Government of Canada
Privy Council Office

National Security and Intelligence Advisor to the Prime Minister

Ottawa, Canada
K1A 0A3

Gouvernement du Canada
Bureau du Conseil privé

Conseiller à la sécurité nationale et au renseignement auprès du Premier ministre

TOP SECRET/
Canadian Eyes Only
Confidence of the Queen's Privy Council
(with attachments)

MAR 0 9 2020

MEMORANDUM FOR THE NATIONAL SECURITY AND INTELLIGENCE ADVISOR TO THE PRIME MINISTER

ELECTIONS SECURITY BRIEFING FOR THE HON. DOMINIC LEBLANC PRESIDENT OF THE QUEEN'S PRIVY COUNCIL FOR CANADA

(Information Only)

SUMMARY

- You are scheduled to meet with the Honourable Dominic LeBlanc, President of the Queen's Privy Council, on March 12, 2020.
- The purpose of this meeting is to provide Minister LeBlanc with a summary of elections security related activities undertaken to help safeguard the 2019 General Election (GE 2019) as well as an overview of the threat environment, particularly as it pertains to foreign interference. You will be accompanied by Deputy Secretary to the Cabinet (Governance) Ian McCowan, Chief of the Communications Security Establishment (CSE) Shelly Bruce, and Director of the Canadian Security Intelligence Service (CSIS) David Vigneault.
- Prior to and during GE 2019, Deputy Ministers provided regular briefings on elections security to the then Minister of Democratic Institutions, Karina Gould. Following GE 2019, the December mandate letter for Minister LeBlanc specified that he is to lead a review of the measures put in place to protect the electoral process, and bring forward recommendations to further protect Canada's electoral and democratic institutions from cyber and non-cyber interference.
- For the purposes of this briefing, it is expected that you will provide an overview of elections security and that Ms. Bruce and Mr. Vigneault will expand upon potential threats observed to GE 2019.
- Please find proposed speaking points enclosed under **Tab A** and additional points, should they be required, under **Tab B**.

Canada

Background

- Ahead of the 2019 General Election (GE 2019), the Government of Canada (GoC) put in place a suite of measures to bolster Canada's defence against covert, clandestine and criminal activities by foreign actors, intent on interfering in our electoral and democratic processes.

- A signature initiative established as part of the plan to safeguard GE 2019 was **the Critical Election Incident Public Protocol (CEIPP)**. The CEIPP was designed to ensure consistency in Canada's approach to publicly informing Canadians during the writ period of serious attempts to interfere with their ability to have a free and fair election. Its administration was overseen by a Panel of five senior civil servants, headed by the Clerk of the Privy Council, responsible for determining whether a threshold for informing Canadians was met, either by a single incident or an accumulation thereof.

- An important, concurrent initiative, created in August 2018, was the **Security and Intelligence Threats to Elections (SITE) Task Force**. Comprised of the Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada (GAC), the SITE Task Force improved situational awareness of foreign threats and helped the GoC assess and respond to those threats.

  In addition to enacting legislative amendments to the *Canada Elections Act* to prohibit foreign funding, several other noteworthy security-focused initiatives to safeguard GE 2019 included:

  - Offering additional **cyber technical advice, guidance, and services** to Cabinet Ministers and political parties, including the establishment of a 24/7 dedicated hotline by the CSE Cyber Centre as well as regular unclassified briefings to technical representatives from each registered political party;

  - Offering **classified threat briefings to SECRET-cleared members of the five major political parties** (all of whom participated with the exception of the Bloc Québécois);

  - **Engaging with digital platforms** to encourage the implementation of voluntary measures to increase transparency and combat the spread of disinformation, including signing the Canada Declaration for Electoral Integrity Online (SITE Task Force also engaged directly with digital platforms to facilitate coordination on operational matters); and,

- **Leveraging CSE's *Get CyberSafe* Campaign** to build Canadians' awareness of cyber threats and offer ways in which they can better protect themselves.

- Conscious of the many partners within the GoC that support elections and elections security, as well as a need to coherently support the Panel, an Elections Security Coordinating Committee (ESCC) architecture was established. PCO, under the Security & Intelligence Secretariat, co-chaired all levels of the ESCC with Elections Canada. This was deliberately designed so that the PCO Security and Intelligence Secretariat could bridge the national security community with other key partners, both internal to PCO (Democratic Institutions and Communications) and external to PCO (Elections Canada and the Commissioner of Canada Elections).

Threats to GE 2019

- Pre-election intelligence briefings and monitoring provided a baseline assessment of the threat landscape for GE 2019. This assessment identified three main areas of potential threat including: **cyber threat activity**, as has been directed against other Western elections (supported by the 2017 CSE public threat report and its update in 2019); **HUMINT threat activity**, as it is the most prominent form of foreign interference in Canada; and, **social media platforms being used as a tool by foreign state actors** to conduct and amplify disinformation campaigns.

- Just prior to the writ period, CSIS conducted threat reduction measures (TRMs) aimed at potential interference activities

The redacted information is about a TRM that the Government of Canada conducted in advance of the 2019 Canadian federal election to reduce the foreign interference (FI) threat posed by the Government of Pakistan.

- Also of note and per regular practice, on two occasions (pre-writ and during the writ), GAC sent a notification to all foreign missions in Ottawa reminding them of the obligation to not interfere in the election.

- The post-GE 2019 findings from the SITE Task Force – which are still being finalized – conclude that from September 2018 to October 2019 they observed:

    1. No evidence to indicate that foreign state actors were specifically targeting Elections Canada or Canadian electoral systems and networks (**cyber threat activity**);

    2. No evidence of broad-based, foreign state-directed interference campaigns in the digital information ecosystem, but noted blind spots in determining state attribution and distinguishing between foreign and domestic disinformation campaigns (**social media platforms**);

    3. Foreign interference activities targeting the election directed largely from China, and to a lesser extent from India and Pakistan,

    4. None of these foreign interference activities were assessed to be part of a broad-based electoral interference campaign and did not have an impact on the outcome of the election; and,

    5. None of the activities met the threshold to pursue criminal investigations.

Reviewing the Safeguards

- With the election now concluded, the focus has shifted to reviewing the measures put in place. As required by the Cabinet directive, a formal evaluation is planned of the CEIPP. An independent report will be prepared, assessing the implementation of the CEIPP and its effectiveness in addressing threats to GE 2019. A classified version will be provided to the Prime Minister and to the National Security Intelligence Committee of Parliamentarians (NSICOP), with a public version made available shortly thereafter. Both reports are expected in the Spring 2020. These reviews (possible timings in **Tab C**) will help inform future actions with respect to safeguarding Canada's democratic institutions.

Alia Tayyeb
a/Assistant Secretary to the Cabinet
Security and Intelligence

Attachments
/Tayyeb/

TOP SECRET//[redacted]/CEO
Confidence of the Queen's Privy Council

March 12, 2020 – Elections Security Brief for Minister LeBlanc

Remarks:

- Attempts by foreign states and non-state actors to interfere in democratic and electoral processes are not new threats, nor unique to Canada. Many nations, including our closest allies, have experienced manipulation and interference to varying degrees in their democratic institutions and processes.

- In light of this ever-growing threat, ahead of the 2019 General Election (GE 2019) the Government of Canada put in place a suite of measures to bolster Canada's defences against covert, clandestine and criminal activities by foreign actors intent on interfering in our electoral and democratic processes.

- This plan was announced by Ministers Gould, Goodale and Sajjan in January 2019 and had four areas of action: enhancing citizen preparedness; improving organizational readiness; expecting social media platforms to act; and, combatting foreign interference.

- The ecosystem supporting this plan was complex and diverse, bringing together 10 different federal departments and agencies, including both traditional security partners like CSIS and CSE, as well as non-traditional partners like Elections Canada.

- I though we could start with a brief overview of some of the structures put in place on the security side and then I will turn to my agency colleagues to provide a summary of the treat baseline and activities observed.

What we did

- There are several primary structures/initiatives that I would like to highlight:

  1. A signature, if not the signature initiative was the **Critical Election Incident Public Protocol (CEIPP)**.

     As you are aware, the CEIPP, which was established with the approval of Cabinet, was overseen by a Panel of five senior civil servants, headed by the Clerk of the Privy Council.

     It was designed to ensure consistency in Canada's approach to informing candidates, organizations, election officials, the Prime Minister and other party leaders, as well as the Canadian public during the writ period of serious attempts to interfere with free and fair elections.

     The Panel was responsible for determining whether a threshold was met, either by a single incident or an accumulation of incidents.

They did not observe any activities that met the threshold for a public announcement or affected Canada's ability to have a free and fair election. This assessment was supported by regular intel briefings and monitoring by SITE – which is another structure I would like to highlight in just a moment.

Before doing so, I would note that PCO Security & Intelligence Secretariat (S&I) served as the Secretariat to Panel and as part of that work, organized the security community to provide the routine **threat updates to cleared members of the political parties**.

All the parties participated in these briefings, with the exception of the Bloc Québécois, who chose not to have anyone cleared. We received positive feedback by the parties on this experience.

2. The **Security and Intelligence Threats to Elections Task Force**, or SITE, was actually created in August of 2018 to address threats of foreign interference to the election.

   SITE brought together several security and intelligence partners, namely the Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and Global Affairs Canada (GAC).

   It represented the first time an interdepartmental effort was undertaken to collect and use intelligence related to foreign interference.

   And it was a success. We'll get into the details in threat briefing but procedurally, SITE fed into the Panel, they improved situational awareness of foreign threats and they helped the government assess and respond to those threats.

3. And finally I would highlight another primary initiative, which was the **Elections Security Coordinating Committee** (ESCC) structure.

   These were DM, ADM and DG-level committees, co-chaired by PCO - under the Security & Intelligence Secretariat – and Elections Canada, to support and ensure coordination among the various moving pieces and mandates.

   Running this out of PCO S&I was deliberately done to bridge the national security community with other key partners, both internal to PCO (Democratic Institutions and Communications) and external to PCO (Elections Canada and the Commissioner of Canada Elections).

What we learned – Next Steps

- There are two facets to the discussion on next steps. The first is what we learned and how we apply it in the elections context, and the second is how this fits into the broader, ongoing, strategic discussions on hostile state activity.

- With respect to the latter, the broader discussion, work is ongoing to identify gaps in legislation, to categorize tools in terms of how Canada can most effectively counter hostile state activity, to look at the role of strategic communications in calling attention to state behaviour, etc. This goes beyond democratic institutions and includes economic security, critical infrastructure and social cohesion. [How and when that conversation is brought to the political level is currently with the Clerk for consideration]

- That said, foreign interference is not a threat that is going away, nor diminishing. We can expect an ongoing need to respond.

- So what's next from the elections perspective? Firstly, there are a number of reviews underway.

- For example, the CEIPP is undergoing an independent assessment, the results of which will be included in a classified report to the PM and to the National Security Intelligence Committee of Parliamentarians (NSICOP).

- A public version will be made available shortly thereafter. [You may wish to turn to Mr. McCowan to elaborate on this report and our response]

- While I would not want to pre-empt the outcomes of the independent assessment, I think we can say with confidence that the Panel was a very useful mechanism. Operationally the work we undertook to support the Panel, the collaboration with non-traditional partners, the conversations with new partners like the political party briefings, was all very valuable.

- A couple of important takeaways from this experience and linking those to ongoing work and next steps would be the importance of collaboration and operational coordination.

- <u>Collaboration:</u> Bringing together the traditional national security community with elections partners, both internal and external to PCO, was a central component of safeguarding GE 2019. The ESCC architecture was key in this effort and operationally this collaboration continues. The networks are built and in place to be leveraged as needed.

- <u>Operational Coordination:</u> The security community itself coordinated in a new way for GE 2019. The SITE structure and format allowed for broad sharing of intelligence within existing mandates. This structure worked and it worked well. For example, it allowed for quicker assessments and for quicker verifications of respective agency holdings.

- SITE continues to meet. They are finalizing a consolidated assessment of their findings from the elections and determining how they will continue looking at foreign interference threats.

- The ongoing operational work of SITE should and will inform future policy actions with respect to safeguarding Canada's democratic institutions.

- All relevant Deputy Ministers continue to meet through established mechanisms and SITE's ongoing operational work will continue to feed into those processes as well.

- In terms of Ministerial threat briefings, these took place regularly with Minister Gould and the intent is for that to continue – either on a regular rhythm or situationally as required.

- Finally, I would note that internationally, Canada's approach has been received with much interest in the security community, particularly the Panel, SITE and the political party briefings.

- We are well-placed to continue this work.

What we saw:

- As I mentioned, we did not observe any activities that met the threshold for a public announcement or affected Canada's ability to have a free and fair election, including in the online space.

- That is not the same as saying we saw nothing at all.

- As it turn it over to my colleagues to elaborate, I say that so we keep in mind that the community provided a baseline assessment of threat and then continued to assess the threat landscape off of this baseline in the lead up to and during the writ.

- So while we may not have seen any major instances of foreign interference in our elections, that does not mean that malign actors do not have the capability or intent to interfere in our democratic institutions. The focus on this issue should most certainly continue.

Additional Material for Use as Required:

General Threat Overview:

- In mid 2019, CSIS briefed the community on their baseline assessment that speaks to what they believed the threat landscape would look like as we moved closer to the election. The assessment points were as follows:
    - Current threat landscape in Canada is consistent with past practice from threat actors:
    - Cyber threat activity has been directed against other Western elections.
    -
    - Use of social media platforms by foreign state actors to conduct disinformation and amplification activity has increased globally.
- Now that the election is over, in re-evaluating the above points, CSIS assess that they remained valid for the duration of the writ period. They continually re-evaluated the above positions as new intelligence came in but nothing substantive occurred to shift this assessment.
- Prior to the election, in their 2019 Threats to Canadian Democracy, CSE stated:
    - Foreign cyber interference targeting voters has become the common type of cyber threat activity against democratic processes worldwide where cyber threat actors manipulate online information, often using cyber tools, in order to influence voters' opinions and behaviours. CSE judged it very likely that Canadian voters would encounter some form of cyber interference related to the 2019 federal election, though not to the scale of the 2016 US Presidential elections.
- This type of activity was not able to be substantiated during the electoral campaign.

SITE Findings:

- The post-GE 2019 findings from the SITE Task Force – which are still being finalized – conclude that from September 2018 to October 2019 they observed:
    - No evidence to indicate that foreign state actors were specifically targeting Elections Canada or Canadian electoral systems and networks (**cyber threat activity**);

1

2. No evidence of broad-based foreign state-directed interference campaigns in the digital information ecosystem, but noted blind spots in determining state attribution and distinguishing between foreign and domestic disinformation campaigns (**social media platforms**);

3. Foreign interference activities targeting the election directed largely from China, and to a lesser extent from India and Pakistan,

4. None of these foreign interference activities were assessed to be part of a broad-based electoral interference campaign and did not have an impact on the outcome of the election; and

5. None of the activities met the threshold to pursue criminal investigations.

China threat update:

- China remained interested in supporting candidates and individuals who it perceived would benefit China's overall strategic interests.
-
- **specific incidents suggestive of FI which were briefed to relevant clients (GC and political parties) during the writ period (e.g., Don Valley).**
-

Russia, Pakistan, India, threat update:

- No reported FI activity vis-a vis Election.

Threat Reduction Measures (TRMs):

- As you were briefed, some potential foreign interference was identified and addressed through CSIS threat reduction measures and/or monitoring by Elections Canada:
  -
  -
  - Pakistan (CSIS TRM)
- Just prior to the writ period, CSIS conducted threat reduction measures aimed at interference activities.

- *The redacted information is about a TRM that the Government of Canada conducted in advance of the 2019 Canadian federal election to reduce the foreign interference (FI) threat posed by the Government of Pakistan.*

- Of note, on two occasions (pre-writ and during the writ), GAC sent a notification to all foreign missions in Ottawa of the pending election, reminding them of the obligation that foreign actors not interfere in the election.

Overall Social Media Assessment:

- Over the course of the elections, RRM Canada analyzed online content for indicators of foreign coordinated and inauthentic activity, including the amplification of potential wedge issues in Canada.

- Overall, RRM Canada did not identify evidence to suggest that foreign activity in any way compromised the integrity of the election.

- Differentiating between foreign and domestic disinformation campaigns is an increasing challenge, including because domestic actors are using disinformation tactics traditionally associated with foreign actors and the tactics of foreign actors are constantly evolving.

- Two examples of higher profile cases the RRM Canada looked into include:

  #TrudeauMustGo Hashtag:

  - A Canadian Professor published research indicating that the a number of active users of the hashtag #TrudeauMustGo had the acronym "MAGA" in their profiles – for "Make America Great Again, the slogan of Donald Trump's 2016 presidential campaign. The professor suggested this could be either right-wing activists banding together across the border or it could be a "malicious agency working for a client to promote a certain message".

    - RRM Canada assessed the bulk of the activity was domestic in origin and found no indication of foreign amplification or links, judging it is likely a result of cross-border activism and not a foreign campaign. Key non-government partners shared these findings.

  Buffalo Chronicle Articles:

  - The Buffalo Chronicle published a number of articles targeting PM Trudeau. The Toronto Star and Buzzfeed News published an investigative piece on the Buffalo Chronicle itself,

claiming the owner has accepted payments in the past to publish negative articles about clients' political opponents.

- Avaaz, which is an online social action platform, posted a petition calling for an RCMP investigation into who may have paid the Chronicle's owner to promote disinformation related to Canada's election, which has garnered at least 22,000 signatures. The Avaaz petition states that "these stories have reached an estimated 20 million views and counting".
    - RRM Canada assessed this number as greatly exaggerated based on its own open-source analysis but cannot fully quantify engagement at this point. They assessed that the most likely reason for the discrepancy is that the metric being used, 'Reach' -- one commonly used on social media monitoring platforms -- measures the aggregate number of followers that each account that shared the content has rather than the number of users that actually engaged with the content, i.e., shared it, liked it or were aware of it.
    - The RRM also noted that Facebook, the primary platform for the article's amplification, had around 240,000 engagements on all Buffalo Chronicle stories involving Canada between March and October 2019.
    - While the RRM does not have any evidence to suggest the articles compromised the integrity of the election, they will continue research and analysis in the days and weeks ahead to ascertain how Buffalo Chronicle content was disseminated on social media to try to assess whether foreign actors are involved.
- This is good example of work extending into the post-election space.