
- Other CSE resources include:
  - Get Cyber Safe

PROTECTED B

Communications plan

- Media, political and public interest is expected to be high
  - Pre-publication comms consults and planning with Elections Canada, PCO, GAC, PS, CSIS
- Communications activities will:
  - Inform Canadians of key findings and trends
  - Explain this assessment is specific to cyber threats and does not address other elements of foreign interference
  - Reinforce that this assessment is a data-driven non-political and non-partisan assessment of cyber threats to Canada's democratic process
- A high-profile approach is recommended
  - Media and stakeholder briefings
  - Chief of CSE as lead spokesperson
  - Seek out supplementary opportunities for the Chief, CSE and Head, Cyber Centre to amplify messaging
- Alternate Approach
  - A digital only release via the Cyber Centre web site, GC newsroom and CSE social media channels, no advance embargo release.
  - Responsive media relations only