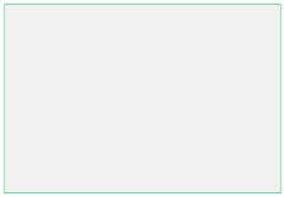
REDACTIONS – LEGEND

Information that relates to investigative techniques or plans for lawful investigations, information that could be injurious to Canada's international affairs, defence or intelligence operations; or personal information about individuals. Public identification of this information would give hostile actors insight into Canadian national security and intelligence operations and priorities, which could adversely affect Canada's ability to counter threats to national security.



Information deemed not relevant to the Committee's study of Foreign Interference.

[redacted]

MEMORANDUM FOR THE PRIME MINISTER
c.c.: Ian Shugart, Catherine Blewett

SAFEGUARDING THE 2019 GENERAL ELECTIONS

(Information Only)

SUMMARY

- The purpose of this note is to provide you with a summary of elections security related activities that were undertaken to help safeguard the 2019 General Elections (GE 2019). It is also to provide you with an overview of the threat environment in the lead up to and during GE 2019, particularly as it pertains to potential foreign interference.

- Ahead of GE 2019, the Government of Canada 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. This included the Critical Election Incident Public Protocol (CEIPP), administered by a Panel of senior civil servants, and the Security and Intelligence Threats to the Elections (SITE) Task Force, among other initiatives. Additionally, prior to the writ period, the Canadian Security Intelligence Service (CSIS) [redacted].

- Pre-election intelligence briefings and monitoring provided a baseline assessment of the threat, [redacted]. While some instances of potential interference were observed [redacted], the Panel concluded that none of these activities met the threshold for a public announcement or affected Canada's ability to have a free and fair election.

- More broadly, it is assessed that the [redacted] in GE 2019 could be due, in part, to the proactive and public stance taken on the issue by the Government of Canada. This includes [redacted], ministerial engagement with the media and Communications Security Establishment public reports in the lead-up to the elections, acknowledging the threat of foreign interference.

- With the election now concluded, the focus has shifted to reviewing the effectiveness of measures put in place. Reviews of the practises and processes, some of which will be made public, will help inform future actions with respect to safeguarding Canada's democratic institutions. We will keep you apprised of any developments.

Background

- Attempts by foreign states and non-state actors to interfere in democratic and electoral processes are not a new threat, nor a phenomenon unique to Canada. Over the past ten years, almost 40 nations have experienced manipulation and interference to varying degrees in their democratic institutions and processes. In light of this ever-growing threat, the Government of Canada (GoC) put in place a suite of measures to bolster Canada's defences against covert, clandestine and criminal activities by foreign actors ahead of the 2019 General Elections (GE 2019).

- 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 coherence and 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 through 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 to Canada's electoral processes 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 to build their cyber hygiene and security, including the establishment of a 24/7 dedicated hotline by the CSE Cyber Centre to field questions and concerns during the electoral campaign as well as regular unclassified briefings to technical representatives from each registered political party;

- Offering **classified threat briefings to [redacted] cleared members of the five major political parties** (all of whom participated with the exception of the Bloc Québécois) to promote situational awareness, provide direct support and encourage the strengthening of internal security practices and behaviours;

- Activating the **G7 Rapid Response Mechanism** (RRM) (as the GAC member of the SITE Task Force) to strengthen coordination among G7 democracies in monitoring malign activities by foreign actors in the social media space. The RRM Canada provided open-source monitoring and data analytics based on indicators and thresholds of foreign interference;

- **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. The SITE Task Force also engaged directly with digital platforms to facilitate coordination on operational matters in line with existing mandates; 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. The Privy Council Office (PCO), under the National Security and Intelligence Advisor, 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).

- The ESCC underpinned a host of activities and brought together these diverse partners to develop a common understanding of roles, responsibilities and mandates. It ensured a coordinated approach was brought to the classified threat briefings referenced above. Also, as part of the ESCC role, a number of table-top exercises were developed and run at Director General, Assistant Deputy Minister and Deputy Minister-level, integrating the national security community with Elections Canada and the Commissioner of Canada Elections. [redacted] cleared members of the major political parties were similarly exercised on a number of potential scenarios.

Threats to GE 2019

- Pre-election intelligence briefings and monitoring provided a baseline assessment of the threat landscape for GE 2019. These assessments identified several major 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); ; and, **being used as a tool by foreign state actors** to conduct and amplify disinformation campaigns.

- As such, supported by regular intelligence briefings and monitoring by the SITE Task Force, the Panel 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.

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 you and to the National Security Intelligence Committee of Parliamentarians (NSICOP), with a public version made available shortly thereafter. It is expected that both reports will be available in the Spring 2020. The NSICOP may resultantly choose to review the security and intelligence community's activities with respect to GE 2019.

- Less formal reviews, "hot washes", and lessons learned discussions, have been undertaken by the ESCC at all levels. The SITE Task Force is also undertaking an internal evaluation with the intent to produce a classified report. Elections Canada is required to produce several unclassified reports, including an after-action report that will be submitted to the House of Commons, and a retrospective report on the conduct of the elections and implementation of legislative changes. The Chief Electoral Officer will also produce a report, likely by mid-2020, which will include recommendations to improve the electoral process. These reviews (possible timings in **Tab A**) will all help inform future actions with respect to safeguarding Canada's democratic institutions.

PCO Comment

- 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. Work stemming from this structure was extensive and comprehensive, ensuring coordinated briefings at all levels over many months, including to the political parties. It facilitated coordinated communications, technical briefings and media responses. It designed and executed multiple table-top exercises to build understanding and ensure readiness across the community. And, it established circulation of two daily reports: 1. A classified daily report, produce by the SITE Task Force, and circulated across the national security community, including the Panel; and, 2. An unclassified daily report, produced by the Government Operations Centre, and circulated across the federal government, including Elections Canada, as well as to political parties. This proved to be an important resource in understanding provincial and territorial dynamics affecting the federal election.

- Some of the salient findings from the ESCC evaluation include positive feedback in these aforementioned areas, particularly as it pertains to information sharing and coordination. Challenges that arose during

GE 2019 and/or areas where further improvements could be considered include:

  - Exploring the role of government in the disinformation and domestic interference space in a way that is conscious and respectful of the privacy, rights, and freedoms of Canadians;

  - Capitalizing on the important role of the Government Operations Centre in establishing links and disseminating information to improve collaboration with the provinces and territories as it pertains to the conduct of elections and information sharing on security issues;

  - Continuing a focus in a non-electoral period on increasing education to build awareness, confidence and resilience on threats to democratic institutions and foreign interference as well as the electoral process; and,

  - Considering the merits and modalities of having SECRET-cleared political party representatives on a more permanent basis.

- PCO will continue to coordinate with partners to ensure work continues in these areas.

- Arguably, this assessment places the level of foreign interference activity in GE 2019 . The proactive and public stance taken by the GoC on this issue may have influenced the behaviour of mal-intentioned actors. This public face included Ministerial engagement with the media as well as CSE public reports in the lead-up to the elections acknowledging the threat of foreign interference. While it is difficult to measure the true impact this may have had, strong consideration should be given to leveraging public communications as a key tool in combating foreign interference beyond the election cycle.

- PCO will keep you apprised of any developments, particularly as the various reports on the election are completed.

David Morrison

Attachment

Xavier/jct

[redacted]

October 29, 2019 – Security Brief for Minister Gould

1. Elections Apparatus Summary:

Panel

- Panel of Five met weekly during the writ period and actively monitored threats to the election.
- The Panel 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 (assessment supported by regular intel briefings and monitoring by SITE).

[redacted]

- This assessment is ongoing by the security and intelligence agencies with some preliminary findings already concluded.
- An "assessment" of the Critical Election Incident Public Protocol (the Protocol) will be conducted in the coming months.

Political Parties

- In accordance with the Protocol, cleared members of the political parties also received routine threat updates. We received positive feedback by the parties on this experience, most notably from the CPC.
- As the writ period is over, these briefings have concluded.

Security and Intelligence Threats to the Election (SITE) Task Force

- SITE will continue to meet and analyze their reporting with a view to producing a consolidated assessment of their findings.
- SITE will also provide lessons learned and recommendations, including whether they or a similar structure should persist to examine threats to democracy more broadly and whether similar structures should be set up for other special events and investigations.

Elections Security Steering Committees (ESSC)

- DG, ADM and DM ESSC meetings (Co-chaired by Elections Canada and PCO S&I and attended by PCO DI, PCO Comms, SITE members, Public Safety and the CSE Cyber Centre) will continue to meet post-election.

- The main objectives will be to: a) present the consolidated SITE assessment; b) conduct a community "hotwash"; and c) ensure coordination regarding all the post-election reporting requirements.

Social Media Platform Engagement:

- SITE operational relationships with social media companies throughout the writ period.

- These engagements included meetings, briefings and exchanges of information on both sides. provided those companies with some information deemed to be of potential concern and also received operational tips from the companies.

- This engagement is expected to continue and has established the foundation for ongoing, productive relationships moving forward.

CCCS Hotline Service:

- All ministers are signed up to the service and all political parties received guidance from CCCS.

- Between Sept 11 and Oct 21, CCCS received one call from a and five calls from political parties

- 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.

3. General Threat Overview:

- In mid 2019, CSIS briefed you on their baseline assessment that speaks to what they believed the threat landscape would look like as we moved closer to the election. As a reminder, 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.

- 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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

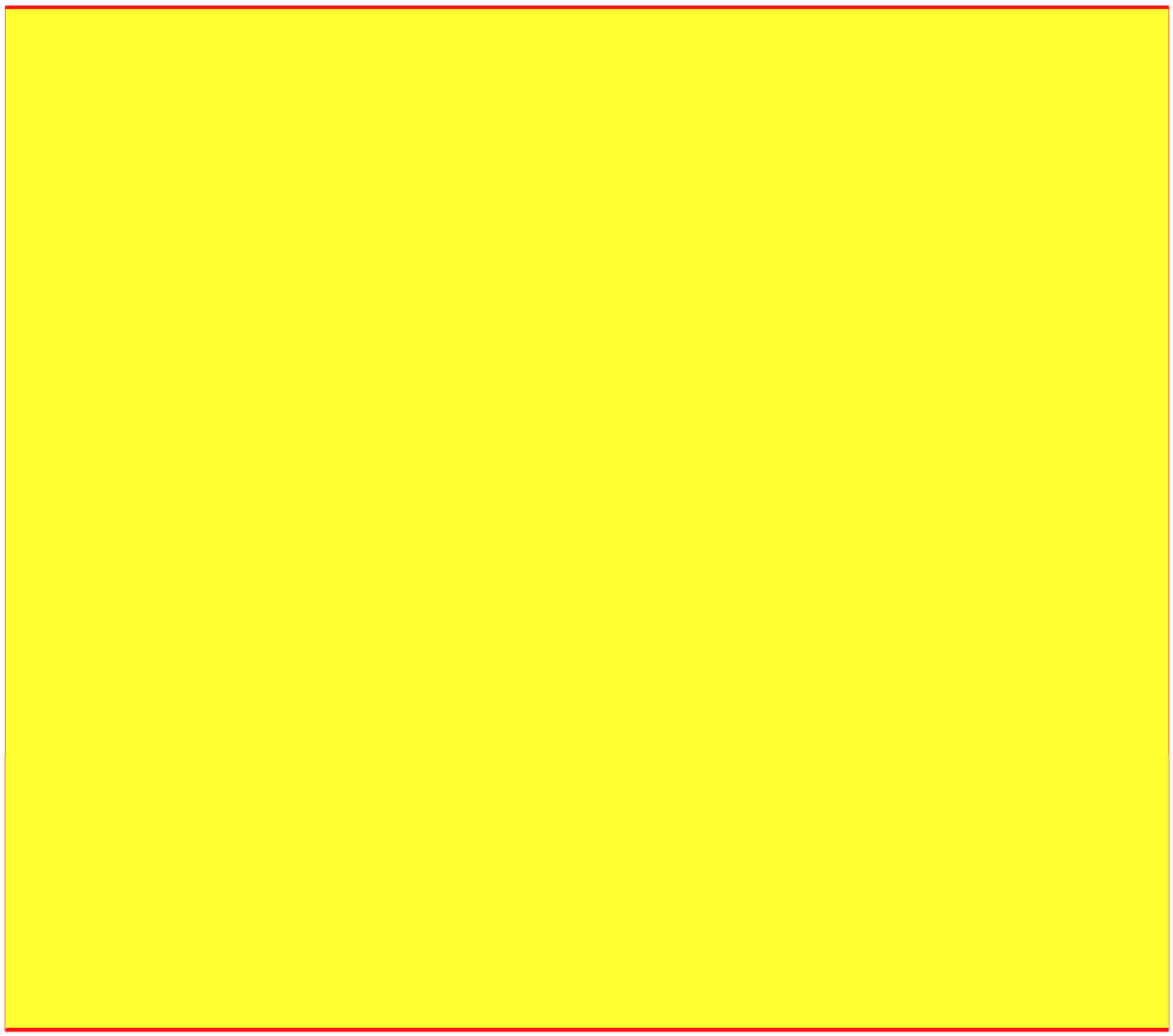
4. Overall Social Media Assessment:

- 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.

[redacted]



- This is good example of work extending into the post-election space.

Elections Security Brief for Minister LeBlanc

Remarks:

SLIDE 2: Challenge on an International Scale

[Delivered by either NSIA or Dep Sec McCowan]

- 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 the past 10 years, almost 40 nations have experienced manipulation to varying levels – this is a global challenge.

- We need to prepare our citizens and systems to respond to this threat. Governments and citizens have to contend with these challenges and risks while respecting democratic rights and freedoms.

- A 2017 public threat report from the Communications Security Establishment (CSE) identified political parties and politicians, electoral activities, and the media as vulnerable to threats, but also noted that our system has inherent strengths built-in. For example, paper-based ballots cannot be "hacked".

- The 2019 update to this report reinforced that it was very likely that Canadian voters would encounter some form of cyber interference during the 2019 elections. Canadian political parties, their candidates and staff were also identified as a likely target.

SLIDE 3: Protection 2019 General Elections

[Delivered by Dep Sec McCowan – talking points in the Deck]

- Potential interjection: As Ian mentions, the ecosystem supporting this plan was complex and diverse, bringing together 10 different federal departments and agencies. In addition, at the crux of this was the work PCO did to bridge of traditional security partners like CSIS and CSE with non-traditional partners like Elections Canada.

- Potential interjection: 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.

SLIDE 4: Protecting Democracy Ecosystem

[Delivered by Dep Sec McCowan – talking points in the Deck]

SLIDE 5: Elections Incident Response Architecture

[Delivered by NSIA]

- Conscious of all the moving parts that Ian has just described, of the various players in the ecosystem, of their mandates and of a requirement to coherently support the Panel, an Elections Security Architecture was established by my branch.

- A primary component of the architecture is the **Elections Security Coordinating Committee** (ESCC) structure. These are DM, ADM and DG-level committees, co-chaired by PCO - under the Security & Intelligence Secretariat – and Elections Canada. The DG and ADM levels continue to meet in the off-cycle, to maintain the connections and momentum established.

- Running this out of PCO S&I is 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).

- It also feeds into the work of the Panel, ensuring coordination of any incident response, and is underpinned by SITE.

SLIDE 6: CEIPP

[Delivered by Dep Sec McCowan – talking points in the Deck]

- Potential interjection: The Panel was responsible for determining whether a threshold was met, by either 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.

SLIDE 7: SITE

[Delivered by NSIA]

- The Security and Intelligence Threats to Elections Task Force, or SITE, was actually created in August of 2018 to improve situational awareness of foreign threats to Canada's electoral processes and help assess and respond to those threats.

- 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 the 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.

SLIDE 8: 2019 General Election – Outcomes

[Delivered by Dep Sec McCowan – talking points in the Deck]

- Potential interjection: Before we focus on the threat briefing, there are areas of focus for the next-steps for elections security that I would like us to keep in mind. The first is how elections security fits into the broader, ongoing, strategic discussions on hostile state activity and the second is what we learned in 2019 and how we apply it to future elections.

    - With respect to the former, 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.

    - With respect to the latter, the threat is not going away, or diminishing. We can expect an ongoing need to respond. A couple of important takeaways would be the importance of collaboration and operational coordination.

    - Collaboration: 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.

    - Operational Coordination: 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.

    - 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.

[redacted]

SLIDE 9: Canada's Ongoing Threat Environment

[Delivered by NSIA]

- What do we know?
- Who are the main threats?
- What happened during the US Election?
- What can we expect and how is this complicated by the current pandemic?

Slide 10: What Do We Know?

[Delivered by NSIA]

- Because of Canada's robust measures for the protections of elections, including a paper ballot system, strong cyber-defenses at Elections Canada provided by the Canadian Centre for Cyber Security, and strong campaign finance laws, foreign nations are forced generally into using more traditional means of interference.

- Attempts by foreign nations to interfere in Canadian Democracy begin before the election writ is dropped, often many months or years before.

[redacted]

Slide 11: Who are the main threats?

[Delivered by NSIA]

[redacted]

- Chinese activity is significant and ongoing, [redacted]

[redacted]

[redacted]

[redacted]

Slide 12: What Happened During the US Election?

[Delivered by NSIA]

[redacted]

[redacted]

[redacted]

Slide 13: What We Can Expect

[Delivered by NSIA]

- [redacted]
- [redacted] China will continue its efforts. [redacted]

[redacted]

[redacted]

- COVID represents an opportunity that could be weaponized through disinformation to change election narratives or influence how voters feel about the safety of polling stations.

Slide 14: Next Steps

[Delivered by NSIA]

- The Panel of Five is meeting to maintain awareness of the threat environment and be ready to act should there be another election call outside the 4-year normal electoral cycle.

- The Election Security Coordination Committee governance structure is now meeting monthly at the DG and ADM level to ensure ongoing connectivity across PHAC and the S&I community.

- SITE has updated their threat assessment and continues to look for, and assess, what hostile states are doing and how those activities may impact the next election.

Government of Canada | Gouvernement du Canada

Protecting Canada's Democracy
General Election Security

Government of Canada | Gouvernement du Canada

Challenge On An International Scale

ACCUEIL | INFO | INTERNATIONAL | POLITIQUE AMÉRICAINE

L'interférence russe et le silence de Donald Trump

Publié le mardi 20 février 2018

GLOBAL

Russia's Interference in the U.S. Election Was Just the Beginning

Democracies across the West are vulnerable to foreign influence—and some are under attack.

SECURITY

Europe prepares cyber defenses to protect elections from Russian interference

REUTERS JANVIER 13, 2017 9:33 PM

Denmark to ramp up cyber security efforts - defence minister

By Teis Jensen

Reuters 21 November 2017

LE MONDE *diplomatique*

décembre 2017, pages 12 et 13

LE SUSPECT IDÉAL DES ÉLITES OCCIDENTALES

Ingérence russe, de l'obsession à la paranoïa

Les Occidentaux se coordonnent pour accuser la Russie de cyberattaques

Chose inédite, les Etats-Unis, le Royaume-Uni, les Pays-Bas et le Canada ont accusé la Russie d'être responsable de cyberattaques majeures.

Australia forms task force to guard elections from cyber attacks

June 09 2018 09:36 AM

Elections 2019: Why India cannot underestimate the 'foreign hand'

India has become more vulnerable to attacks. Only, the 'weapons of mass destruction' now are data and social media, which any nation can use to influence our elections.

Election Interference in the Digital Age: Building Resilience to Cyber-Enabled Threats

#EUProtects | 15 October 2018 to 16 October 2018

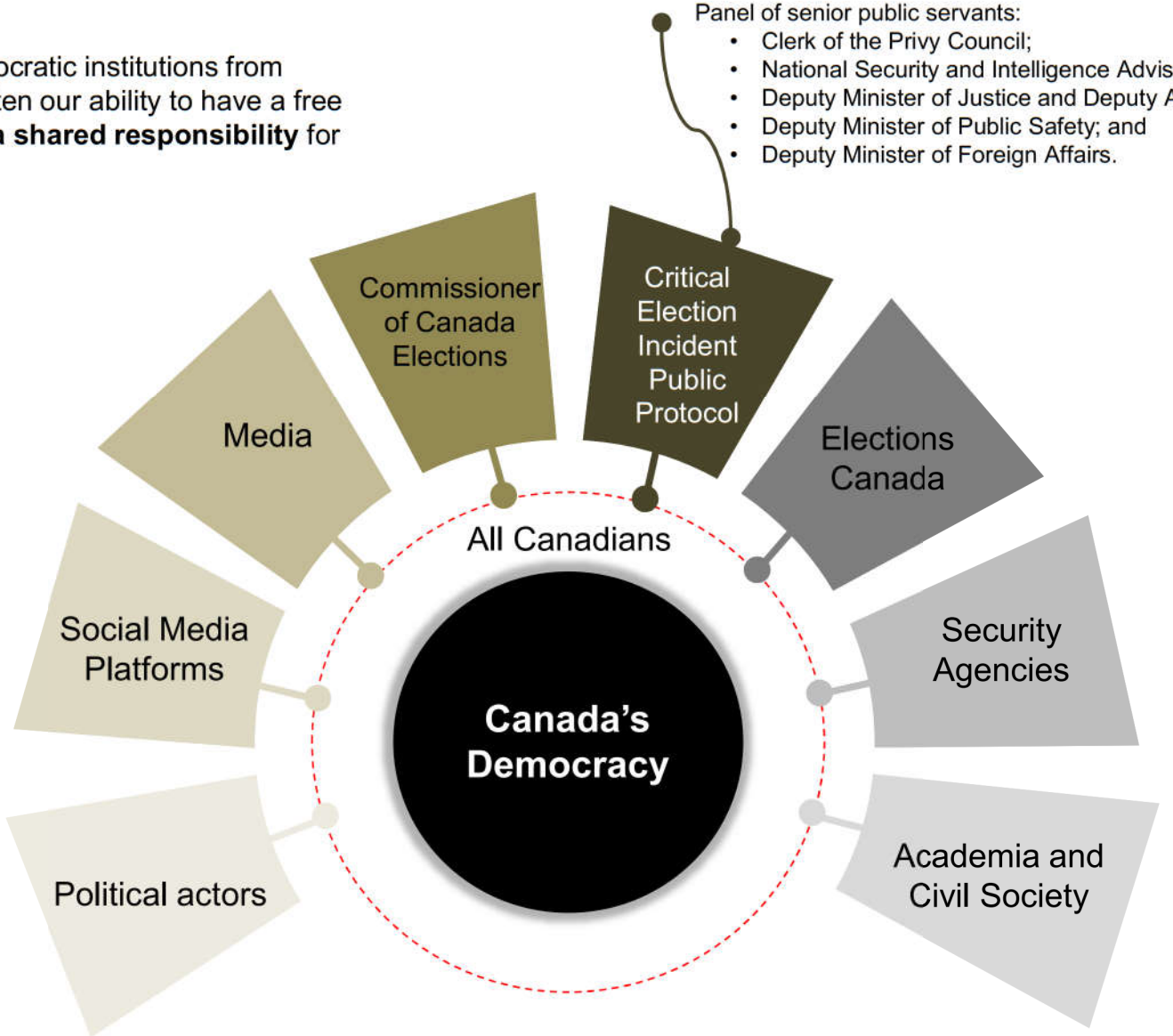
Protecting 2019 General Election

- **January 30, 2019** - Announcement details range of measures, new and existing, to protect the General Election, including:
  - Security and Intelligence Threats to Elections (SITE) Task Force;
  - Creating the Digital Citizen Initiative;
  - Offering additional cyber technical advice, guidance, and services to political parties;
  - Offering classified threat briefings to key leadership in political parties; and
  - Engaging with social media platforms, including through the Canada Declaration for Electoral Integrity Online
- **June 11, 2019** - Cabinet Directive on the Critical Election Incident Public Protocol (the Protocol) published
- **May 2019** - Panel began meeting to prepare for election

Government of Canada | Gouvernement du Canada

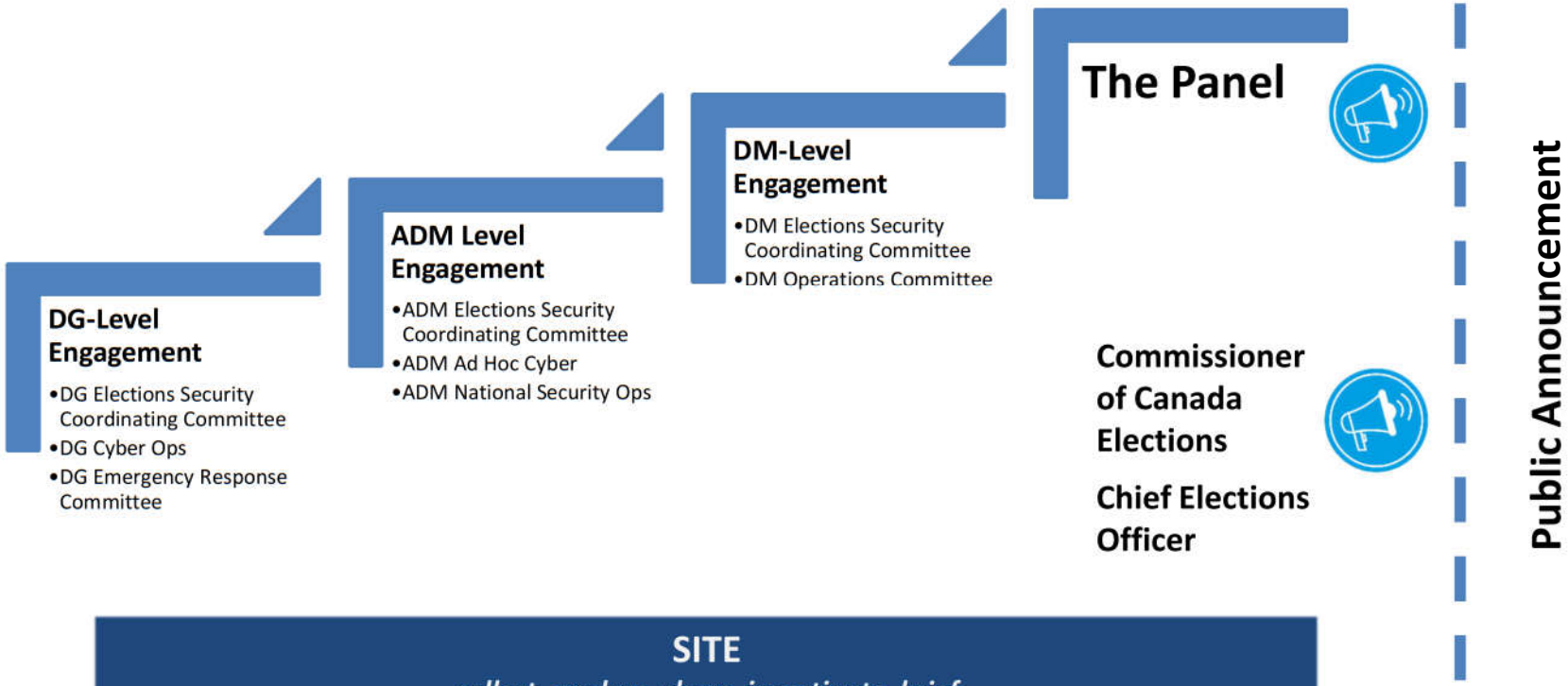
Protecting Democracy Ecosystem

Protecting our democratic institutions from incidents that threaten our ability to have a free and fair election is **a shared responsibility** for all Canadians.



Government of Canada | Gouvernement du Canada

Election Incident Response Architecture



SITE

collect, analyze, share, investigate, brief

In accordance with existing mandates and Canadians laws

CSE, RCMP, CSIS, GAC

Government of Canada | Gouvernement du Canada

Critical Election Incident Public Protocol

CRITICAL ELECTION INCIDENT PUBLIC PROTOCOL

1 AWARENESS

THE GOVERNMENT OF CANADA BECOMES AWARE OF AN INTERFERENCE ATTEMPT IN THE ELECTION DURING THE WRIT PERIOD.

2 SHARING INFORMATION

HEADS OF NATIONAL SECURITY AGENCIES BRIEF THE CRITICAL ELECTION INCIDENT RESPONSE PANEL:

Clerk of the Privy Council

National Security and Intelligence Advisor

Deputy ministers of Justice Canada, Public Safety & Global Affairs Canada

3 ASSESSING THREAT

IF THE PANEL FINDS THAT THERE IS A SUBSTANTIAL THREAT TO A FREE AND FAIR ELECTION:

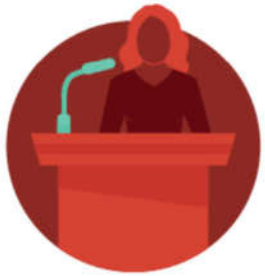
Inform the Prime Minister, political party officials and Elections Canada of the incident and that a press conference will be held

4 PUBLIC ANNOUNCEMENT

CANADIANS ARE INFORMED OF:

What is known about the incident

Any steps they should take to protect themselves



Security and Intelligence Threats To Elections (SITE) Task Force

UNCLASSIFIED//FOR OFFICIAL USE ONLY

SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE

WHAT ARE WE TALKING ABOUT?

Covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada

Security and Intelligence Threats to Elections Task Force - Partner Roles

Leading to Election 2019

	MANDATE/ROLE	ACTIVITIES
CSE Communications Security Establishment	**Information Technology Security** • Providing advice, guidance, and services to help ensure the protection of electronic information and of systems of importance **Foreign Intelligence** • Collection of foreign intelligence for Government of Canada on threat actors **Supporting CSIS and RCMP** • Providing assistance on technical operations	• Providing intelligence and cyber assessments on the intentions, activities, and capabilities of foreign threat actors • Protecting Government systems and networks related to elections through cyber defence measures • Providing cyber security advice and guidance to political parties, provinces and other institutions involved in democratic processes
CSIS Canadian Security Intelligence Service	**Intelligence and Threat Reduction** • Collection of information about foreign influenced activities that are detrimental to the interest of Canada and are clandestine or deceptive or involve a threat to any person • Countering such activities through threat reduction measures **Intelligence Assessment** • Providing advice, intelligence reporting and intelligence assessments to Government of Canada about foreign influenced activities	• Providing threat briefings and intelligence reporting to Elections Canada and the Commissioner of Elections • Providing an assessment of hostile state activity methodologies and capabilities to Government of Canada decision makers
GAC Global Affairs Canada	**G7 Rapid Response Mechanism** • Open source research on global trends and data on threats to democracy • Partnership with G7 countries to share information and coordinate responses to threats as appropriate	• Providing research on disinformation campaigns targeting Canada by foreign actors • Reporting on global trends, metrics, and incidents • Coordinating attribution of incidents
RCMP Royal Canadian Mounted Police	**National Security** • The primary responsibility for preventing, detecting, denying and responding to national security-related criminal threats in Canada • Investigates criminal offenses arising from terrorism, espionage, cyber attacks, and foreign influenced activities • The key investigatory body for Elections Canada if criminal activity is suspected	• Investigates any criminal activity related to interference or influence of Canada's electoral processes • Works closely in partnership with intelligence, law enforcement and regulatory agencies

Government of Canada / Gouvernement du Canada

2019 General Election – Outcomes

- No threats met the threshold and therefore none were reported to Canadians.
- Procedurally, an evaluation of the CEIPP was conducted and written by Mr. Jim Judd.
  - while the Panel did not intervene during the 2019 election, it was prepared to do so and decision-making about potential interventions did take place behind the scenes as appropriate;
  - the Panel included a range of public service experience and was supplemented where needed; and,
  - the Panel was appropriately supported and worked well with its principal partners (e.g., Elections Canada, security agencies).
- That does not mean no activity was observed. SITE conducted a review and produced a classified, after action report.

Government of Canada | Gouvernement du Canada

Canada's Ongoing Threat Environment

What do we know?

Who are the main threats?

What Happened During the US Election?

What can we expect and how is this complicated by the current pandemic?

What do we know

[redacted] foreign state actors over time have largely used [redacted] in an effort to influence Canada's electoral processes.

- This is partly a result of the way that Canada conducts its elections (paper-based ballots, relatively robust federal financing laws, political party constitutional nomination processes)

[redacted]

Government of Canada | Gouvernement du Canada

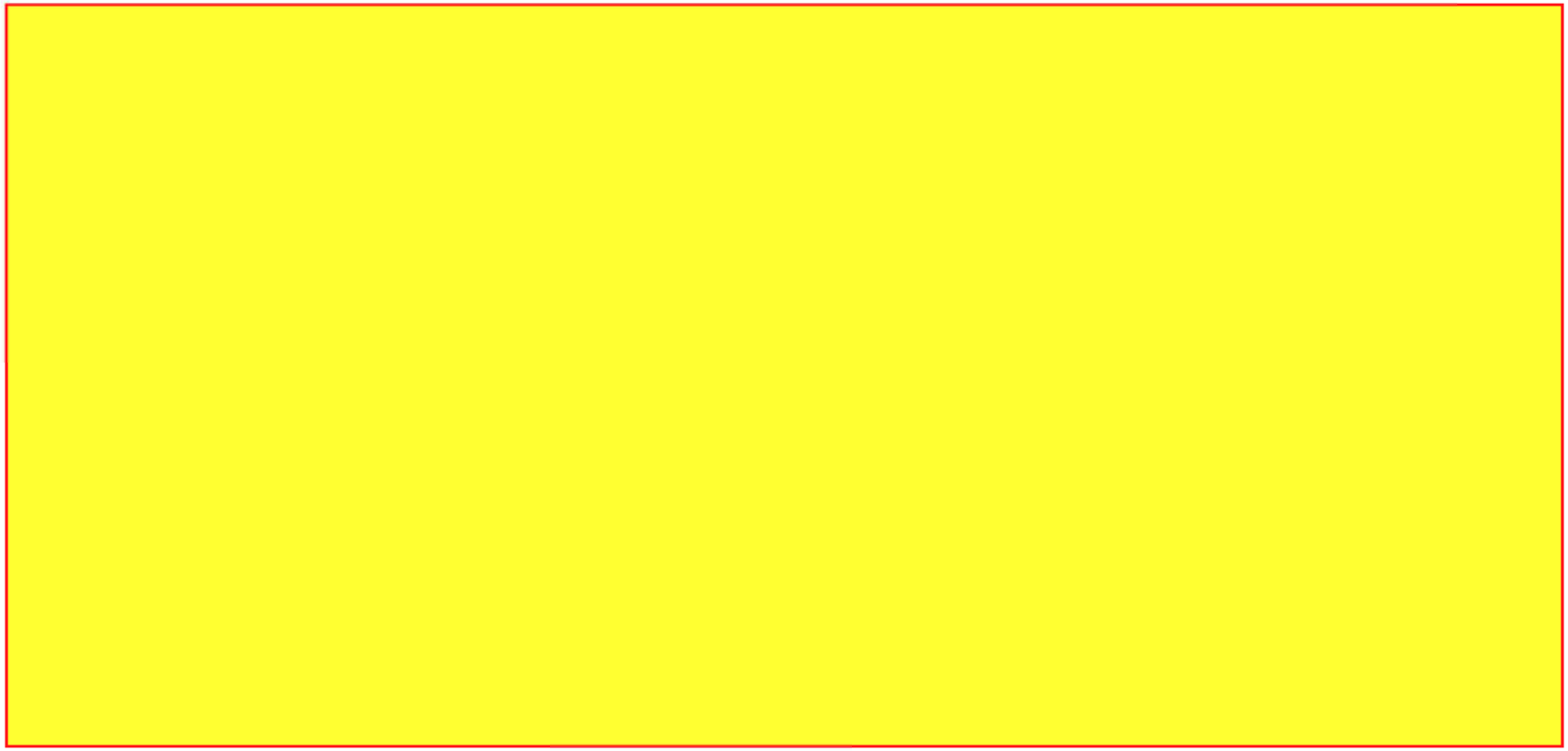
Who are the main threats?

The People's Republic of China (PRC), followed by [redacted] the Russian Federation, pose the top-tier foreign interference (FI) threats to Canada's democracy.

[redacted]

Government of Canada / Gouvernement du Canada

What Happened During the US Election?



2022-12-08

Government of Canada / Gouvernement du Canada

What can we expect?

Consistent with the 2019 Canadian Federal election, there is no evidence of a significant specific cyber threat to Canadian elections or electoral processes.

PRC [redacted] threat activities have not shifted or diminished following the 2019 election.

[redacted]

Foreign state actors are increasingly able to [redacted] leverage domestic political rhetoric in their online disinformation campaigns, making this type of interference more difficult to attribute.

[redacted]

COVID related social and political restrictions may limit [redacted] may create additional opportunities for online disinformation campaigns.

Next Steps

- The Panel of Five has begun meeting again
- The Election Security Coordination Committees are meeting to monitor and adapt to emerging trends and threats
  - PHAC now has representatives at all levels to coordinate response should adversaries use the current pandemic to augment their efforts
- SITE continues to track, assess, react and share intelligence on foreign interference activity by foreign state and non-state actors.

Daily Foreign Intelligence Brief, 21 February 2020

2. China/Canada: Subtle but Effective Interference Networks

- ***CA Assessment:*** Investigations into activities linked to the Canadian federal election in 2019, reveal an active foreign interference (FI) network

National Intelligence Assessment
Évaluation nationale du renseignement

NIA 02/2019

CANADA: National Security Outlook 2019

Executive Summary

- Canada's **2019 federal election** will be an attractive target for foreign states who want to influence or undermine our democratic processes.
-
-

Bottom Line for Canada

-
- Espionage and foreign interference activities are the most significant threat to Canada's long-term prosperity, while terrorism is the greatest threat to Canadian lives and public safety.
-

Espionage and Foreign Interference Activities

3. ***China is still the most active and sophisticated perpetrator of espionage[2] and foreign interference activities[3] in Canada.***

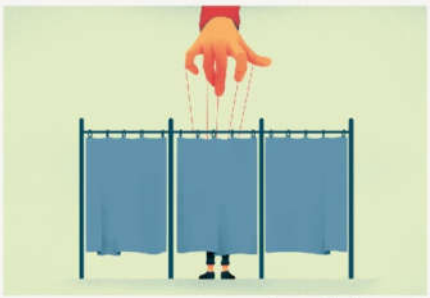
as well as academia, and the private sector to influence opinions, collect intelligence and access sensitive information that furthers China's economic, military, and security interests. The threat is pervasive and goes beyond elections.

THREATS TO THE 2019 CANADIAN ELECTION

Canada is an attractive target (a G7, NATO, and Five Eye country) of foreign state efforts to influence our democratic processes. While the threat of foreign influence is constant (and not always covert), efforts tend to increase in the lead-up to elections. These activities usually have one the following objectives:

- Changing the prospects for political actors;
- Manipulating public discourse and underlying public opinion;
- Damaging or sowing doubt about the integrity of the electoral process; and,
- Influencing the behaviour of elected officials and the public.

Efforts to covertly influence policy actors and outcomes continue to occur across Canada, directed against all major political parties and at all levels of government (federal, provincial, municipal).



Source: The Economist

In the long-run, these activities could weaken public trust in democratic institutions and processes, and undermine the integrity of the decision-making process.

[2] **Espionage** is the state-sponsored collection of sensitive political, economic, or security information by clandestine means.

[3] **Foreign interference activities** refer to actions by state actors, proxies or co-optees that are covert, deceptive, or coercive and go beyond normal or acceptable diplomatic activity and are meant to mislead or actively undermine the host state.

Bottom Line for Canada

37. Canada's threat environment is multi-dimensional and dynamic. We face the same broad national security threats as in 2018, though many of these have expanded, contracted or transformed.

Espionage and foreign interference activities are significant threat to Canada's long-term economic prosperity.

CANADA
National Security Outlook 2019

KEY JUDGEMENTS

ESPIONAGE AND FOREIGN INTERFERENCE ACTIVITIES

China is the most active and sophisticated perpetrator of espionage and foreign interference activities in Canada.

THREATS TO THE 2019 CANADIAN ELECTION

Canada is an attractive target (a G7, NATO, and Five Eye country) of foreign state efforts to influence our democratic processes. While the threat of foreign influence is constant (and not always covert), efforts tend to increase in the lead-up to elections. These activities usually have one the following objectives:

- Changing the prospects for political actors;
- Manipulating public discourse and underlying public opinion;
- Damaging or sowing doubt about the integrity of the electoral process; and,
- Influencing the behaviour of elected officials and the public.

continue across Canada, directed against all major political parties and at all levels of government (federal, provincial, municipal).

In the long-run, these activities could weaken public trust in democratic institutions and processes, and undermine the integrity of the decision-making process.