UNCLASSIFIED/ NON CLASSIFIÉ

CANADIAN CENTRE FOR CYBER SECURITY

Cyber Threats to Canada's Democratic Process

Presentation to the

Advisory Committee for Political Parties (ACPP)

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

UNCLASSIFIED/ NON CLASSIFIÉ

Cyber Threats to Canada's Democratic Process

- The Cyber Centre is working on the fourth iteration of "Cyber Threats to Canada's Democratic Process"
  - Public document – Planned release in Fall 2023
- 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

UNCLASSIFIED/ NON CLASSIFIÉ

TDP 2021 – Key Considerations

- Why Target Canada's Democratic Process?
  - Canada takes an active role in the international community, participating in key multilateral forums.
- Effects of Cyber Activity Against Democratic Processes
- Impacts of the COVID-19 Pandemic on Democratic Processes
  - Overall, the changes to electoral procedures due to COVID-19 appear to have had limited impacts on the cyber threat to elections.

SHORT-TERM GOALS

- Call into question legitimacy of election process
- Amplify false or polarizing discourse
- Reduce voter turnout

MEDIUM-TERM GOALS

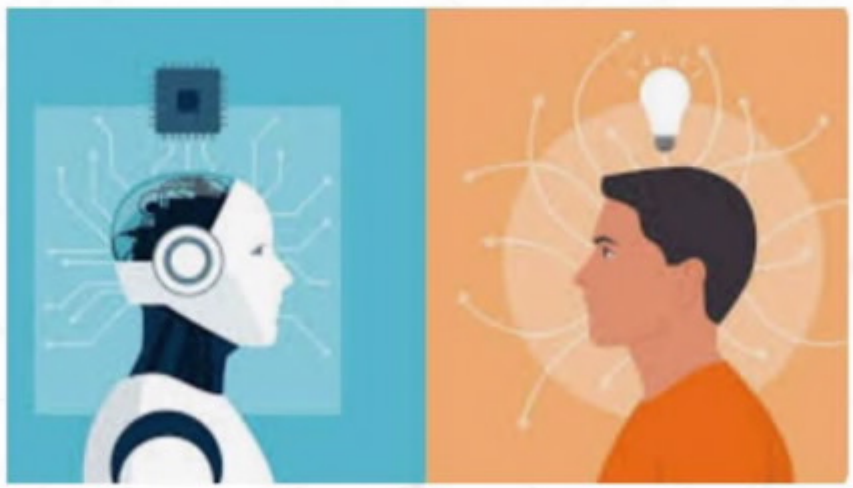
- Polarize political discourse
- Weaken confidence in leaders

LONG-TERM GOALS

- Reduce confidence in democracy
- Promote foreign economic, ideological, or military interests
- Create divisions in international alliances

AI and disinformation

- Biggest change from former TDP's is the introduction of AI
- "AI" = Machine Learning Enabled technology



Global Trends: Initial Key Findings

- **Trend 1: Targeting of democratic processes has increased**
  - Since 2021 we observe that the proportion of elections targeted increased from 23% in 2021 to 26% in 2022.
- **Trend 2: A small number of countries continue to be responsible for most of the attributed cyber threat activity targeting foreign elections**
- **Trend 3: The majority of cyber threat activity targeting elections is unattributed**
  - Since 2021, more than half of the perpetrators of cyber threat activity targeting national elections were unknown.
  - The number one type of incident = Denial of Access or Distortion of Election Commission Website(s)
- **Trend 4: Online disinformation is now ubiquitous in all national level elections globally and generative AI is increasingly being used to influence elections**
  - Between 2021 and spring 2023 all national elections (146 in total) were subject to online disinformation
  - Since 2021, we have detected an increase in synthetic content being produced relating to national level elections, almost certainly related to the increased accessibility of many of these technologies.

Traditional Cyber Threats to Elections

Two main themes:

- **Cyber Threat Activity Against Election CI**
  - How Cyber Threat Actors target election systems and infrastructure.
  - Ex: DDoS on Election Commission website, Hacking into an electronic voter database, etc.

- **Cyber Enabled Influence Campaigns**
  - How Cyber Threat Actors try to influence the electorate through influence campaigns that are cyber-enabled.
  - E.g.: “hack-and-leak”, social media account hijacking.

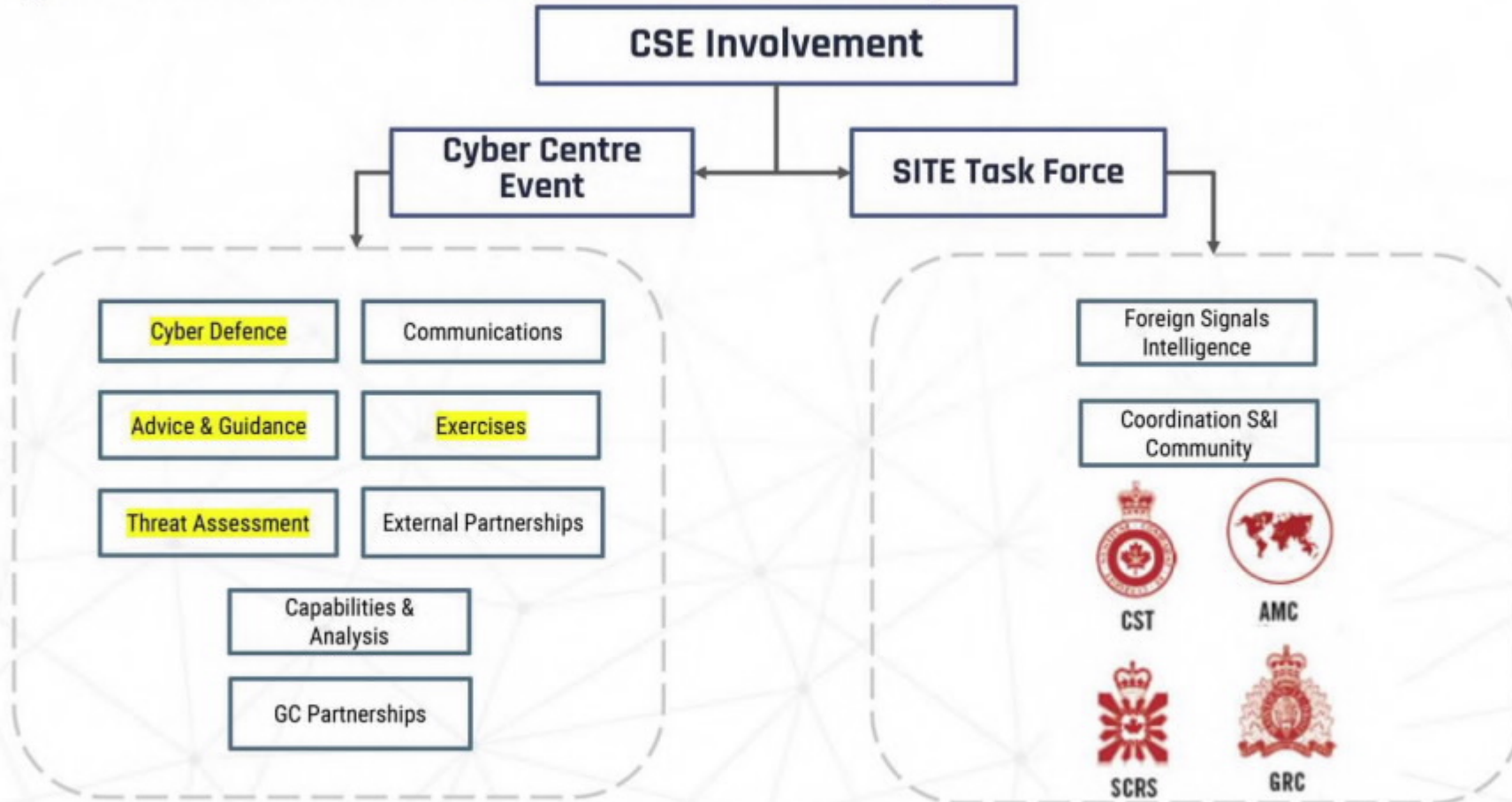
UNCLASSIFIED/ NON CLASSIFIÉ

AI Technology and Disinformation

AI Technologies: Deepfake videos, fake profiles/GAN imaging and text generators (ChatGPT)

- How Cyber Threat Actors try to influence the electorate using AI
- Deepfake detection models; inaccuracies in detecting deepfakes and generated text

The Cyber Centre's Election Security



Cyber Centre Services

- Hotline
  - Actions after dissolution of the House of Commons
- Subscription Services
  - Cyber Alerts
  - Cyber Flashes
  - Weekly Technical Report
- Reporting and Analysis Services
  - Malware.gc.ca
  - Incident Reporting Portal
  - Partner: RCMP Fraud Reporting portal

Register via: *contact@cyber.gc.ca*

UNCLASSIFIED/ NON CLASSIFIÉ

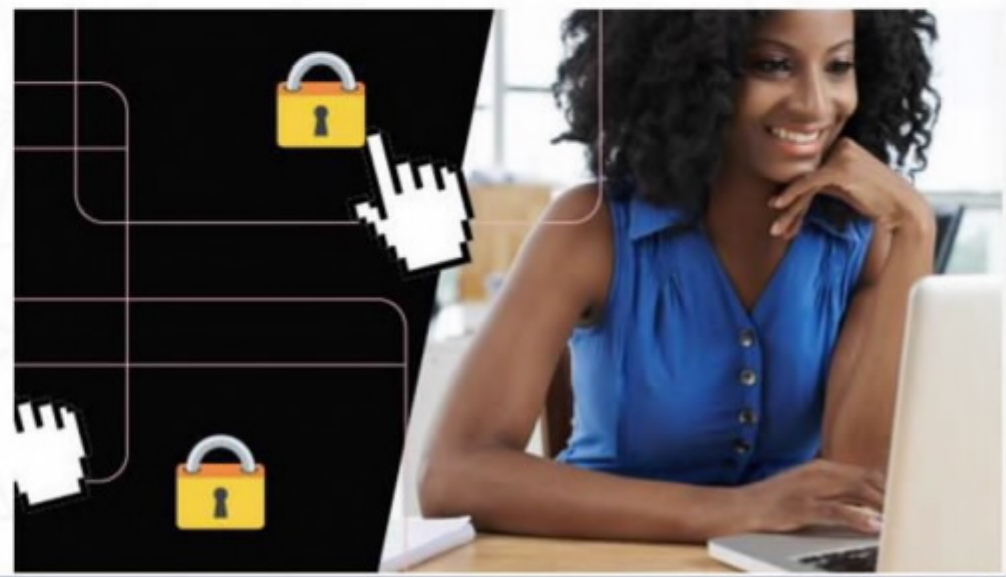
Targeting of Senior Officials

- Almost certainly routinely targeted by foreign intelligence services
- Personal accounts and devices of senior officials present an alternative to hardened accounts and services
- State-sponsored actors may be particularly aggressive during periods of transition or heightened tension
- Cybercrime and hacktivism are assessed to be considerably less damaging to Canada's strategic position than sophisticated cyber threat activity

UNCLASSIFIED/ NON CLASSIFIÉ

Protecting One's Online Presence – Best Practices

- Utilize a PIN, complex password or passphrases to protect yourself
  - Passphrases are a memorized phrase consisting of mixed words with or without spaces
- Keep private information private including your personal information, informative pictures, geotagged photos and banking or financial information private
- Use multi-factor authentication (MFA)
- Review your privacy settings often to control who can see what
- Phishing, spear-phishing and whaling
  - Stop, review, and reach out to the sender
- Protect your website



UNCLASSIFIED/ NON CLASSIFIÉ

Discussion