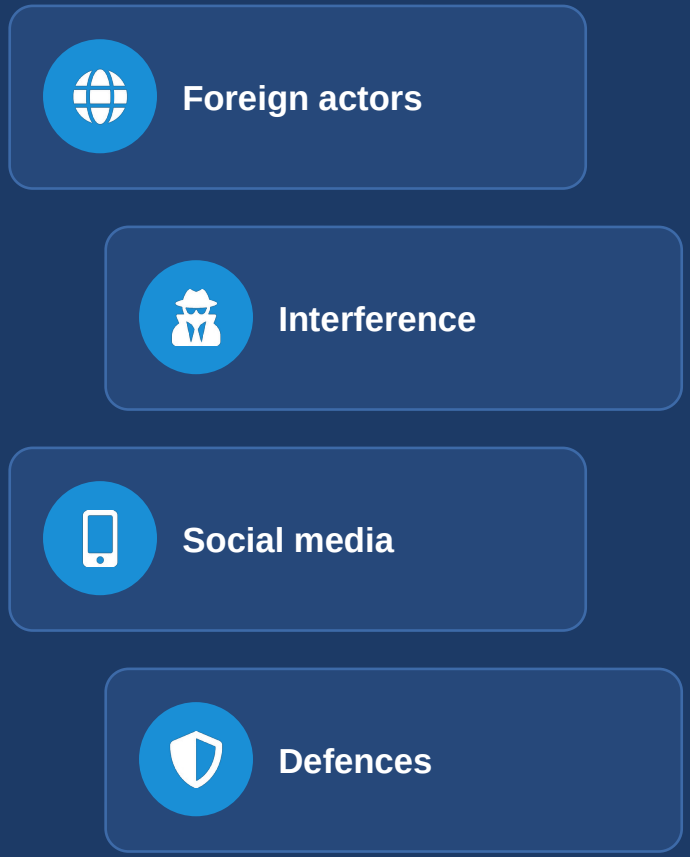
CHV2O Democratic Values in Action, Lesson 3

Foreign Interference and Disinformation

Protecting democratic debate



Today's goals

We are learning…

- The difference between foreign influence and foreign interference.
- Methods foreign actors use to interfere, including on social media.
- How Canada and citizens defend democracy against interference.

I can…

- Explain the difference between open influence and interference.
- Identify methods of foreign interference.
- Name institutions that defend Canada's democracy and what they do.
- Judge the credibility of a suspicious election post.

Today's plan

Time	What we're doing	You will…
0–8 min	**Hook**	Vote and explain
8–25 min	**Methods and defences**	Take notes
25–33 min	**Model**	Follow
33–45 min	**Methods and Defences**	Sort scenarios (page 1)
45–67 min	**Case File**	Analyse the case (page 2)
67–75 min	**Check and exit**	Answer

Warm-up: influence or interference?

- A foreign ambassador gives a public speech praising a trade deal.
- Fake accounts, secretly run from abroad, spread false claims about a candidate.
- A foreign news channel openly broadcasts its country's view of events.
- Someone in Canada is warned their relatives abroad will suffer if they speak out.

Big idea

Countries try to influence each other openly all the time. Foreign interference is different: it is secret, deceptive or threatening, and it targets voters, communities and debate in Canada. Knowing the methods is the best defence.

Words to know

foreign influence	Open efforts by other countries to shape opinions or decisions. *Diplomacy, public speeches, international news.*
foreign interference	Secret, deceptive or threatening activity by or for a foreign state. *Harmful to Canada's interests and democracy.*
inauthentic account	A fake or automated account pretending to be a real person. *Often used in large networks (bots).*
transnational repression	A foreign state threatening or harassing people living in other countries. *Often aimed at diaspora communities.*

Methods of foreign interference



Disinformation

False stories, fake accounts and AI-made images or audio, spread to divide people or mislead voters.



Covert funding

Secret money passed to groups or campaigns to sway decisions.



Intimidation

Threats against people in diaspora communities or their families abroad.



Cyber attacks

Hacking election systems, campaigns or officials, sometimes to leak altered files.

Who defends Canada's democracy?

Defender	What they do
Elections Canada	Runs federal elections; gives official voting information
Commissioner of Canada Elections	Enforces election law, including bans on foreign donations
CSIS	Investigates threats to security; can warn people who are targeted
Canadian Centre for Cyber Security	Protects government and election systems from cyber attacks
Platforms and journalists	Remove fake networks; fact-check and report
Citizens	Check before sharing; report threats; vote with good information

Canada's public inquiry

From 2023 to 2025, a federal Public Inquiry into Foreign Interference examined attempts to interfere in the 2019 and 2021 federal elections and in Canada's democratic institutions.

Its final report, released in early 2025, found that foreign interference is a real threat and recommended stronger defences, better information for the public, and more protection for communities that are targeted.

Model: checking a fake voting post

Task: “URGENT from Elections Canada: this year you can vote by text! Text your choice to 55555 before Election Day.” Credible?

Stop: the post uses urgency to rush me, and it asks me to do something unusual. Investigate: the account is two days old and only copies the Elections Canada logo. Find other coverage: Elections Canada's official website lists the real ways to vote (on election day, at advance polls, by mail or at an Elections Canada office), and none is by text. Trace: no official source says this. Judgement: this is disinformation meant to stop people from voting. I won't share it, and I'll report it.

Why it works

- Uses all four moves.
- Checks the official source.
- Names the purpose.
- Says what to do next.

Guided practice: Methods and Defences

On page 1, with a partner:

1. Read the four methods at the top.
2. Label each scenario: influence, method or defence.
3. Name the method where it applies.
4. Explain what makes scenario 1 different from 2.

Your turn: Case File

On page 2, on your own:

1. Read the four weeks of the invented case.
2. Identify the method used in weeks 1 to 3.
3. Explain which democratic value each method harms.
4. Judge the responses, and advise a voter.

Quick check

- What makes foreign interference different from open influence?
- Name three methods of foreign interference.
- What does the Canadian Centre for Cyber Security do?
- Why is the “vote by text” post clearly false?

Check yourself

Be honest. This helps you choose what to work on next.

Success criteria	Not yet	Almost	Got it
I can explain the difference between open influence and interference.			
I can identify methods of foreign interference.			
I can name institutions that defend Canada's democracy and what they do.			
I can judge the credibility of a suspicious election post.			

Exit ticket

1 In one sentence: what is foreign interference?

2 Which defence against interference matters most? Why?

3 One thing you'll check before sharing election news.

Next class: Parties and the Political Compass.

Teacher reveal

Interference: answers

Open influence (1): The ambassador speaks publicly and openly, so people know who is speaking and why.

Disinformation (2): A secret network of fake accounts spreads false claims about a candidate.

Intimidation (3): Threats against relatives abroad aim to silence a person living in Canada.

Cyber attack (4), covert funding (5): Hacked and altered emails; secret foreign money passed to a local group.

Defences (6, 7, 8): A platform removes fake accounts; CSIS warns a target; a student checks before sharing.

Case, methods: Disinformation and fake accounts (week 1); intimidation of community members (week 2); hack-and-leak cyber attack (week 3).

Case, responses: CSIS briefing, platform removals, a fact-check and police contact. Strong answers judge which worked fastest and what citizens could add.