Foreign Influence Activity Binning Models:

The FBI/DOJ "5 Buckets"

1. Cyber operations targeting elections infrastructure (incl. critical infrastructure)
2. Cyber operations targeting political/campaign infrastructure (parties, politicians)
3. Covert influence operations to assist or harm political organizations, campaigns, and public officials
   - covert financial, logistical, or other campaign support
   - social media "bots" to amplify messaging
   - stolen info illicitly acquired through illegal cyber operations targeting government institutions, media, political organizations/campaigns
4. Covert influence operations, including disinformation operations, to influence public opinion and sow division
   - create/operate social media pages and other forums to attract US audiences and spread disinformation
   - target discrete populations based on political and demographic characteristics
   - mobilize Americans to sign online petitions and join issue-related rallies
5. Overt influence efforts
   - use foreign media outlets or lobbyists to reach policymakers or public and spread divisive narratives and political positions
   - may not be illegal

Variant of "5 Buckets"

1. Cyber operations targeting elections infrastructure
2. Cyber operations targeting political/campaign infrastructure (parties, politicians)
3. Covert political influence operations
   - primary targets: primarily politicians, political parties, campaigns, government officials
   - techniques:
     - covert financial support, traditional espionage, disinformation (e.g. smearing campaign via social media)
     - exclude: cyber operations (e.g. phishing campaign against politician)
4. Covert public influence operations
   - primary targets: public, discrete populations
   - techniques:
     - disinformation operations, traditional espionage (e.g. state agents influencing university student unions), etc
     - exclude: cyber operations
5. Overt influence efforts

CCCS Categories of Threats

1. Threats against elections
2. Threats against politicians and political parties
3. Threats against traditional and social media

Stakeholder-Centric "4 Hods"

1. Threats against elections infrastructure
2. Threats against politicians, political parties and campaigns
3. Threats against influential sectors – news outlets, social media companies, journalists, lobbyists, think tanks, academia etc
4. Threats against general public and local diaspora

	Scenarios
HOD 1 Cyber ops on infrastructure	▪ The National Register of Electors server was hacked and voter information was stolen by possible organized crime entity and sold on various e-Crime sites. State-sponsored cyber actors are likely to use the information for attack campaigns.
HOD 2 Cyber ops against political parties/persons	▪ APT29 leaking disclosures of sensitive information of a Canadian electoral candidate via a successful phishing campaign.
HOD 3 Covert political influence	▪ [redacted] state actor using bots/trolls to promote one Canadian political party over another on social media. ▪ False-front hacktivist group DCLeaks and Guccifer 2.0 initiated direct, private communication with Canadian journalists via email and private messaging with fake documents of Canadian political candidates.
HOD 4 Covert public influence	▪ Ukraine-based actor seeding particular news stories on fraudulent news platform appearing to originate from Canada. ▪ Chinese government using Chinese student groups at Canadian universities to sway opinions of local student population wrt Canadian political parties.
HOD 5 Overt influence	▪ China using closed social media groups (e.g. WeChat) in Canada to influence Canadian electorate. ▪ Suspected foreign state-supported agents bought political ads on Facebook to target specific populations with propaganda during the Canadian election campaign.