Centre for International and Defence Policy
POLICY BRIEF

July 2021 Volume 7, Issue 3

Securing Elections: A Comparative Assessment of Canada's Response to Foreign Interference

Jean-Nicolas Bordeleau
Royal Military College of Canada

Security Threats to Elections

Attempts by foreign states to influence the process and results of national elections have plagued democracies around the world. A report by Communication Security Establishment Canada (CSEC) indicates that a quarter of the world's electoral contests held in 2018 were targeted by cyber threat activities.[1] Canada is not immune to these security threats to elections. Recent Canadian federal elections have been the target of several foreign interventions. In 2015, Russia used bots and proxies to launch cyber-attacks and disinformation campaigns aimed at delegitimizing candidates and misleading voters. [2] During the same election, Chinese-owned corporations contributed large sums of money to political campaigns across the country.[3] Acknowledging the mounting threat of election interference in Canada, this policy brief assesses the government's efforts to secure the electoral process. This assessment will compare Canadian election security policies to those of members of the Five Eyes intelligence alliance (FVEY) who share Westminster parliamentary traditions: the United Kingdom, Australia, and New Zealand.

Security threats to the Canadian electoral process are alive and well. Election interference by foreign entities is serious and poses a significant threat to Canada's democratic institutions. Through cyber-attacks and disinformation campaigns, interveners can damage the reputation of leaders and undermine the trust voters have in the electoral process.[4] As a pillar of democracy, trust is essential in maintaining a stable electoral process and transparent government. Protecting the integrity of the electoral process is therefore crucial to preventing civil conflicts, sustaining legitimacy, and promoting political participation.[5] Indeed, trivializing the menace of electoral interventions puts in jeopardy the fundamentals of democratic order and responsible government.

This comparative policy analysis highlights shortcomings in Canada's election safeguarding plan and proposes new policy directives that ought to be considered by the Canadian government. Implementing these security strategies will place Canada in a better position to defend its democratic institutions and uphold the values that define responsible government.

What Makes an Effective Election Security Policy?

In order to compare the election security policies of Australia, Canada, New Zealand, and the UK, it is necessary to establish a framework upon which to base the comparative assessment. In other words, what factors make an election security plan effective? The framework used in this policy brief focuses on three key components to determine whether an election security policy is indeed effective:

1. Is the policy multidimensional and cross-departmental?
2. Does the policy establish clear consequences for infringement?
3. Is there an implementation unit and/or policy oversight?

The first conceptual factor is concerned with the dimensionality and administration of the policy. To be effective, an election security policy needs to tackle complex and multi-faceted challenges. That is why one of

the key factors to evaluate the effectiveness of a security policy is whether or not it is multidimensional (i.e., whether it attacks the policy issue from multiple angles). Public policy scholars also highlight the need for a whole-of-government approach to security policy implementation.[6] In other words, a successful election security plan includes cross-departmental planning, coordination, and collaboration.

The second criterion within the framework is the presence of clear consequences in the event of infringement. In policy terms, this means that new legislation enacted under the election security plan needs to have actionable enforcement mechanisms. If a policy does not have such mechanisms, the legislation is unenforceable and completely obsolete. For example, if a new law prohibits a specific action but does not include any punishment, then there is nothing preventing individuals from engaging in that action. That is why new policy plans need to include enforceable punishments to support the policies and legislation.

The last factor relates to the implementation of the policy. In order to be effective, an election security policy plan needs to have an ongoing oversight process which serves as both an accountability and assessment tool. By overseeing the implementation of the policy, government agencies can provide necessary recommendations and adjustments to improve the policy. [7] This proves especially important in a security setting, where policies must continually adapt to new problems and challenges.

Canada's Election Security Plan

The Government of Canada released its election security plan in early 2019, only months before a federal election. Their plan is divided into four areas of action: enhancing citizen preparedness, improving organizational readiness, combatting foreign interference, and expecting social media platforms to act.[8] Each pillar has its own focal point, introducing a specific set of security policies, executive actions, or legislative amendments.

The first pillar—enhancing citizen preparedness—focuses on community outreach and voter information campaigns in order to limit the impact of foreign interference on Canadian citizens. In line with this area of action, the government introduced the Critical Election Incident Public Protocol (CEIPP). This new document highlights the procedure to be taken by key government stakeholders when faced with an electoral integrity incident. Most notably, the CEIPP puts in place a threshold for when the general public should be informed of a foreign electoral intervention.[9] In the event that a threat to electoral integrity is deemed considerable, a public announcement will notify the population of the incident and propose steps that can be taken for Canadians to limit the consequences of said incident.

The election security plan's second area of action is improving organizational readiness. This pillar is primarily concerned with providing technical and security advice to common targets of election interference: political parties, campaign teams, and election authorities. As part of this pillar, the Canadian Centre for Cyber Security issued two publications: the *Cyber Security Guidance for Election Authorities* and the *Cyber Security Guide for Campaign Teams*. These comprehensive guides are made available to all election actors and provide essential information on securing data and technology. The guides also include a framework on how organizations can provide cyber security training to their staff. Under the organizational readiness pillar, intelligence and national security agenices are also required to provide classified "threat brefings" to political party leadership.[10]

Combatting foreign interference, the third pillar in Canada's election security plan, is operationalized through the Security and Intelligence Threats to Elections (SITE) Task Force. This task force includes members from the Canadian Security Intelligence Service (CSIS), CSEC, the Royal Canadian Mounted Police (RCMP), as well as Global Affairs Canada (GAC). This multi-agency team monitors election security threats, protects government systems from foreign attacks, and is tasked to "detect and disrupt attempted foreign interference activity."[11] The means through which these agencies can defend the integrity of the electoral process are highlighted in Bill C-76, the *Elections Modernization Act*. This legislation, which received Royal Assent in late 2018, includes provisions that prohibit the intentional use and dissemination of false statements along with restrictions on funding from foreign sources.[12] However, it does not include clear guidelines to punish unlawful financing activities.

The plan's last area of action—expecting social media platforms to act—is focused on handling the growing problem of disinformation on the web. The title of the pillar says it all: the government expects social media platforms to enhance their mis- and disinformation guidelines. This portion of the election security plan serves as a call for corporations running digital platforms to take more concrete steps in regulating what information can and cannot be shared online. Under Bill C-76 and the *Canada Declaration on Electoral Integrity Online*, social media companies are required to keep a registry of all political and election-related ads. Doing so will facilitate government and independent oversight and make place for greater transparency between social media platforms and the general public.

Election Security Across the Five Eyes

The UK government's response to security threats to elections has been far less extensive than in Canada. Despite growing evidence of foreign interference in the Brexit referendum, the British government has not presented a single policy to protect the integrity of its elections and referenda.13 This inaction has resulted in several reports of foreign interference becoming "the new normal" in UK politics. 14 Prime Minster Boris Johnson has even been sued by members of Parliament over his failure to ensure free and fair elections.15 It is clear that there is little Canada can learn from the UK when it comes to election security policies. However, seeing as the UK government's inaction is both divisive and damaging to its democratic process, it is clear that taking no action is simply not an option.

Australia's response to election interference has been far more robust and in-depth than that of the UK. In an attempt to completely eliminate the threat of electoral interventions the Australian government introduced a series of laws which defines numerous interference activities as criminal. It also imposes severe prison sentences for individuals or groups found to break the laws. Unlike the Canadian and British response, Australia has not been afraid to introduce criminal consequences for those who engage in activities which may affect the integrity of its democratic institutions (especially elections).16 The new laws have already been enforced and led to the arrest of the leader of a Chinese community organization with ties to Chinese intelligence services.17

In addition to its legislative efforts, the Australian government has created the Electoral Integrity Assurance Taskforce (EIAT). Much like the Canadian SITE Task Force, the EIAT is a multi-agency team with the specific task of coordinating the defence of elections from foreign threats. However, the EIAT is more extensive than its Canadian counterpart. In total, the EIAT is composed of personel from over eight governmental agencies and departments. One of its most important tools is the Foreign Influence Transparency Scheme Public Register. Whereas the Canadian government has the full liberty to decide whether or not to disclose an interference incident, the Australian EIAT registers every known foreign election interference activity and renders that information publicly available through its Transparency Register website.

The New Zealand government's response to electoral interference and threats to electoral integrity has been relatively similar to that of Canada. By passing the Electoral (Integrity) Amendment Bill, the New Zealand legislature created new campaign finance guidelines prohibiting foreign donations and setting clear reprimands to those who do not abide.18 While these legislative changes closely resemble what has been seen in Australia and Canada, New Zealand has decided to adopt a unique secretive posture in its fight against security threats to elections. Like Australia and Canada, New Zealand has a national security team responsible for election security. However, contrary to Canada and Australia, the New Zealand team operates in total secrecy and does not reveal any information regarding its operations or the election interference activities it monitors.19 This is in stark contrast to the Australian model, in which all interference activities are registered and shared.

Lessons for Canada

On the surface, the Canadian election security plan looks good: it includes a whole-of-government approach, it has legislative and executive actions, and it provides a clear mission to the SITE Task Force. Nevertheless, it still faces several shortcomings, chief among which is its overwhelming reliance on passive and unenforceable security policies. The UK's inaction in the face of security threats to elections is clearly not a model Canada should look to. The New Zealand and Australian experiences, however, provide some important lessons for Canada.

First of all, Canada could use more enforceable security policies like Australia and New Zealand. The Transparency Register established in Australia proves far more effective at informing the general public of election interference than Canada's CEIPP. In fact, it should be noted that no announcements stemming from the CEIPP occurred during the 2019 federal elections. That comes even though there have been numerous reports of election interference in news media.20 The CEIPP offers too much discretion to the government when it comes to deciding when an interference activity is reported to the public. That is why Canada should turn to a more Australian-like approach to enhancing citizen preparedness by establishing enforceable mechanisms. Moreover, the Elections Modernization Act should be further modernized to resemble legislation passed in Australia and New Zealand. As it stands, Bill C-76 does not include clear and concise enforcement mechanisms or consequences for individuals or corporations found not to be abiding by the law. This legislative ambiguity makes it difficult for national security agencies to enforce and execute the laws appropriately, leaving room for unlawful behaviours from foreign agents and domestic political actors. Canada should look to the examples of Australia and New Zealand and include clear legal and penal consequences for unlawful election-related conduct.

The Canadian government also ought to improve its multidimensional approach to combattting foreign interference. While the SITE Task Force is already a multi-agency team, its Australian and New Zealand counterparts include an even greater number of departments and security agencies. For instance, the Canadian SITE Task Force could incorporate members from Elections Canada which would provide greater expertise in election management. The SITE team could also develop closer ties with political parties and legislative bodies to ensure a larger whole-of-governement approach. Greater inter-departmental cooperation between security agencies, election management bodies (EMBs), and key political actors would improve the multidimensionality of Canada's response in a way that ressembles what has been achieved in Australia and New Zealand.

Lastly, little is know with regard to the implementation oversight surrounding Canada's election security plan. With that being said, this appears to be common across all FVEY countries examined in this analysis. While it is not certain whether or not there is oversight, the present analysis recommends such oversight to take place. The last factor of the assessment framework indeed posits that security policies require active oversight and policy feedback. In the coming years, election security plans that included implementation oversight will be easily distinguishable from those that did not since they will most likely still be relevant and effective. Policies with no implementation oversight will not be actualized and therefore will become obsolete as new threats to elections arise. This is why active policy oversight and actualization is necessary, especially when it comes to election security.

Conclusion

In conclusion, Canada's current election security plan can be considered as the middle-ground plan in comparison to Commonwealth FVEY members. The Canadian plan is far from the UK's inaction policy, yet it falls short of Australia's comprehensive election security plan. While Canada's current policies look good on the surface, they lack the substance needed to actively eliminate the security risks associated with foreign interference and cyber threats. The Canadian government should learn from its intelligence allies down under and adopt more cooperative, multidimensional, and enforceable security policies. Election security is possible, but Canada needs to up its game and adopt a more robust election security plan.

Editor of the CIDP Policy Brief Series: Thomas Hughes

ENDNOTES

[1] Canadian Centre for Cyber Security, 2019 Update: Cyber Threats to Canada's Democratic Process (2019): 16.

[2] Marcus Kolga, Trolling Trudeau – Fears of Foreign Interference in Canada: Marcus Kolga for the Atlantic Council (Macdonald Laurier Institute, 23 October 2019).

[3] Devin Tuttle, Marcus Kolga, and Ai-Men Lau, Canada Can No Longer Ignore Foreign Interference from China: Devin Tuttle, Marcus Kolga and Ai-Men Lau in The Province (Macdonald Laurier Institute, 2 February 2020).

[4] Jean-Nicolas Bordeleau, Foreign Electoral Interventions: An Experimental Study of the Behavioural and Attitudinal Effects on Canadian Voters (Undergraduate Thesis, 2021).

[5] Pippa Norris, Why Electoral Integrity Matters (Cambridge: Cambridge University Press, 2014).

[6] Philipp Trein et al., "Policy Coordination and Integration: A Research Agenda" Public Administration Review (2020): 1-5.

[7] Evert Lindquist, "Organizing for Policy Implementation: The Emergence and Role of Implementation Units in Policy Design and Oversight," Journal of Comparative Policy Analysis 8, no. 4 (2006): 311-324.

[8] Democratic Institutions, "The Government of Canada's Plan to Safeguard Canada's 2019 Election" Speech by the Honourable Karina Gould, the Honourable Harjit Sajjan, and the Honourable Ralph Goodale (30 January 2019), https://www.canada.ca/en/democratic-institutions/news/2019/03/speech-thegovernment-of-canadas-plan-to-safeguard-canadas-2019-election.html (accessed 3 March 2021).

[9] Democratic Institutions, "Cabinet Directive on the Critical Election Incident Public Protocol,"https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html (accessed 5 March 2021).

[10] Democratic Institutions, "Improving organizational readiness," https://www.canada.ca/en/democratic-institutions/news/2019/01/improving-organizational-readiness.html (accessed 6 March 2021).

[11] Democratic Institutions, "Combatting foreign interference," https://www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.html (accessed 3 March 2021).

[12] Lori A. Ringhand, "Foreign Election Interference: Comparative Approaches to a Global Challenge," Election Law Journal: Rules, Politics, and Policy (2021): 1-9.

[13] Amy Mackinnon, "4 Key Takeaways From the British Report on Russian Interference", Foreign Policy, 21 July 2020, https://foreignpolicy.com/2020/07/21/britain-report-russian-interference-brexit/ (accessed 6 March 2021).

[14] Ibid.

[15] Emma Woollacott, "UK Prime Minister Sued BY Own Lawmakers Over Russian Election Interference," Forbes, 29 October 2020, https://www.forbes.com/sites/emmawoollacott/2020/10/29/uk-prime-minister-sued-by-own-lawmakers-over-russian-election-interference/?sh=55af88725c0b (accessed 6 March 2021).

[16] Damien Cave, and Jacqueline Williams. 2018. Australian Law Targets Foreign Interference. China Is Not Pleased. June 28. https://www.nytimes.com/2018/06/28/world/australia/australia-security-laws-foreign-interference.html. (accessed 6 March 2021).

[17] Rod McGuirk, "Australia accuses head of Chinese group of foreign meddling," ABC News, 5 November 2020, https://abcnews.go.com/International/wireStory/man-charged-australian-foreign-interference-law-74033964.

[18] Graeme Orr and Andrew Geddis, "Islands in the Storm? Responses to Foreign Electoral Interference in Australia and New Zealand," Election Law Journal: Rules, Politics, and Policy 20, no.1 (2021): 82-97.

[19] Laura Walters, "Govt agencies tight-lipped on any threats to election," Newsroom, 16 October 2020, https://www.newsroom.co.nz/govt-agencies-tight-lipped-on-any-threats-to-election (accessed 6 March 2021).

[20] Nicole Bogart, "Foreign actors tried to influence Canadian election talk, but did they succeed?" CTV News, 25 November 2019, https://www.ctvnews.ca/politics/foreign-actors-tried-to-influence-canadian-election-talk-but-did-they-succeed-1.4701228 (accessed 6 March 2021).