UNCLASSIFIED

## Critical Election Incident Public Protocol

### Table of Contents


| ITEM | TAB |
|---|---|
| Critical Election Incident Public Protocol – Version Shared with Political Parties | A |
| Critical Election Incident Public Protocol – Questions and Answers | B |
| Critical Election Incident Public Protocol – Current Web Version | C |
| Critical Election Incident Public Protocol – Current Web Graphic | D |
| Protecting Democracy – January 30, 2019, Technical Briefing Transcripts | E |
| Protecting Democracy – January 30, 2019, Minister's Announcement Transcripts | F |
| PCO Communications – Draft Scenario Note on Technical Briefing | G |
| PCO Communications – GoC Election Communications Steering Committee Agenda | H |
| PCO Communications – Presentation to the Group of Five DGs Communications | I |
| PCO Communications – Protecting Democracy Artboards | J |

# Critical Election Incident Public Protocol

## 1.0 Introduction

The protection and preservation of Canada's democratic institutions and practices is one of the core responsibilities of the federal government.

National security threat and risk assessments, along with the experience of key international allies, underscore that Canada's 2019 General Election may be vulnerable to foreign interference in a number of areas. Recognizing this, significant work has been undertaken within the federal government to protect and defend electoral systems and processes. As part of this work, the Government of Canada has established the Critical Election Incident Public Protocol (CEIPP) in order to ensure coherence and consistency in Canada's approach to publicly informing Canadians during the writ period about incidents that threaten Canada's ability to have a free and fair election.

## 2.0 Purpose

The *Cabinet Directive on the Critical Election Incident Public Protocol* sets out the ministers' expectations with respect to the general directions and the principles to guide the process for informing the public during the writ period of an incident that threatens Canada's ability to have a free and fair election.

The Protocol is an application reflective of the caretaker convention. The caretaker convention puts into practice the principle that the government is expected to exercise restraint in its activities and "restrict itself" in matters of policy, spending and appointments during the election period, except where action is "urgent" and "in the national interest".

During the caretaker period, announcements that must proceed are to be made in the name of the department to ensure a distinction between official government business and partisan activity.

## 3.0 Scope of Application

The Critical Election Incident Public Protocol will have a limited mandate. It will only be initiated to respond to incidents that occur within the writ period and that do not fall within Elections Canada's areas of responsibility (i.e., with regard to the administration of the election, as identified in the *Canada Elections Act*). Incidents that occur prior to the writ period will be addressed through regular Government of Canada operations.

# 4.0 Panel

The CEIPP will be administered by a group of senior civil servants who will, working with the national security agencies within the agencies' existing mandates, be responsible for determining whether the threshold for informing Canadians has been met, either through a single incident or an accumulation of separate incidents.

This Panel will be comprised of:

- the Clerk of the Privy Council;
- the National Security and Intelligence Advisor to the Prime Minister;
- the Deputy Minister of Justice and Deputy Attorney General;
- the Deputy Minister of Public Safety; and
- the Deputy Minister of Foreign Affairs.

# 5.0 Process

The protocol lays out a process through which Canadians would be notified of an incident that threatens Canada's ability to have a free and fair election, should notification be necessary.

During the writ period, the protocol for a public announcement would be:

1. The national security agencies will provide regular briefings to the Panel on emerging national security developments and potential threats to the integrity of the election.

2. If the head of a national security agency (i.e., the Communications Security Establishment, the Canadian Security Intelligence Service, the Royal Canadian Mounted Police or Global Affairs Canada) become aware of interference in the 2019 General Election, they will, in consultation with each other, consider all options to effectively address the interference. Barring any overriding national security/public security reasons, the agencies will inform the affected party (e.g., a candidate; a political party; Elections Canada) of the incident directly.

3. The Panel will evaluate incidents to determine if the threshold (as set out in Section 6 below) for informing the public has been met. The Panel will operate on a consensus basis and will draw on expertise from across government, including national security agencies working within their existing mandates.

4. If a public announcement is deemed necessary, the Panel will inform the Prime Minister, the other major party leaders (or designated senior party officials who have received their security clearances sponsored by the Privy Council Office)

and Elections Canada that a public announcement will be made. These leaders would all receive the same briefing information.

5. Immediately after having informed the Prime Minister, the other political parties and Elections Canada, the Clerk of the Privy Council, on behalf of the Panel, would ask the relevant agency head(s) to issue a statement to notify Canadians of the incident(s).

# 6.0 Threshold for Informing the Public

A public announcement during the writ period would only occur if the Panel determines that an incident or an accumulation of incidents has occurred that threatens Canada's ability to have a free and fair election.

Determining whether the threshold has been met will require considerable judgement. There are different considerations that could be included in making this judgement:

- the degree to which the incident(s) undermine(s) Canadians' ability to have a free and fair election;
- the potential of the incident(s) to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence or information.

The Panel brings together unique national security, foreign affairs, democratic governance and legal perspectives, including a clear view of the democratic rights enshrined in the *Canadian Charter of Rights and Freedoms*.

Although a disruptive event or interference may emanate from domestic and/or foreign actors, as a starting point, the focus should be on foreign interference. That being said, attribution of foreign interference attempts may be challenging or not possible within the timelines permitted by events, given that attempts to unduly influence the election may involve misdirection and disinformation. Further, it is possible that foreign actors could be working in collaboration with, or through, domestic actors. Ultimately, it is the impact of the incident on Canada's ability to have a free and fair election that is at issue in the determination of whether the threshold has been met, and if a public announcement is required. For clarity, Canadians – and democracy – are best served by election campaigns that offer a full range of debate and dissent. The Protocol is not intended to, and will not, be used to respond to that democratic discourse.

# 7.0 Announcement

The announcement would focus on:

a) notification of the incident;
b) what is known about the incident (as deemed appropriate); and
c) steps Canadians should take to protect themselves (e.g., ensure that they are well informed; cyber hygiene), if relevant.

# 8.0 Existing Authorities

Nothing in this Directive in any way alters or expands the mandates of the national security agencies or any other department or agency. Specifically, nothing in this Protocol supersedes the RCMP's independence.

# 9.0 Assessment

Following the 2019 election, an independent report will be prepared, assessing the implementation of the Critical Election Incident Public Protocol and its effectiveness in addressing threats to the 2019 election. This report will be presented to the Prime Minister and to the National Security and Intelligence Committee of Parliamentarians. A public version will also be developed. The report is intended to help inform whether the Protocol should be established on a permanent basis going forward to help protect the integrity of future elections or what adjustments to the Protocol should be made to strengthen it.

UNCLASSIFIED

## Critical Election Incident Public Protocol (CEIPP) – Questions and Answers

**What is the threshold for the Critical Election Incident Public Protocol?**

The Critical Election Incident Public Protocol (Protocol Group) is a mechanism for communicating with Canadians during the writ period in a clear, transparent, and impartial manner about egregious incidents that threaten the integrity of the election. The threshold is limited to addressing exceptional circumstances that could impair our ability to have a free and fair election, whether based on a single incident or a culmination of incidents.

Determining whether the threshold has been met will require considerable judgement. This is why the Government of Canada has carefully selected five senior civil servants (Protocol Group) who have vast experience in security, international affairs, law, public policy, and public safety, to bring various considerations to the decision-making table.

**Will Canadians be informed about all incidents that the Government is aware of?**

The national security agencies take all threats seriously and will work to investigate all attacks. Canadians will be informed of those incidents that meet threshold, but again, the threshold is very high.

**Does the Protocol cover domestic actors? Does the Protocol cover misinformation? Satire and Jokes?**

It does cover domestic actors. Again, engagement of the Protocol is focussed on the potential impact of an incident, not who is behind the incident.

The Government distinguishes between misinformation and disinformation. Where these terms differ is that disinformation is the malicious, intentional spread of false or misleading information to foment confusion, to disrupt or to destabilize. Misinformation, on the other hand, has no malicious intent behind it and is often the result of a lack of awareness or knowledge. The Protocol would cover incidents related to disinformation, but again, the threshold is high, and the context is important. This is why the Protocol involves the careful consideration of the Critical Election Incident Response Team.

**How can you ensure the integrity of the CEIPP when the members were hand-selected by the Government in power? How can we trust the group of deputies to inform Canadians given that they serve at the pleasure of the Prime Minister?**

We have great confidence in the integrity of Canada's public service. It has been recognized as the most effective civil service in the world.

This group of deputies has unique national security, foreign affairs, democratic governance and legal expertise, as well considerable experience. I have no doubt that

they will bring that perspective and experience to bear in this role, with the utmost of care, integrity and due diligence.

**Who is charge in the group of deputies? Is a consensus required to inform Canadians? What happens if there is no consensus? Who makes the decision?**

The group is expected to come to a decision jointly, based on consensus. If there is no consensus, there will not be an announcement.

**Is there a time limit for reaching the decision to inform Canadians?**

No. It will more important to get right than to make a decision quickly given magnitude of a potential announcement.

**When the CEIPP determines that a threat has met the threshold, does the PM decide whether or not to make the information public? Can the PM veto the decision to inform Canadians?**

No.

**What would be three examples of scenarios or situations where the threshold would be met? What is a concrete example of something that would meet the threshold?**

This is clearly hypothetical and will be highly contextually dependent, but something similar to the French Macron leak could be concrete examples of incidents we believe would meet the threshold.

Organized disinformation campaigns – whether they take the form of a deepfake or a social media campaign – that are not easily disproven, widespread, including mainstream reporting on them, could also, we believe, meet the threshold.

Again, the threshold is very high. The threshold is limited to addressing exceptional circumstances that could impair our ability to have a free and fair election, whether based on a single incident or a culmination of incidents. The incidents in question would pose a significant risk of undermining Canadians' democratic rights, or have the potential to undermine the credibility of the election.

But I really want to emphasize that the context and details will matter in making the determination of whether the incident or incidents meet the threshold, and I don't want to prejudice any decision that the group at the centre of the Protocol could have to make.

As part of our preparation for this year's election, we have and are continuing to look at a range of scenarios (e.g., diaspora coercion, deep-fakes, manipulation of politicians) to test the threshold.

**Is this going to be like James Comey announcing a week before the end of the election that there is a problem?**

This is why we are putting the Protocol in place and why we are announcing it now. We want to make sure Canadians understand how they will be informed in an incident threatens to disrupt the election. It is also why there is a group of very senior public servants at the heart of the Protocol. It will not be one person deciding what Canadians should know.

**Will this protect all/small parties, or only large parties? Does this apply only to national incidents?**

I want to underline again that the Protocol is centred on the potential impact of an incident, not who is behind the incident or who an incident affects. That said, the threshold is very high. Not all incidents will be of the magnitude that they could undermine our ability to have a free and fair election. So while the impact of an incident or group of incidents that rises to the level of threshold may be regional or national in nature, it will not address every concern that an individual or party may have.

**Which parties have taken you up on the offer for support?**

The Communications Security Establishment has offered technical support, advice, and guidance to political parties in Canada. With respect to the activities or uptake of individual parties, you will need to ask them.

**Why is the Chief Electoral Officer or the Commissioner of Canada Elections not included in the Protocol?**

The Protocol is comprised of a five-member panel of senior public servants. These individuals bring together unique national security, foreign affairs, democratic governance, and legal perspectives.

The scope of Protocol is very explicit in that it will only address incidents that occur during the writ period and do not fall within Elections Canada's areas of responsibility (i.e., the administration of the election). As such it would have been inappropriate to try to include either the Chief Electoral Officer or the Commissioner of Canada Elections in the Protocol. Their focus remains on their primary objective – the administration of the election.

The Chief Electoral Officer stated that "Elections Canada welcomes a whole-of-government approach to this important priority." We agree with the CEO in his remarks that "no single entity working alone can ensure election security." As preparation for the next federal election moves forward, Elections Canada will continue to be an important partner and will continue to work closely with the national security agencies.

**Do political parties have a role in the Protocol?**

While the parties do not have a direct role in the operation of the Protocol, I do want to highlight three things.

First, that the Protocol does explicitly include a provision for informing candidates, organizations or election officials if they have been the known target of an attack, unless there is an overarching national security reason not to do so. It also includes a provision for informing political parties, together with the Prime Minister and Elections Canada when the panel has identified a substantial threat to a free and fair election and will be informing Canadians.

Second, this dovetails with other work we have been doing to offer assistance to political parties to help ensure their own IT systems are adequately protected against malicious cyber activity. This work includes sponsoring security clearances for, and providing classified threat briefings to, key political party leadership to help them strengthen their internal security practices.

And third, we have consulted with the major parties as we have developed the Protocol.

**How will SITE feed information to the Group of Five as part of the Protocol?**

SITE brings together Canada's national security agencies – CSE, CSIS, RCMP – with GAC to address covert, clandestine, or criminal activities interfering with, or influencing, Canada's electoral processes.

SITE ensures that this work is being done in a coordinated manner that aligns with the respective legal mandates of the agencies.

Each of Canada's national security agencies have their own practices for briefing up their internal organizational structures, including the heads of those agencies, as part of their regular operational practices.

The Protocol will not change this.

What the Protocol will add to this is a process for sharing relevant information with the panel of senior public service officials who will decide if incident(s) does meet the threshold of interfering with Canada's ability to have a free and fair election.

Where national security agency heads believe that some incident or incidents could potentially pose a threat to the integrity of Canada's upcoming federal election, they will coordinate with the NSIA to brief the panel accordingly either through regular briefings or on an ad hoc basis as is required.

For example, I suspect that if we were to experience an attempt to unduly influence our election like we saw in the 2016 US General election, the members of SITE would be:

- sharing information with each other about what they were seeing to ensure a coordinated view of what was happening (again respecting their different legal mandates);

- that the members from each individual agency would be integrating that information into their ongoing work monitoring and detection work, including briefing up their respective chains; and

- where the respective head of the appropriate agency, or agencies, feel as though the information that they have leads them to believe that there may be an incident or incidents that meet the threshold – like hacking and leaking a political party's email or coordinated efforts to spread disinformation in a manner that could influence the outcome of the election in the US example – they will brief the panel accordingly.

Government of Canada / Gouvernement du Canada

Home > Democratic Institutions > Protecting Democracy

# Critical Election Incident Public Protocol

The Critical Election Incident Public Protocol (the Protocol) lays out a simple, clear and impartial process by which Canadians should be notified of a threat to the integrity of the 2019 General Election.

The Protocol includes provisions for: informing candidates, organizations or election officials if they have been the known target of an attack; briefing the group of senior public servants at the heart of the Protocol; informing the Prime Minister and other party leaders (or their designates) that a public announcement is planned; and notifying the public.

The Prime Minister cannot veto the decision to notify Canadians of a critical incident

## Panel

At the heart of the Protocol is a group of experienced senior Canadian public servants who will be responsible for jointly determining whether the threshold for informing Canadians has been met, whether through a single incident or an accumulation of incidents.

The protocol will be implemented by a five-member panel of

Canada's senior public servants.

It will be comprised of the following members:

- the Clerk of the Privy Council;
- the National Security and Intelligence Advisor;
- the Deputy Minister of Justice and Deputy Attorney General;
- the Deputy Minister of Public Safety; and
- the Deputy Minister of Global Affairs Canada.

These individuals bring together unique national security, foreign affairs, democratic governance, and legal perspectives.

## Mandate

The Protocol will have a limited scope.

It will be activated for incidents that may occur within the writ period and that do not fall within Elections Canada's areas of responsibility (i.e., the administration of the election). Incidents that occur prior to the writ period will be addressed through regular Government of Canada operations.

Having these five individuals fulfill this role is consistent with the *Caretaker Convention*. The Caretaker Convention puts into practice the principle that the government is expected to exercise restraint and "restrict itself" in matters of policy, spending and appointments during the election period, except where absolutely in the national interest.

During the caretaker period, necessary announcements are made in the name of the department to ensure a distinction between official government business and partisan activity.

The Protocol Panel will not serve as a mechanism to referee of the election.

## Threshold

The threshold for the Panel's intervention during the election will be very high. It will be limited to addressing exceptional circumstances that could impair Canada's ability to have a free and fair election.

As such, potential considerations could include:

- the potential impact of the incident on the national interest;
- the degree to which the incident undermines Canadians' democratic rights;
- the potential of the incident to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence.

The Prime Minister cannot veto the decision by the Panel to notify Canadians.

## Announcement

If the Panel determines that the threshold has been met, the Clerk would direct the relevant national security agency head(s) to hold a press conference to notify Canadians of the incident(s).

The announcement would focus solely on:

- notification of the attack;
- what is known about the attack (as deemed appropriate); and/or
- steps Canadians should take to protect themselves (e.g., ensure that they are well informed; cyber hygiene), if required.

The announcement will not address attribution (i.e. the source of the attack) and will not include classified information.

Further, while the announcement might affirm that steps are being taken to address the situation, it would not necessarily provide details of those actions.

**Date modified:**
2019-03-15

# 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

Government of Canada / Gouvernement du Canada

CANADA.CA/EN/DEMOCRATIC-INSTITUTIONS

Canada

**TRANSCRIPTION/TRANSCRIPTION**
**BRIEFING/MISE À JOUR**
**Transcription prepared by Media Q Inc. exclusively for PCO**
**Transcription préparée par Media Q Inc. exclusivement pour BCP**

DATE/DATE: January 30, 2019 9:45 a.m. ET
LOCATION/ENDROIT: NPT, OTTAWA, ON
PRINCIPAL(S)/PRINCIPAUX: Government officials – not for attribution
SUBJECT/SUJET: Embargoed technical briefing prior to an important announcement regarding safeguards to Canada's democracy and combatting foreign interference.

**Moderator:** Bonjour et bienvenue à cette séance d'information concernant l'initiative pour protéger la démocratie. Thank you for taking the time to participate in today's technical briefing with regard to protecting democracy initiative. My name is (government official). I'm with the Privy Council Office and I'll be your moderator today for the tech briefing. La séance d'information sera donnée par des représentants du Bureau du conseil privé, des Affaires mondiales Canada, Services canadiens du renseignement de sécurité et le Centre de la sécurité des télécommunications, la Gendarmerie royale du Canada et Patrimoine canadien.

We will begin with a presentation by (government official), the Assistant Secretary to the Cabinet of the Privy Council Office, then open it up for questions for media in the room and on the phone. Other representatives from other departments are available to answer questions as well.

Please limit yourself to one question and one follow-up until everyone has had an opportunity to ask a question. Donc un petit rappel de vous limiter à une question et un suivi. N'hésitez pas de poser vos questions dans la langue de votre choix. I wish to remind you that this briefing is for background only, not for attribution and under embargo until the ministers make the announcement shortly after this technical briefing. Un rappel que cette séance est tenue à des fins d'information seulement et on d'attribution, et frappée d'embargo jusqu'au moment où les ministres feront l'annonce suite à cette séance.

We're now ready to begin our briefing and I'll turn it over to (government official).

**Government official 1:** Merci, (government official) et bonjour tout le monde. It might not be everyone's cup of tea but I feel quite comforted having officials from CSE, Canadian Centre of Cybersecurity, CSIS, the RCMP, Global Affairs, Canadian Heritage and PCO as well. I want to thank them for their hard work in getting this initiative to its fruition and actually for their ongoing work protecting our democracy.

Comme (government official) a mentionné, cette présentation technique vise à appuyer l'annonce des ministres Gould, Goodale et Sajjan concernant les efforts du gouvernement du Canada pour protéger la démocratie canadienne avant les élections de 2019. Des efforts d'ingérence par des acteurs étatiques et non étatiques dans les

processus démocratiques ne sont pas des nouvelles menaces. Ce qui est nouveau, les nouvelles technologies Web offrent des opportunités et moyens novateurs pour interférer à une vitesse et sur une échelle sans précédent.

Les gouvernements et les citoyens doivent se préparer pour affronter ces défis et en respectant nos droits et libertés démocratiques. Nous devons préparer nos citoyens et nos systèmes pour faire face à cette menace. Prochaine dispositive.

Les préparations canadiennes tirent parti de l'expertise pangouvernementale. Comme vous pouvez le constater, il s'agit d'un effort pluriministériel. Nous avons également travaillé de façon productive avec Élections Canada et les commissaires à l'élection fédérale. As election 2019 approaches, we have been watching and learning from other countries. We've made our own assessment of Canada's readiness and created a meeting-Canada approach which we are laying out today. Next slide.

Pour lutter contre une menace aux facettes multiples, il faut une approche polyvalente. Le cadre d'intervention compte donc quatre piliers :
améliorer la préparation des citoyens;
améliorer la préparation des organisations;
compter sur les entreprises de médias sociaux faire le pas; et
lutter contre l'ingérence étrang re en partenariat avec nos alliés.
Next slide, please.

The government has been advancing work under each of these four pillars from the beginning of this mandate. Some of the highlights include CSE's public threat report on threats to Canadian democracy which was first released in June 2017 and which is in the process of being updates in advance of this year's election. There's also been the establishment of the Canadian Centre for Cybersecurity to bring Canadians cybersecurity resources together in one spot and to add those resources. This was part of budget 2018.

The security intelligence agencies have also been working directly to support Elections Canada and have deployed cyber defences to protect Elections Canada cyber infrastructure. This has been underway for a few years now and has been the subject of close collaboration between Elections Canada and the national security agencies. There's also been engagement with parliamentarians, the parties and provincial officials on the cyber threat so they can protect themselves. And more generally – and this is part of our message – is that the activities of the national security agencies adjust and react to the evolving threat on a daily basis. It's part of their ongoing work and continues to this day and will continue up to the election 2019 and beyond. Next slide, please.

Recent amendments to *The Canada Elections Act*, Bill C-76, strengthens Canada's ability to act in the face of interference attempts. New provisions which will be enforced by June 2019 – and some are in force now – also provide the Chief Electoral Office and the Commissioner of Canada Elections with new enforceable powers. In the case of the Commissioner, he has the power to launch investigations and compel testimony. In the

case of – these are just for instances – and in the case of the Chief Electoral Officer, he has a broaden educational mandate which is in place now, I believe.

There is also requirement in the legislation for the social media platforms to create an ad registry of all partisan ads during the pre-writ and writ periods. On this, Canada is one of the first jurisdictions in the world to require this as part of their elections. Next slide.

On top of that, Canada is taking a sweeping series of new measures to protect the 2019 general election. Let me just run through them quickly. So leveraging the newly established security and intelligence threats to election task force, to improve awareness of foreign threats and support assessment and response. This is quite an unprecedented collaboration between CSE, CSIS, GAC and the RCMP. So that's a mouthful of acronyms. So Canadian Security establishment, Canadian Security and Intelligence Service, Global Affairs Canada and the RCMP.

There's also a Canadian Heritage-led creation of a digital citizen initiative to expand citizen-focused programming on resilience against disinformation and supporting a healthy information ecosystem, and the call for proposals goes out today, synchronized with the announcement. There's also the establishment of the Critical Elections Incident Public Protocol. This is a new mechanism for informing and notifying Canadians during the writ period in a clear and impartial manner should there be incidents that threaten to undermined the conduct of a free and fair election.

In addition, national security agencies are offering additional cyber technical advice, guidance and services to political parties to inform their cyber practices and security. In addition, the government of Canada will be offering in-depth classified threat briefing to key leadership and political parties again by the national security agencies to promote situational awareness and encourage them to strengthen internal security practices and behaviours. Another element of the initiative is the RCMP has formed a foreign activity interference team to investigate and disrupt criminal acts conducted as part of the interference.

A couple of other things. Global Affairs Canada recently activated its rapid-response mechanism to strengthen coordination among G7 democracies in responding to threats to democracy and monitoring malign foreign actors in the social media space. So looking externally at social media action that kind of comes to Canada and might be maligned in intent.

In addition, Minister Gould is engaging with digital platforms to implement specific measures to increase transparency and combat the spread of disinformation. As mentioned earlier, we only have in coming months CSE will release an update to its cyberthreats to Canada's democratic process report to help them inform Canadians of the risk at play. And we're also leveraging CSE's Get Cybersafe Campaign to build Canadians' awareness of cyberthreats in order to improve their cybersecurity and offer ways in which they can better protect themselves.

So as you can see, it's an extensive set of new measures coordinated across government that will be put in place in advance of the 2019 election. So next slide, please.

Just by way of wrap-up, it's a dynamic threat environment. We all know this and so Canada's response has to be dynamic as well. It will continue to evolve as the threat evolves. One of the things to point out is that we're regularly internally testing our capacity and we'll continue to probe using scenarios and practise and refine our approaches.

And finally, just to say that all Canadians have a responsibility to help ensure Canada has a free and fair election in 2019 and that starts by being a critical co-consumer of media and having good cyber practices online. Thank you for your time. We'll be happy to answer your questions.

**Moderator:** And we will now take questions from the room first. We'll follow those by an opportunity for those who have joined us on the phone ask questions as well. Donc on procède maintenant à la période de questions débutant ici dans la salle et ensuite au téléphone.

**Question:** How much is this dependent on Bill C-59 getting through the Senate. There's many changes that are coming to (off microphone), all the security protocols, let's say the CSE can do. How much of this plan can be independent of any pending legislation?

**Government Official 2:** So it is important that C-59 pass and Minister Goodale, I'm sure, would be pleased to speak to that. But for this set of initiatives, they're not dependent on C-59 at all, I believe. Just checking with my colleagues. There's nothing here that – that we've announced in this that is depending on the passage of C-59.

**Government Official 2:** No, that's fine. I mean from the security and intelligence component, a lot of that leverage is our existing mandate and intelligent collection and investigative capacities. Global Affairs has already set up the rapid-response mechanism as part of the G7 commitment and all of that is not dependent on new authorities and C-59.

**Question:** What about – now, you're going to have Elections Canada with new invested powers and also ---

**Government Official 2:** The Commissioner. The Commission of Canada Elections, Yves Côté.

**Question:** Simply the Commissioner?

**Government Official 2:** Yes.

**Question:** So this is a new role for an organization that hasn't traditionally taken this sort of thing. They haven't been exposed to foreign election interference or even election interference from actors that could be within Canada as we saw with Karim Baratov who was charged in the Yahoo hacking. So is the Commissioner prepared? Are the tools there to coordinate with Elections Canada and these other national security bodies in a very untraditional role for this organization?

**Government Official 2:** So the Commissioner of Canada Elections, as you quite properly point out, does have new powers. First is the power to initiate investigations. So in the past in previous elections he had to wait for a request before he could launch an investigation. Now, if he sees something that he is worried about, he could launch an investigation. The second feature is that he could compel testimony which is an enhanced power.

This was thoroughly vetted as part of Bill C-76 through PRAC (sic). It's a power that in fact I believe the Commissioner is on record as saying that he welcomed and thought it was a good thing. In terms of the coordination, I'm not sure that coordination is quite the right word. I mean the Commissioner has independent powers and would use those powers. There might be some sharing of information, but I don't see it. Coordination suggests that they're working actively together. The Commissioner of Canada Elections is independent and has an independent mandate that has since been enhanced.

**Question:** (off microphone) Who within national security organizations is really vested with monitoring any type of online foreign interference or any type of electoral interference? You know that could happen. I don't think that this is something that the Commissioner will necessarily be able to recognize. I guess it'd have to come from experts who say, oh wow, there's a foreign act (sic) that could be influencing the strange Facebook campaign like we see in the United States.

**Government Official 2:** So I think you'll appreciate it's quite context dependent, but I think depending on the nature of the incident you could see that CSE might have a role. It could be that if there's a human intelligence – so particularly if there is an external foreign interference coming into Canada you could imagine CSE. You'd imagine that the rapid-response mechanism would notice some of that because they're monitoring it together with international allies. So they could be involved with identifying it. If it's a human intelligence element then you might find that CSIS would have part of it. And all within their existing mandates.

**Question:** But I guess that's why I'm asking about coordination. So these national security organizations may – like what happened in the United States. The FBI knew about. The Russian activity with the election, but Mr. Comey (ph) decided not to act at the time because of – well, I guess we'd have to ask Mr. Comey.

**Government Official 2:** Right.

**Question:** Is there going to be some sort of mandate where if there is something noticed by national security organizations they have to notify. The Commission just started (of microphone).

**Government Official 2:** No. It's an important point. Part of it will depend on the timeline. So when is this happening? So if it's happening within – after the dropping of the writ during the election, then the national security agencies using their existing – in their existing mandates and roles would be required to inform the protocol group. So this is a new part of the – that's being initiated today that sets up five public servants, five senior public servants to assess whether or not there has been a – if I can use your language – a Comey-like incident, and whether or not it's something that impairs the development of a free and fair election in Canada.

So the national security agencies, your point is coordination, like who do they tell? If it's during the writ period, they tell the protocol group. If it's outside the writ period, so regular government operations apply and it would be the minister and the prime minister who'd be informed.

**Moderator:** Raymond?

**Question:** (off microphone) des mesures que vous annoncez aujourd'hui.

**Government Official 3:** J'aimerais commencer par vous dire que les mesures ça se passe depuis longtemps. Je peux vous souligner le 155 milliards qui a été investi dans le Centre canadien de la cybersécurité. Aujourd'hui aussi, on annonce 7 milliards de dollars envers des projets et des programmes de littératie civiques et pour supporter les Canadiens pour être plus informés et plus critiques dans la lecture d'information.

**Question:** Donc le total de l'opération pour la prochaine élection, vous diriez que c'est combien?

**Government Official 3:** C'est difficile de mettre un numéro là-dessus. On a fait beaucoup d'investissements au cours de plusieurs années. Aussi, on a fait beaucoup de priorisation interne pour bouger des ressources de certaines priorités vers celle-là comme on note que c'est une priorité importante. Donc c'est difficile de mettre un numéro fixe là-dessus.

**Moderator:** Rita?

**Question:** So talk about this new critical protocol and you know some egregious incident and there's to be a threshold. Can you give us a sense like what meets that threshold? When – if that's a high bar, what's an egregious incident that would kick that into action?

**Government Official 2:** So you'll appreciate that's very context dependent. It's got to be something disruptive that impacts Canada's ability to have a free and fair election. I would note that it was developed with an understanding of what's happened in other countries in mind. So something that certainly would be considered by the protocol group would be, let's say – and this is really not – we're really talking about something like a regional, national scale.

Something like, you know, has occurred in France, hacking or leaking a party's email, and the seeding of phony emails. It could also be a deep faked video that goes viral. It could be calculated disinformation campaign that comes from overseas that is spotted. It'd be very context dependent. I would say that it's important that the threshold be high. That you know as you folks know better than I, you know, elections are very rough-and-tumble things. We're not -- there's no -- no one is monitoring, you know, the election you know elections will continue to be rough and tumble, but what we're looking at is foreign interference, disinformation campaigns on the scale on what we've seen in other countries.

We think it's important to – if that should happen – that the threshold be exceeded that Canadians be informed of what's happened. That they understand and that they, you know, are able to take corrective actions in knowing that in fact this is disinformation and should be ignored.

**Question:** So follow to that – a two-prong answer to the question. Who determines whether it meets that threshold or not? Who ultimately makes the call for that? And also, is there (inaudible) however that in some of those cases that we've seen overseas, people didn't realize how big it was until it had an actual impact on the election. Like it was after the fact that we realized how big things were. So in the moment, you might not realize it. So how is that going to be – how can you deal with that? And who makes that call?

**Government Official 2:** Yes, ok. So I'll take them. I think they're key to the protocol. So the five people who will form the protocol group are the clerk of the Privy Council and Security to the – and Secretary to the Cabinet; the National Security and Intelligence
Advisor; the Deputy Minister of Justice who's also Deputy Attorney General of Canada; the Deputy Minister of Public Safety; and the Deputy Minister of Global Affairs Canada.

And I think it's important to take a moment just to explain why those people were chosen because there's some important reasons which are based in our system of government that made them the right choice. The first is just their knowledge base. So these are folks who would have detailed knowledge of national security issues. They'd have detailed knowledge – as a group – detailed knowledge of global affairs and foreign affairs; detailed knowledge of issues of democratic governance and detailed in-depth knowledge of rule of law, including the Charter of Rights and Freedoms.

So they have that knowledge base. They would come at it with that knowledge base and it would allow them to be informed by it. The other thing is just their experience, right. These are, as you can tell, Canada's finest public servants. They're used to – and this speaks to your second question – they're used to making quick decisions and they're used to dealing with imperfect information.

**Moderator:** Marie, prochaine question.

**Question:** If you could just – in terms of the ---

**Government Official 2:** Yes. So part of what we're trying to do in the protocol – actually, if I could say one more thing about the group. In our system of government, it's a Westminster system and during the election time period, a caretaker convention is in place. So public servants, particularly senior public servants, have the responsibility for the continuity of government. And so that makes them the appropriate group in our system of government to take the lead. And as non-partisan officials, they're also the appropriate group to take the lead.

On the second part – and I'm sorry, I've, gone too long – on the second part of your question, it's true we won't know everything at the moment something's happened. There will be most likely a faw (sic). You know, we won't know all the pieces. We may not know who's doing it. Sometimes our experiences we look to other countries as that can take weeks. It can take months. But what we can do is note the disinformation. We can inform Canadians to the best of our knowledge and understanding what has happened and what they can do to protect themselves. And that's what we're trying to do in this case. Sorry for the long answer.

**Moderator:** Marie.

**Question:** Oui, je voulais continuer là-dessus. Can I ask my question in French? You can answer in English if you need to.

**Government Official 3:** Oui.

**Question:** Would you understand French?

**Government Official 2:** Yes.

**Question:** Pour continuer là-dessus, comment est-ce que vous envisagez cette prise de décision là du *threshold*, de la différence entre, ben, c'est juste une vidéo virale sur Facebook ou c'est carrément une tentative – ou soit une tentative d'influencer l'élection ou quelque chose qui a le potentiel d'effectivement avoir cet effet-là? Comment est-ce que vous envisagez le *tipping point* dans le fond que ces cinq personnes-là doivent mesurer?

**Government Official 2:** It's going to be very challenging. It's why we picked people of extreme – who have nuanced understanding of our system of government; who have nuanced understanding of issues around rule of law and national security issues. Because – I mean, one of the considerations is just the call of the information, right. A lot of what will go into their decision making will be kind of a scale in scope. Is this something that's truly impacting the course of the election or is this something that's here today and gone tomorrow?

So they'll have to make what is a very difficult decision of whether this merits an intervention which itself affects the course of the election. So it has to be something significant. It's not something that is, you know, seen by a very small number of people. That would not make the threshold. Our hope is that the protocol does not have to be initiated at all. So that would be our hope in this.

**Question:** If I can just change tracks just for a second, because there is the G7 group and it mentions international interventions. Like a coordinated – can you just explain?

**Government Official 4:** Yes. So I think actually we've got an expert from Global Affairs on the rapid-response mechanism. But just to say that this comes out of the Charlevoix conference and it's a way of bringing together G7 countries to share best practices and share real-time information on external foreign interference threats. But (government official), why don't you take it away.

**Question:** C'est dans quel contexte que vous voyez une intervention internationale?

**Government Official 4:** So for the protocols that have been developed for the rapid-response mechanism should anyone member of the G7 determine that there has been a level of activity that they're concerned about, they can request coordinated action by the G7. This would be something that would also take a longer timeframe because this is done by consensus within the G7. So we've seen the G7 issues statements in the past. So it is a longer process, but it's another tool in our – at our disposal that we can actually make stronger statements to call out action in an international arena on behalf of the G7 community.

**Question:** But I mean other than a statement (off microphone)?

**Government Official 4:** Well, the – what we envision is that in all likelihood it could be coming out as a joint statement depending on the activities. It would then be at the national discretion of each G7 member what additional activities they want to take. So for example, if it was triggered or requested by Canada, we may have a higher level of action that we want to take. But not all G7 members are bound to take the same actions.

**Moderator:** Elizabeth?

**Question:** Social media giants, the Facebooks, the Twitters, etc. what has their attitude been? And have you been dealing with them, coordinating with them as you've been preparing this?

**Government Official 2:** So they of course were impacted by Bill C-76, *The Elections Modernization Act* and the requirement to have an ad registry. In addition, Minister Gould has commenced discussions with the social media platforms to kind of lay out her expectations and the government's expectations that the best practices that are being developed around the world in response to these sorts of foreign interference would be brought to Canada in advance of the 2019 election.

**Question:** If you take a look recently – for up until recently, pro-public and a couple of other places had built – had collectors that – where they could scoop up the ads as they were being seen by Canadians, for example. It was (inaudible) for us at CBC in the Ontario election for example. Facebook has just broken it because it was – and I know when I dealt with Facebook, there were groups that were registered, who were placing ads. Facebook wouldn't reveal who was behind those groups. They wouldn't reveal where the money was coming from or even whether it was coming in Canada. Does – how does that square with the fact that they're now supposed to be cooperating with you?

**Government Official 2:** So I expect – and Minister Gould will be speaking with Facebook to have better understanding the reasons behind their actions. On top of that, I mean this development which is very recent, as you know, I think helps underscore why it's important that we are requiring an ad registry as part of Bill C-76 and as part of Election 2019 in both the pre-writ and the writ period. So there is a requirement built into legislation. Canada is one of the few jurisdictions that has it currently. So inaction like that by Facebook underscores the need to have legislation.

**Moderator:** Alex.

**Question:** One of the weakest links in this sort of – is actually the media and political parties. I'm wondering if there is any thought given to outreach to put the parties and the media about, you know, protocols in terms of how we proceed with document dumps or anonymous tips or that sort of thing. Is there any sort of liaison capability?

**Government Official 2:** There is. I mean there has been engagement with the political parties on the protocol. There has been a briefing of them. They are part of the protocol, by the way. So should it be decided by the five protocol group that the threshold has been exceeded and there is a need for a public announcement, the political parties will be informed in advance, the major political parties will be informed in advance as part of that.

In terms of outreach, we have done some quiet things. We recently had some reporters from – I believe it was NATO – who came and shared their experiences with disinformation here in Ottawa. But you're quite right, that's the sort of thing that we should continue doing and it needs to accelerate in advance of the election.

**Question:** So have you done any outreach to publishers, to media executives, that sort of thing?

**Government Official 2:** Not so far.

**Question:** Not so far. Is there a plan to do that?

**Government Official 2:** No. It's not part of this announcement.

**Question:** Outside of the writ process, is this task force or group of five going to remain active and perhaps disclose other, you know, hacking attempts, nation-state-backed hacking attempts?

**Government Official 2:** No. The protocol group only exists during the caretaker convention period which is from the dropping of the writ to the election. Of course, I mean they will have to be active in the sense of – they will have to be briefed in advance of the dropping of the writ, but they won't be actively deciding anything. And if something were to happen outside the writ period, it'll be just through normal government operations that the writ would follow.

**Question:** The reason I ask is because some people feel non-partisan public servants only disclosing cyber attacks in the course of an election, you know, might give the sense that they're actually influencing the election rather than if this was a normal you know, matter-of-fact process where anytime there is a major cyber attack or disinformation or influence campaign, you know, that would be disclosed as a matter of fact.

**Government Official 5:** I think it's just a question of when the government is in place outside the writ period, it's appropriate that the government make that announcement and it's only in the exceptional circumstance of the writ period that would have you issue or initiate the protocol group. Of course, public servants might be involved in any announcement outside the writ, but -- (government official), you want to jump in?

**Government Official 6:** Yes, maybe I'll jump in. It's (government official). I'm responsible for Operations at the Canadian Centre of Cybersecurity. And I think it was one of the investments that was highlighted by Asia (sic) as has been done before. I think it's important to notice that many of the things that are presented today and were refocused for this upcoming election are actually part of working groups and efforts that look at democratic processes at large.

So we're all focused on the federal elections that are coming up soon, but there are elections ongoing in Canada 12 months a year. So many of the activities that you're hearing about today continue and persist. From a cybersecurity perspective, of course we report. We make people aware of what's happening on all the thresholds that are relevant and if it has to do with foreign influence or interference, it would just be the normal course of activities, also something we report.

**Moderator:** Ok. So we're going to Campbell and then we'll go to Julia.

**Question:** Experience has shown that these things – foreign interference in election campaign and political processes aren't always critical events like (inaudible) hack for something larger that may be concerted networks spreading messages that are disruptive towards the – what we saw in the United States. And they're not necessarily partisan either. They don't necessarily reach the definition of partisan advertising. So if the government of Canada finds, believes that there is a foreign network spreading politically oriented messages in Canada, will they tell us? Will they tell Canadians? Do you have a way to map that? Or alert people?

**Government Official 2:** So what you're speaking to is it might not be overtly partisan in that it supports one part and over another but it might be highly disruptive setting one group of Canadians against another group of Canadians. So the key issue – and that's classic disinformation actually – this could be a situation. It depends on kind of the level of impact but it is exactly the sort of thing that would – could meet the threshold. If it's highly disruptive. It's Canadians and thereby impairs our ability to have a free and fair election, whether it advantages one party or another is not as important as the disruptive effect. So very much so the threshold could be engaged in the scenario you outlined. Sorry, (government official) you wanted.

**Question:** That's what I'm asking. You know such a network exists or appears to exist, can you inform people even if you don't feel – should you not inform Canadians even though you don't feel it needs – a threshold and disrupt – we expect transparency in our elections and that kind of network operates in the shadows.

**Government Official 2:** So I mean one of the comments I can make is that foreign interference as a concept even outside elections is not something new to security intelligence and law enforcement agencies. What we're doing in the lead up to the election and the security and the task force that we've set up is to try and bring some people from those agencies together to really focus our efforts and make sure we have proper protocols, information sharing. But it draws upon an expertise that exists in each of those agencies that pre-existed for a long time.

So those networks you're talking about with respect to foreign interference are things that we have some expertise and we'll continue to track. When we have hit thresholds for public attribution of certain things in the past, for instance in malicious cyber activities that the Cyber Centre has named particular actors and particular countries, not specifically in the context of elections, but we do make those decisions when we can. But they have to be done carefully and after detailed analysis and considerations.

So it's very much case by case when and what the right thing to do is when we see those activities.

**Moderator:** Julie.

**Question:** Which malicious foreign actors are you most worried about?

**Government Official 5:** This whole government approach is neutral as the source country. It's the threat that matters not the country.

**Question:** (off microphone) malicious foreign actors. I want to get examples. What are you thinking?

**Government Official 5:** We're thinking of any foreign actor that could impair the safe conduct of the Canadian election.

**Question:** So nobody really is on your radar?

**Government Official 5:** I think it's fair to say, you know, just based on my last comment – the source is less important to us than the potential for interference. And so, anything that's covert, clandestine and criminal is going to be on our radar. The attribution of those activities to specific countries again has to be carefully analyzed and considered. It's not something I can responsibly talk to today, but if we hit that threshold where something needs to be made public in the interest of Canadians, the group of individuals who will be meeting during the writ period will do that.

**Question:** Were there foreign interference in the last election?

**Government Official 6:** What we've been monitoring in fact is all the previous elections. As you know in public source there had been reported interference around the world in elections. What's worrisome and we've seen a trend in the last few years and in fact an increase in that form of interference. And this is why you're seeing these measures being put in place today.

Now, in the last Canadian federal election, there were no activities that were observed that would have put into question the validity of our elections. Not at all. There were some minor pockets but nothing that crosses a threshold of concern. But what's more worrisome again is the world trend and that's why you need to take measures and be proactive and put preventions in place. And all those measures are about being ready for something that's occurring in 910 (sic).

**Question:** Have we had any foreign interference in any Canadian election recently? Provincial or anything, or is it the world trend that we're most concerned about, but nothing specifically has happened?

**Government Official 5:** I think that's actually a pretty fair statement. If we were just judging by 2015, we wouldn't be doing this extensive set of measures. It's because we are looking around the world at the experience of other democratic countries that we've felt the need as a government to take these – in some cases quite remarkable steps.

**Question:** Give an example. Anything that's gone on here provincially, municipally, federally?

**Government Official 2:** I think a good source to look at would be – we see this – the Cyber Centre did a report last year on threats to democratic processes and it mentions a little bit about that and there's some vignettes in there about the types of things that we see. It's a good reference place. But in terms of specifics of our current operations, I don't think we can speak to that.

**Question:** I have a question about the obligation of the social media platforms because that is such an important part of disinformation and disruption. I know there is a legislation requiring the ad registry. What's the obligation on Facebook, Twitter or whatever during the writ period if their platform are seen to be the vehicle for disinformation and manipulation? How do you deal with them and what can they be compelled to do?

**Government Official 5:** So that's exactly the sort of conversation that Minister Gould is having with the social media platforms right now. Obviously, they're adapting to this new world as our governments. So part of what we're saying, and just to repeat it, is they're providing these new practices elsewhere in the world in response to specific threats. What Minister Gould is setting out is a government of Canada's expectation that those best practices come to Canada.

**Question:** (off microphone) good faith obligation right now because you know they're international in their scope? Is that a good faith obligation or will there be a legal compulsion baked into the rules that forces Facebook to be a good faith actor?

**Government Official 5:** So it will depend on the discussions that there had. So those are ongoing. Our initial indications with the difference social media platforms has been positive. They're seized with the issues. They are making some changes and that's part of what the discussion that Minister Gould is leading will determine.

**Question:** But simply, I guess, timeframe with the elections set for October, if you can't reach or can't good faith consensus, if Minister Gould can't convince to buy into Canada's vision obviously there's not enough time for legal changes (off microphone) get something done before the election?

**Government Official 5:** It will depend. Like it – I think that she's in the midst of our conversations right now. She's going to push them. She's going to lay out her expectations of the government of Canada and we'll see where those discussions go.

**Question:** One question on the protocol group and whether it meets the threshold for disruptive and a critical sort of incident. It sort of feeling like Campbell said. A lot of it is repetition of small things that in their totality (crosstalk) disruption. So how quickly can the protocol group – how does it deal with that? You know obviously if it's a big giant thing that becomes fairly obvious process, but the micro manipulations, how do you deal with that?

**Government Official 2:** So both are in scope. It can be a single incident or it can be an orchestrated set of small incidents. It doesn't matter. It's the impact it has on whether Canada can have a free and fair election that matters.

**Question:** If you see enough of it, you go with it?

**Government Official 2:** Yes.

**Question:** J'aimerais justement avoir plus de détails là-dessus. Qu'est-ce que vous considérez comme une élection libre et juste? Qu'est-ce qui fait que c'est possible d'avoir un exemple plus précis de critères qui va guider ces cinq personnes à agir ou pas à informer les Canadiens parce que ce sont de très bons principes? Mais concrètement, ça veut dire quoi? À quel moment ils se disent bon ben là on est ---

**Government Official 3:** Donc le groupe de cinq personnes vont être informés par les renseignements qu'ils reçoivent de nos agences de sécurité nationale. Cette décision demande beaucoup de jugement de leur part et ça va dépendre de leur jugement. Il y a un groupe de cinq personnes donc c'est une décision qu'ils vont prendre ensemble. Et le critère c'est que les Canadiens ont tous la même opportunité pour faire un vote libre et sans préjugé.

**Question:** Et au niveau – pas de critères précis d'établis? Pas déterminés?

**Government Official 3:** Non. Le critère est très clair. Le seuil d'intervention c'est une élection libre et juste.

**Question:** Pis qu'est-ce que – mon collègue Davis vous posait des questions là-dessus. Qu'est-ce que vous vous attendez en attendant de Facebook, de Twitter, des gens, des médias sociaux? Est-ce que vous vous attendez à ce qu'ils soient plus fermes envers ce qui se passe sur leurs plates-formes? C'est quoi l'objectif du gouvernement, parce que là les discussions sont portées mais vous voulez atteindre quel stade d'engagement de leur part?

**Government Official 3:** Je dirais on espérait qu'ils continuent à renforcer leurs termes et conditions que les plates-formes ont déjà en place. Et qu'ils soient des bons partenaires avec le gouvernement. Les discussions comme mon collègue a dit sont en cours maintenant. Donc ce serait difficile de préjuger ces discussions.

**Moderator:** Mike at the back and then we'll take questions from the phone after this.

**Question:** So just sort of building on one of the couple of other colleagues who have said given that this is never really one big even, because that one is obvious, and given that it is ongoing, was there any thought in having this group formed for a longer period other than the writ period so they could continue to monitor this and continue to be at a bit of an arms' length from the government?

**Government Official 5:** So the protocol group is established just for the writ period. They will receive briefings of the state of play. So if your concern is that they're a bunch of things that happened just before the writ period and they don't count towards the establishment of the threshold, I think that's not true. They would be considered as part of the state of play of the election.

**Question:** I guess what I'm saying is because everybody would say the campaign is well underway in the House of Commons or elsewhere you know, one would think that just the writ period ---

**Government Official 5:** I guess ---

**Question:** Really short period.

**Government Official 5:** So what I'd say is that before the writ period it's regular government operations that apply. So if there was something that happened say in June then you know ministers would be informed, the prime minister would be informed and action would be taken. (government official) would you?

**Government Official 2:** Just to clarify. I think this is what (government official) was saying too but you know security and intelligence agencies will continue to advise people like the national security advisor and that group of people during regular government operations before the writ period. So the information that they're going to receive even after the writ period starts will not be new to them. Security and intelligence agencies are routinely briefing people like this.

**Question:** You don't typically name bad actors? I mean when you named Beijing a couple of years ago that was very rare. So I think, Mike, if I could the question is you know you see hundreds of cyber attacks every week and you don't name actors. To suddenly start naming them during the writ period I think would cause some people to think maybe there's you know politics being played.

**Government Official 5:** I think – so there will be an update to cyber threats to Canada. It's – the report exists from June 2017. There will be an update in coming months. So that'll give Canadians a good sense of the state of play as we know it up to that point. If something occurs prior to the writ period, it will be deal with through regular

government operations. I'm not sure we can – I don't want to set your expectations too high that if a threshold is set and passed and something is announced that that day the finger will be pointing to one or another malicious actor, it may not be possible. It can take a period of time for that to happen and just you know if it's in the writ period, it's between 35 and 50 days now.

So if you had something happen mid-campaign, chances are the best you could do is say this is false. Here's how you defend against it. This is disinformation. But you may not be able to say this is caused by that group or another group. That will take forensic assessment.

**Government Official 6:** Let me just jump in to your comment of attributions. I understand the appetite for consular (sic) attribution. Attribution is a tool in a basket of measures that we use. You have to be diligent when you use that tool to have the effect that you're trying to cause. If you over use the tool of attribution it becomes noise and it becomes irrelevant. People get accustomed to the practice and it doesn't have any effect.

So while you're seeing the government choose to use that tool at very specific moments to cause a specific effect and use the fact that it's unique and it does not happen frequently as a signal that this more important and something needs to be done. So it is part of that escalation. But there are – you can never forget – and of course it's not in the regular discourse but a number of measures that we take – that are in place that we take every day and they go back to the – it's a collection of events and it's the sum of events, absolutely. And we report all these events and we monitor all these events.

And it's the sum of these events that make the determination that sometimes we do go to the attribution threshold, if you wish.

**Moderator:** Donc on procède maintenant avec les questions au téléphone. We have questions on the phone, please.

**Operator:** Merci. Thank you. Please press *1 at this time if you have a question. Veuillez appuyer sur *1 maintenant pour poser une question. There will be a brief pause while participants register for questions. Il y aura un court délai vous permettant de vous enregistrer dans la file d'attente pour les questions. Our first question – notre première question – is from Dylan Robertson (ph) from the Winnipeg Free Press. Please go ahead. À vous la parole.

**Question:** Hi there. You've spoken a bit about the social media platforms and the (inaudible) discussions. I'm more curious is if you guys have spoken with the social media platforms, if you could name the names and if they've been helpful because it seems like they haven't really been before permanent committees or other government? Who have you spoken and have they actually provided information? Or been abstinent about it?

**Government Official 5:** So they haven't been abstinent about it or else the discussions wouldn't be continuing. But I think it's premature to kind of say very much because those discussion are ongoing. (Government official), do you ---

**Government Official 6:** Maybe I can add in a cybersecurity context, we talked to all companies that are in the Canadian ecosystem and expect some behaviour. I think in fairness to social media platforms, they have taken some steps in recent years. They have taken some of their social responsibilities. Many have cleaned up their terms and conditions for the user terms and conditions and are taking action for the misuse of their platforms.

Ultimately, they're private sector entities. They have reputation to maintain and I think in any event or unfortunate incident during elections or in the course of the year, if we chose to attribute something to a platform this would be something that would be really bad to them. So they're not unlies (sic) to those – to the criticality of their actions and I think we're seeing improvement over time.

**Moderator:** Do you have a follow-up?

**Question:** I also want to ask about the (inaudible) if you guys have a policy in place or you know have you heard anything from that? What happens with MSM (sic) the media (inaudible) a fair bit understand? Do you guys have any sort of things to prevent that kind of disaster from happening again?

**Government Official 5:** We have nothing to add on that subject.

**Question:** Like nothing learned from it?

**Government Official 5:** Nothing to add. This is not the group to discuss that.

**Moderator:** Take the next question on the phone, please.

**Operator:** Thank you. We have a question from Catherine Twuney (ph) from CBC News. À vous la parole. Please go ahead.

**Question:** Hi, thank you. I'm just looking at this incident protocol page – we're talking about if the panel finds that there is a threat that it will inform the prime minister, all the party officials and Elections Canada of the incident and then a press conference will be held, sorry. How can you ensure that this process doesn't become muddled by partisanship if you're alerting the parties and the prime minister?

**Government Official 5:** So the – it's we can give you that assurance because the purpose of alerting the prime minister and alerting party leaders and alerting Elections Canada it's just for information. There is no decision making by any of those groups. It's determination by the protocol group that there will be an announcement and it's simply for information alerting of that prospect.

**Moderator:** Follow-up, Catherine?

**Question:** Yes. A follow-up on a previous question about accountability. After the election will there be any kind of public report or any kind of briefing on how this protocol when and what was discussed? Will we have a sense of, you know, how close they came to maybe making an announcement? Those kinds of things.

**Government Official 2:** There will be an assessment as to whether the critical election is in a public protocol served its purpose properly. So there will be a hot wash or an assessment and we'll look, as we always do, to improve.

**Moderator:** We'll take one more question.

**Question:** Will the assessment made public?

**Government Official 5:** I can't say at this point, but there will be an assessment.

**Moderator:** And we'll take one more in the room here. I think that'll be – that's it for time. So way in the back row.

**Question:** I'm just wanting to clarify that you talked about foreign interference, but what about domestic? If you have domestic malicious actors who are trying to disrupt or you know put out messages that just exacerbate divisions, intentions and that kind of thing. Can you deal with that?

**Government Official 5:** If there was something that came to the knowledge of the protocol group that is more domestic in nature that had the attributes of disinformation, then it is something that would be considered for the threshold. It's the impact on the conduct of a free and fair election that matters most, not the source.

**Question:** But domestic and foreign?

**Government Official 5:** Yes.

**Moderator:** Follow-up?

**Question:** Just to clarify. So protocol only in elections, but then the site, the security threat intelligence before election ---

**Government Official 2:** It's up now.

**Question:** That's running all the time.

**Government Official 5:** Yes. Absolutely.

**Question:** So have you actually come across anything that you're going to inform the ministers, the prime minister and ---

**Question:** Who's on site? Who's on the site?

**Government Official 1:** Yes, so the task force brings together Global Affairs, CSIS, RCMP and CSE each with its own agency and with its own mandate. And so those things are coming together in a coordinated way before the election.

**Question:** (off microphone)

**Government Official 1:** Yes, so it's virtual group that leverages the existing work in each of those agencies and really is seeking information sharing protocols, prioritization across the departments before and leading up to the election. To this specific comment there, each of these departments and agencies on site have unique mandates so CSIS and RCMP will do investigations into things that are happening in Canada. CSCI is very foreign focused and you know we're limited to looking at foreign targets but the group together will be providing insights on anything that we see.

**Question:** Can I just (off microphone) your answer to John's question. You say there is disinformation even if it's domestic it would be considered under the threshold. What's the difference between domestic misinformation and domestic political spin?

**Government Official 5:** So disinformation, so there's kind of – what's the – go ahead. You've got the ---

**Government Official 4:** Certainly. Just to distinguished between disinformation and misinformation, I think that's a really important place to start. Misinformation is where it's not malicious you know it's often done in error or a lack of knowledge. Disinformation has malicious intent. That's the definition that we use. And that's where really the focus is. It's not on things that you know are shared in error. It's really where it's concerted effort to disinform people.

I would also add to you point, these measures are not intended to tamp out you know important and you know vital democratic debate. There is a threshold for where it's criminal activity or covert of clandestine. That's where really you know the focus is. Anything below that is part of a health democracy and we don't want to step on that.

**Question:** So it has criminal or covert – two other things that you said. Given an example please.

**Government Official 5:** So I would just simply add that in a domestic situation there are other tools available, right. It could be criminal and intent. And so the RCMP might have a role. It could be something that's a violation of *The Elections Act* in which case

the Commissioner of Canada Elections has a role. Our expectations overall is that the protocol if it were to be initiated is more likely to be initiated in response to a foreign. But it is the disruption that matters not the source.

**Question:** But you know what I mean. I mean misinformation by a party about Syrian refugees behind terrorists for example. That can influence someone's vote, right. So I'm trying to see where is the line between a party being deliberately dishonest to gain vote and – it is dishonest but --

**Government Official 5:** The line is

**Question:** But you know the difference between that (crosstalk) you need to intervene.

**Government Official 5:** We hummed and hawed over this. Democratic debate is rough and tumble. The line will be very generous for political parties. That's not what intent – it's not intended to catch political parties or to referee the election. It's the case of covert, malicious actions done. You know if it were to occur probably from overseas into the Canadian election. That – there is no intention to be an orator of truth here. That's your role.

**Moderator:** Sorry. We have to wrap it us. Sorry, Julie, we're out of time. We have to wrap it up. Perhaps we can chat with you afterwards. So mesdames et messieurs merci. Merci à tous les représentants aujourd'hui. This concludes our tech briefing but stay tuned for the announcement at 11:00 a.m. Merci beaucoup.

-30-

**TRANSCRIPTION/TRANSCRIPTION**
**NEWS CONFERENCE/CONFÉRENCE DE PRESSE**
**Transcription prepared by Media Q Inc. exclusively for PCO**
**Transcription préparée par Media Q Inc. exclusivement pour BCP**
**DATE/DATE:** January 30, 2019 11:00 a.m. EST
**LOCATION/ENDROIT:** National Press Theatre, Parliament Hill, Ottawa, Ontario

**PRINCIPALS/PRINCIPAUX:**
The Honourable Karina Gould, Minister of Democratic Institutions
The Honourable Ralph Goodale, Minister of Public Safety and Emergency Preparedness
The Honourable Harjit Sajjan, Minister of National Defence

**SUBJECT/SUJET:** Minister of Democratic Institutions Karina Gould, along with Minister of Public Safety and Emergency Preparedness Ralph Goodale and Minister of National Defence Harjit Sajjan, makes an important announcement regarding safeguards to Canada's democracy and combatting foreign interference.

**Moderator:** Bonjour et bienvenue au Théâtre National de la Presse. Welcome to the National Press Theatre. I'm Elizabeth Thompson with CBC. Today we have with us Minster Ralph Goodale, Minister of Public Safety and Emergency Preparedness, the honourable Karina Gould who is the Minister of Democratic Institutions and the Minister of National Defence, Mr. Harjit Sajjan.

They will be talking about the steps the government will be taking to combat possible foreign interference in the next election. Afterwards there will be questions. It will be one question, one follow up and I will be strict about enforcing that.

**Hon. Ralph Goodale:** Karina is going to begin.

**Hon. Karina Gould:** Thank you for joining us today, merci d'être avec nous aujourd'hui. Canada's next federal election is set for this October. In recent years elections around the world have been targeted by both cyber and non-cyber attacks. Allies such as the United States, the UK, France and Germany have all experienced degrees of foreign interference in recent elections.

Ces attaques malveillantes sont parfois si bien masquées qu'elles sont difficiles à détecter. Elles menacent aussi d'affecter notre confiance dans notre système et nos processus démocratiques. We cannot allow this trust to be broken. I want to assure Canadians that our government is prepared and has a plan to defend our election against threats.

We have deliberated across many government departments as well as with the major political parties. Nous avons discuté de la question avec de nombreux ministères fédéraux ainsi qu'avec les principaux partis politiques. First off I must say Canada's

electoral system is already strong. Notre système électoral est reconnu à l'échelle mondiale pour son efficacité et son intégrité.

Comme notre système électoral fédéral utilise des bulletins de vote en papier il est moins vulnérable aux cyber attaques et à la manipulation des résultats. We have robust transparency requirements and political financing and advertising rules. Our elections modernization act, Bill C76, has new measures against foreign funding and advertising and new penalties for the misuse of computers to affect the results of an election.

Enfin nous avons trois organismes de sécurité de première ligne. Ces institutions de calibre mondial s'adaptent constamment à l'évolution des différentes menaces. À titre de Ministre des Institutions démocratiques j'ai pour mandat de diriger les efforts déployés par notre gouvernement pour défendre le processus électoral contre les cyber menaces.

We have been watching and learning from the experience of others making our own assessments and have developed a plan that will protect Canada's election. Our plan has four areas of action – combating foreign interference, strengthening organizational readiness, expecting social media platforms to act, enhancing citizen preparedness.

Ce plan propose une approche pangouvernementale. To discuss efforts to combat foreign interference further I would like to now call upon my colleague the Minister of National Defence.

**Hon. Harjit Sajjan:** Thank you Karina. Our government has been working together to protect our democratic institutions and identify potential threats to our democratic process. In order to do so we asked the Communication Security Establishment to analyze the nature and extent of cyber threats to Canada's own democratic process.

The first report of its kind CSE published its finding to that request in June of 2017. Our government believes that our democracy is strongest when all our citizens can vote without threat of interference. By releasing this report publicly we make all Canadians aware of the potential threats and the challenges we face as a country.

As CSE concluded in its report on cyber threats, Canada's electoral system and democratic institutions are not immune to foreign interference seen in other parts of the world. In fact, it found that cyber threat activity against the democratic process is increasing around the world. It also concluded that Canada could be targeted by any of our adversaries who use cyber capabilities to try to influence the democratic process.

These findings demonstrate the need for all Canadians and institutions, especially those involved in the democratic process, to be vigilant. Nothing is more important to this government than protecting our democracy and ensuring that our next election is fair and free. That is why we have a government wide plan to prepare and respond to threats.

As Minister Gould has announced, our plan includes four areas of action the first of which is combating foreign interference. The front line of our efforts to fight foreign interference is made up of Canada's three security agencies including the Communication Security Establishment for which I am responsible and together with the RCMP and CSIS these three security agencies work every day to protect Canada's national security, the safety of Canadians and the integrity of our elections.

Our security agencies also work closely with Elections Canada to protect their systems, provide security advice and let them know about potential threats. Our national security agencies remain vigilant in monitoring the capabilities and activities of potential adversaries who may attempt to interfere with Canada's upcoming election.

From an international perspective, Global Affairs Canada has also been working with partners in other democracies around the world who face similar threats to their electoral process. At the G7 Summit in Charlevoix last summer partner nations agreed to a rapid response mechanism. This coordinated effort will strengthen our ability to identify and respond to diverse and evolving threats to our democracies.

As with Global Affairs Canada, the G7 rapid response mechanism coordinating unit will act as a focal point for Canada and all of its G7 partners. The coordination unit will be tasked with sharing information and threat analysis and critically identifying opportunities for coordinated responses when an attack occurs.

The RRM coordination unit will provide analysis and reports on threat patterns and trends. The information shared across the G7 will be used to develop a better understanding of the evolving threat environment. This will help us better position ourselves to anticipate, identify and respond to threats across the G7.

Under Minister Goodale's mandate, the RCMP is relocating assets to create a foreign actor interference investigative team which my colleague will describe in a moment. Our government has established initiatives like the new security and intelligence threats to elections known as SITE, a taskforce chaired by CSE which brings together CSIS, RCMP and Global Affairs Canada to help prevent covert, clandestine or criminal activities from influencing or interfering with the electoral process in Canada.

SITE combined with the G7 rapid response mechanism and the RCMP foreign actor interference investigative team demonstrate that our government is dedicating the resources needed to protect it against cyber threats and foreign interference to our electoral process. We are also improving how government organizations work together to address these threats.

As you know as part of the 2018 national cyber security strategy CSE established the Canadian Centre for Cybersecurity under the leadership of Scott Jones. The Centre consolidates the cybersecurity operational units from three existing departments into

one organization. This consolidation improves the government's organizational readiness to respond to cyber threats.

CSE continues to protect the government of Canada's information systems and networks against cyber security threats every single day. In addition CSE has offered to provide security advice and guidance to federal political parties on ways to strengthen their networks and systems. The Centre is also responsible for the get cyber safe public awareness campaign which educates and informs Canadians on ways to be safer online.

In the lead up to the 2019 federal election CSE will be releasing an updated report on cyber threats to Canada's democratic process. I encourage all Canadians to use these resources. Before I pass it over to Minister Goodale I would like to take a moment to thank all of the women and men at CSE for their tireless commitment to protecting Canadians. Due to the nature of their work they may be less known but their dedicated service helps keep all Canadians safe.

**Hon. Ralph Goodale:** Thank you Harj, Karina. What we're announcing today is a plan to protect the integrity of Canada's 2019 federal election. As Minister Gould mentioned the plan has four parts – combating foreign interference, strengthening organizational readiness, expecting social media platforms to act responsibly and enhancing the preparedness of every citizen.

Karina will deal with the latter two of those in a moment. Minister Sajjan and I are focused on the first two. From time immemorial governments worldwide have been engaged in efforts to mould public opinion and government policies in other countries to advance their own interests.

As long as that is done in an open, peaceful, transparent manner within the law it's fine. It's called diplomacy or treaty negotiations. Our Team Canada efforts to shape opinions and build support in the US for NAFTA are a good example – public, factual, lawful, no basis for objection. When that type of activity becomes covert or clandestine, when it consists of lies and disinformation aimed at misleading people, destabilizing the economy or society or manipulating the democratic process, a bright red line gets crossed.

It could be the old fashioned way, hostile intelligence services collecting or stealing political, economic, commercial or military information. It could be foreign agents providing illegal funds to support candidates or bribe officials. It could be cultivating personal or financial ties to coerce or manipulate diaspora.

Increasingly the interference is higher tech – social media have been used to falsely slander elected officials. Trolls and bots are despatched to stoke anxiety, even hysteria around sensitive issues. Fake news masquerades as legitimate information. As we've seen these issues are of deep concern among G7 and Five Eyes partners.

The Americans were obviously affected in 2016. Both parties were hacked. Bot nets were rampant. One study estimates about one fifth of all Tweets posted during the final month of the 2016 US campaign were generated by bots. This wasn't citizens intensely engaged in the democratic process. It was contrived and electronically generated meddling intended to pervert the conversation.

In France bot nets were used to promote false and defamatory propaganda against the leading candidate. In Germany in the 2017 parliamentary elections 7 of the 10 most shared articles about Angela Merkel on Facebook were false. There is no doubt that covert and corrupt activities originating in foreign capitals are taking place.

They're intended to corrode systems and pervert the course of democracy. To combat foreign interference you have to detect it. That's the work of our SITE taskforce and the agencies that are part of it consisting of the Canadian Security Intelligence Agency, the Royal Canadian Mounted Police, the Department of Global Affairs under the chairmanship of the Communicator Security Establishment.

Whether it's hacking, intimidation, bribery they have the tools and skills to identify the interference and its source. For example the RCMP has set up a special foreign actor interference investigative team to disrupt foreign activities that constitute criminal acts. CSIS conducts ongoing threat investigations that help identify, mitigate and counter illicit foreign activities that target Canadians.

Equipped with intelligence and evidence our police and security agencies will work with other organizations and institutions to improve their readiness and capacity to plan for, respond to and mitigate foreign threats. Minister Sajjan has referred to the 2017 CSE report that found Canadian political parties were vulnerable to cyber-attacks.

CSIS is also aware of attempts by foreign states to interfere with our political process and manipulate public opinion. All political parties have a responsibility through best practices in their IT systems and vigilance against abuses to combat foreign interference. We all want the parties to have the latest most reliable information.

To that end for the first time our security agencies will provide direct security briefings to key members of national political campaigns. They will need to obtain the appropriate security clearance in advance. These multi-partisan campaign officials will be able to receive regular briefings including classified information on the foreign interference activities both cyber and human that target Canadian democratic institutions.

The news media is also a key player. Never has journalism been under such pressure from those who would masquerade as legitimate but whose strings are pulled by foreign authorities as they use cyber space to manipulate. I will leave it up to all of you to set your own high standards of reporting and analysis by which genuine journalism can be measured and distinguished from what's fake.

With respect to social media, those who provide the platforms have an important role to play in ensuring they are contributing to and not detracting from political discourse. Individually and through the Five Eyes and the G7 we have challenged the social media operators to help us combat terrorist propaganda, the sexual exploitation of children and human trafficking.

More and more insidious interference to subvert democracy is being added to the list of harms that these service providers need to help stop and they are uniquely positioned to do so.

**Hon. Karina Gould:** Minister Goodale has touched on the role that social media plays in our democratic process. Les plateformes numériques telles que Facebook, Twitter et Google sont devenu des espaces importants pour la tenue de débats démocratiques. However these platforms have been manipulated to spread disinformation and create confusion which has the potential to disengage people in the democratic process.

We are concerned about the risk online manipulation poses to the integrity of our election. We expect social media platforms to take concrete actions to help safeguard this fall's election by promoting transparency, authenticity and integrity. I have initiated conversations with the social media platforms to identify these actions. As a starting point we are looking for a commitment from social media companies to implement changes in Canada that they have already applied in other countries.

Je suis déterminée à assurer une pleine transparence et à tenir les Canadiens au courant des progrès réalisés à cet égard. The fourth area of action is enhancing citizen preparedness. Les citoyens impliqués et informés est la meilleure défense contre les menaces à la démocratie. Des citoyens en mesure de reconnaitre la désinformation et la manipulation en ligne sont moins susceptibles d'en être les victimes.

To help build those skills we are dedicating $7 million towards digital news and civic literacy programming that will help Canadians critically assess news reporting and editorials, know how and when malicious actors exploit online platforms and acquire skills on how to avoid being susceptible to online manipulation by malicious actors.

Au cours des derniers mois notre gouvernement s'est penché sur la meilleure façon de réagir à un acte d'ingérence qui remettrait en question l'intégrité du processus électoral. Our considerations included when and how Canadians should be informed and by whom. Our goal was to find the right way to instill confidence in the message and the messenger while remaining impartial.

Today I am also announcing the critical election incident public protocol. The protocol establishes a simple and impartial process to inform Canadians of a threat to the integrity of the 2019 federal election. It is designed to avoid the kind of gridlock that could prevent an effective public announcement. The core responsibility for the protocol resides in a group of senior civil servants.

Ce groupe rassemble des perspectives juridiques et de sécurité nationale d'Affaires Étrangères et de gouvernance. Les membres de ce groupe possèdent l'expérience nécessaire pour évaluer de façon rigoureuse les faits relatifs à la sécurité et les répercussions de la communication d'une menace d'une telle ampleur aux Canadiens. Il représente les échelons les plus élevés de la fonction publique et ont pour mandat d'agir de manière impartiale, transparente et juste.

Let me be clear. This is not about refereeing the election. This is about alerting Canadians of an incident that jeopardizes their right to a free and fair election. If something happens during the campaign, Canadians will be able to trust that the right people have decided to make it public, that the information is accurate and that the announcement is not partisan in nature because this issue rises beyond partisan considerations.

Le protocole a une portée restreinte et un seuil d'intervention très élevé en ce qui concerne les annonces publiques. Le protocole s'appliquera seulement aux incidents qui ont lieu pendant la période électorale. If the group determines that the threshold has been met, the Clerk of the Privy Council will direct the head of the relevant security agency to notify Canadians of the incident.

Par souci de justice et de transparence nous avons consulté les quatre partis politiques à plusieurs reprises dans le cadre de l'élaboration de ce protocole. It is important that Canadians trust the purpose of the protocol and the decisions made by the senior group of public servants will be made in an impartial manner.

Our hope is that such a public announcement never happens but it is essential that we inform Canadians now of a structure in place to keep them informed and engaged. We are adapting to new realities from a position of strength. The measures announced today will bridge gaps that this evolving environment creates.

Pour qu'une démocratie soit forte et résiliente il faut que les citoyens aient confiance dans le processus et la légitimité des résultats. Together we are working hard to prepare for a free, fair and secure 2019 federal election so we can continue to uphold the trust and confidence that Canadians have in our democracy. My colleagues and I welcome your questions.

**Moderator:** Time for questions. There will be one question, one follow up. I will be strict because we are going to be limited in time. We'll do around the room and then go to the teleconference. First question Julie Van Dusen, CBC.

Question: Mr. Goodale you talked about bots in the US and false information about Angela Merkel. Can you give us an idea what kind of incidents could happen here that would prompt the Canadian government to alert Canadians in the middle of a campaign? Could you give us an idea?

**Hon. Karina Gould:** One of the things that's important is that the threshold for alerting the public needs to be high. It needs to be something that is compromising the ability for a free and fair election to take place. However over the past two years we have learned from incidents around the world, specifically in allied countries like the US or France as to what kinds of incidents those would be. Of course they would be context dependent but this protocol is put in place to ensure that having learned from the experiences of our allies we can act swiftly in Canada.

Question: I'll ask my next question but I was hoping for some examples. I'm assuming they're similar to those you mentioned. Your documentation talks about malicious foreign actors seek to undermine our democratic society and institutions. Who might they be?

**Hon. Karina Gould:** As we have seen around the world there have been incidents of foreign state actors that have tried to manipulate public discourse during an election. What's important to note is our government is prepared to defend Canadian democracy.

Ultimately what we're talking about today is ensuring that when a Canadian walks into a ballot booth, when they mark their ballot, that they are making their decision based on the information that is out there and we as a government are providing the tools and information they need to make an informed choice.

Ultimately it's Canadians who are deciding the outcome of the election and our job as a government is to make sure that they have the tools and resources to make those decisions.

Question: One of the weakest links in this ecosystem is the news media itself. I'm wondering if you have undertaken any outreach to publishers, to executives in major networks to discuss the possibility of foreign actors attempting to (off microphone)

**Hon. Karina Gould:** Thank you for that question. I think it's very important. Obviously the media has an incredibly important role to play in protecting our democracy. Without a strong fifth estate we don't have a robust democracy in Canada. One of the things that happened in the fall was the NATO strategic communications centre came to Parliament Hill and offered a session for the parliamentary press gallery.

It was not as well attended as one might have expected. There were some members who did come and I think that was a good first step. Given their experience they have asked NATO StratCom to come back and they have done good work with journalists throughout NATO countries.

I would encourage journalists, news outlets to engage with them on best practices in other countries, particularly our allied countries because the media does play such an important role when it comes to how Canadians consume information.

Question: Minister Goodale, you were Cabinet Minister (off microphone) (Laughter) I'm wondering if you could –

**Hon. Ralph Goodale:** That was a low blow.

(Laughter)

Question: I'm wondering if you could reflect a bit not in your current Cabinet role but as an MP about how foreign powers, particularly Russia, has attempted to influence western countries.

**Hon. Ralph Goodale:** A lot has changed in the intervening years. Some of the old techniques of personal influence are still used and abound in some circles but what we have to recognize in the big change in the intervening years is technology.

The fact that you now don't have to be in the same room face to face with the person that you're trying to influence or manipulate, you can do that by remote means. You can do it by electronic means, by a bot or a troll. It's the advent of that technology that makes things so much more immediate.

The impact of that external influence is magnified many times, the sorts of things that happened reported publicly in the American election campaign of a couple of years ago would not have been physically possible in previous elections. The timeframe involved was telescoped so the magnitude was many times magnified.

We have to be aware that all the old fashioned techniques still apply of trying to exercise influence in a clandestine covert way but layered on top of that are all the tools of modern technology protected by techniques of encryption and activities on the dark web and all of that that makes it that much more difficult to detect and then accurately analyze as to exactly who is doing what to whom and what is the motive behind it.

That is why in the SITE taskforce under the chairmanship of CSE, the Communication Security Establishment, with all of its cyber expertise, the RCMP task force is there, CSIS is there, Global Affairs is there, the rapid response mechanism represented through Global Affairs is there, all to make sure that we're bringing all of our modern defence mechanisms to bear for the objective of making sure Canadians can make their own independent impartial decision on the basis of what they truly believe as Canadians is the right thing to do and not manipulated by a foreign capital.

Question: À quoi vous attendez des géants web comme Twitter et Facebook? Qu'est-ce que vous leur demandez?

**Hon. Karina Gould :** J'ai initié les conversations avec les géants du web et j'ai trois – le gouvernement a trois expectations qui seront d'assurer que les patrons digitaux assureront l'intégrité de nos élections, qu'ils ont l'authenticité dans les activités sur leurs plateformes et la transparence aussi.

Ils ont pris des initiatives et mes officiels sont en contact avec eux et ils sont en train de nous informer des actions qu'ils prennent. Par exemple je sais que Twitter removes fake accounts qu'ils detect sur leur site mais c'est seulement des pas initiaux. Nous espérons que les actions qu'ils ont prises dans les autres juridictions pour protéger les élections, par exemple dans les États-Unis ou en France en Allemagne seront appliquées ici au Canada.

Nous sommes en train d'espérer qu'il y a plusieurs actions aussi et je crois que ce n'est pas seulement le gouvernement qui espère ça mais c'est aussi les Canadiens qui utilisent leurs plateformes parce que nous espérons que comme Canadiens, ton smart phone, ton ordinateur que tu as la confiance que les interactions que tu as sur ces plateformes sont authentiques et l'information que tu reçois est de bonne information.

Question : (Off microphone) les plus susceptibles de mener ces campagnes. Vous pensez à la Russie? La Chine est embrouillée avec le Canada.

**Hon. Karina Gould :** Comme vous pouvez voir dans le rapport de l'Établissement sécuritaire des communications qui a été publié l'année dernière, il y a deux ans maintenant, il y a des états, il y a des acteurs qui ne sont pas des états mais la chose importante est de savoir pour les Canadiens que nous comme gouvernement nous sommes en train de préparer.

Nous sommes préparés pour les éventualités de n'importe où viennent les menaces cyber et c'est pour assurer les Canadiens qu'il y a un plan et qu'il y a un effort pangouvernemental pour protéger nos institutions démocratiques.

Question: In terms of the special group to warn Canadians, in France it was fake emails but in the US it was real emails. At what level would the protocol raise questions about a leak if it's real information does that make a difference whether the information is real or fake or a mix of both? Does that make a difference?

**Hon. Karina Gould:** It will be context dependent and what's important to note is that it could be one event or it could be a culmination of a series of events. It will be up to this group of highly respected civil servants to make that decision. It will be based on information evidence provided by the security agencies.

What's important is we as a government have asked for it to be five individuals so it will be consensus based and it will be discussed in order to alert the public. Cyber threats can come in many different forms. Some of them may be low level and not have a great impact. Some may be greater and we want to ensure that the gravity of announcing something to the public is taken into consideration.

Question: It was made clear at the briefing that right now this is a caretaker approach during elections. Right now the burden is on Ministers, on the government to warn Canadians of anything. Are any of you aware of people or groups currently getting ready to influence the election and if so who?

**Hon. Karina Gould:** We are a member of the G7, of NATO, of the Five Eyes. It would be naïve of us to assume that we are not a target for a cyber-attack. That being said, we are constantly monitoring. As my colleague can comment, the CSE will be coming out with an update to its cyber report in the coming weeks and months. We look forward to receiving that. That will be made publicly available.

Question: Could you be more specific? What are you asking from the social media companies that you are meeting with now? What do you need to see from them to make sure that Canada's process and election decisions are not (off microphone)?

**Hon. Karina Gould:** As I said the first thing I've asked for is for activities and actions that have already taken place in other jurisdictions to be applied here in Canada as well such as for example Twitter has their ad transparency centre, to apply that in Canada. That's a good example of one of the things we're asking for.

We are constantly monitoring what they're doing. The EU has made some requests ahead of the EU elections. We'll be following that and seeing if that should be applied in Canada as well. Importantly it rests on those three pillars in terms of the integrity, authenticity and transparency of the activities that take place on their platforms.

Frankly we see the social media companies while they're starting to take some responsibility still have a way to go and I think for their consumers and users they want to know when they're interacting on those platforms that they can have confidence in the interactions they're having.

It's not a stretch to say that parliamentarians in Canada but also around the world are looking closely at the activities and the responses of social media platforms to how they respond with regards to our democracy in terms of how we move forward.

Question: There are aspects of Bill C59 which is before the Senate now which would enhance the powers to protect critical digital infrastructure, to prevent cyber-attacks. It`s taking a while in the Senate, might not get passed until June. Are security agencies in Canada going to be ready and have the proper tools to deal with foreign actors that have influenced the most powerful country in the world and how they could have voted in today's President?

**Hon. Ralph Goodale:** Two points: there is nothing in the plan we have announced today that is specifically dependent on C59. However C59 is a very important piece of legislation. It changes the national security architecture. Someone asked that rude question about the Cold War (laughs).

When you think of it, with the passage of time the CSIS Act was written in 1984. The fax machine was ground-breaking new technology in 1984. If you were buying a cellphone you'd have to carry it in both hands. Technology ahs moved dramatically. The flow of reports from oversight agencies like CERC and the judgments of the federal court over that 30 or 40 year period have totally changed the legal and constitutional context.

C59 addresses all of that to provide the modern framework. There are some new tools that are provided in the legislation. There is critically a transparency imperative brought to bear, not just the national security and intelligence committee of parliamentarians which was in a separate piece of legislation. But there`s the new national security and intelligence review agency, the commissioner of intelligence and other measures brought to bear in C59.

C59 is urgent in its own right. I am very anxious for it to receive the appropriate consideration and passage in the Senate and we will work very carefully with Senator Gold and the committee chaired by Senator Boniface to assist in the Senate's deliberation. We're anxious to see it passed as rapidly as possible. It is important for the security of Canada. The powers and activities we're contemplating in this package today are not specifically dependent on C59.

**Hon. Harjit Sajjan:** There is tremendous capability and Bill C59 will give us allow our legislation to catch up to the capabilities but I think Canadians can have significant confidence in the defence of Canada and making sure not only our elections will remain free. It's because of our people, the people that we have are absolutely incredible.

Yes, our investments will have an impact and the legislation will allow them to do more but I'm extremely proud of the people we have in all our security agencies because they've been dealing with a multitude of different threats. This is just a new type of threat that we have to deal with. The recommendations that have been brought forward, one thing I can assure you. Canadians can have confidence because the people who are behind all this technology.

Question: The government has said repeatedly that there have in fact been attempts at foreign interference with the Canadian government process. Mr. Goodale repeated that again today and yet you have so far refused to tell us what those attempts have been. Are we to conclude from that that those were not serious enough to warrant alerting the public?

**Hon. Karina Gould** Yes.

Question: Can I ask you about domestic actors? You've been stressing foreign actors through this press conference and yet your officials say this is meant to apply to domestic actors as well and some would suggest that's probably more likely in Canada

that you're going to have malicious actors trying to influence the outcome or just be disruptive.

Where do you draw a line between normal political activity during a campaign in which there's a good deal of misinformation being spun around versus something that's more orchestrated and malign?

**Hon. Karina Gould:** I think that's a really important question. This space is notoriously tricky in that regard. With regards to foreign interference it's more clear cut. One could argue ensuring that our elections are free from foreign interference is the basis of what this announcement is today.

However there were other changes made to the Canada Elections Act in C76 that would strengthen the investigative powers but also the ability to apply the law through both Elections Canada and the Commissioner of Canada Elections.

As I mentioned in my remarks there have been new additions with regard to the malicious use of a computer, hacking internally is still an illegal event and that would be monitored and enforced by the existing authorities in Canada.

Also with regard to the spread of false information we clarified the legislation to ensure it would be -- the Commissioner would be able to apply it based on the recommendations we received from both Elections Canada and the Commissioner in the CEO's report following the last election.

Also with all party support we tightened the restrictions with regards to foreign funding in our political system writ large. There are a number of mechanisms in C76 that will ensure the integrity of the system domestically that are very important to highlight as well.

As the CSE report noted cyber-attacks were focused on foreign attempts but this could also be the result of criminal activity or so-called hack-tivist groups and if they are in contravention of the Elections Act we have the tools to be able to go after them through Elections Canada and the Commissioner. That resides in their domain.

Question: You're aware the Elections Act has had a fake news sanction for 17 years and yet your government last year took this a step further. It arranged a contract with a third party through the Department of Canadian Heritage, called the Public Policy Forum that with subsidies proposes to in its words "expose in real time disinformation in digital media".

No follow up but two questions for you now. What assurance can you give because we can't get any records on this from Privy Council Office, Department of Heritage or Department of Justice, what assurance can you give that no federal agency or any freelancer paid by a federal agency will supervise, monitor or interfere in election coverage?

What is the bright red line between investigating Russian bots and going after coverage or commentary of chatrooms or websites or YouTube channels that say things that you don't like?

**Hon. Karina Gould:** What is really important to note is that in no way whatsoever does this announcement limit Canadians' freedom of expression or free speech. What we're talking about today is foreign interference activity that try to manipulate the conversation.

What we have seen around the world is incidents where what looks like legitimate domestic actors are actually masquerading. It's actually foreign actors masquerading as domestic actors. That's not always easy to detect. It's done specifically not to be easy to detect. These are covert operations to try and manipulate Canadians.

What we are trying to do is if that information is available to us as a government or to the media to ensure Canadians have the tools to make informed choices. With regard to civic education and civic awareness there are a multitude of very capable organizations in Canada who will be able to provide guidance to Canadians on how to evaluate information that is coming at them.

Ultimately it's not our job to tell Canadians what is good or bad information but to provide them the tools when something comes at them to make a choice on their own and say where this information is coming from, who is behind it and what their objective is.

With regard to the money I announced today the objective is to have civil society organizations in Canada who can help provide some of the civic awareness and education to evaluate news, digital media etc., the information coming to Canadians so they can make their informed choice of how they digest this information and how they share it or not.

Question: I want to be sure I've grasped this. You can't constitutionally affect a free press or free speech. You're telling me that you're going to pay some organization, presumably the Policy Forum, to rate the accuracy of digital media in an election year and no-one finds that --

**Hon. Karina Gould:** I'm actually not telling you that. What I'm saying is we are providing funding for civic education and awareness to help with media and digital literacy. When you open up a newspaper you have a sense that this is coming from a journalist who is professional, who has done their research and whose information is coming from a reliable source.

Depending on which newspaper that is you have a sense of where that information is coming from. When you go onto a social media platform and you see a meme or a

story, if it's being shared by a friend or a cousin or someone trusted you may implicitly share that information because it's coming from a trusted source.

What we think is important and what Canadians think is important is to understand where that information is coming from and to have at their disposal the tools and information to be able to assess that information critically, to assess its validity, to assess the source and then to make their own decision about how they use that information. That's what I think is important.

Question: Minister Gould you touched on this so I think you anticipated the question being raised either by some parties or by reporters. You mentioned this isn't about refereeing the next election.

How do you anticipate or how can you envision a balance between denouncing disinformation and what some would call political spin where quite often any of the parties use information that is a little false, very false to make political gain. How can you explain that balance so people aren't worried about what this might do?

**Hon. Karina Gould:** An election period is a period of heightened information and heightened discourse that's going on. It's incredibly important and vital to our democracy to ensure that the space for legitimate domestic discourse takes place.

That's where the protocol would only be enacted at a very high threshold if there is evidence that foreign interference is at a moment where a free and fair election could be called into question.

That's why we have engaged with the political parties. We've met half a dozen times so far and will continue to do so. It's why political party leaders will have and their officials will have security clearance to ensure we're building confidence into the process. They will be alerted before a public announcement but also importantly they also have a direct line to CSE should they want to seek advice or should they raise something on their own.

The important part is that we're announcing this today to continue to build confidence and trust into the process so that if something arises all implicated stakeholders will have trust in the process.

Question With all due respect, your officials or the officials during the briefing recognize it could be domestic disinformation. It's not just foreign actors. Where is the line between a domestic actor doing misinformation for political gain and a domestic actor doing disinformation? You mentioned interfering with the election.

Memes denouncing some politicians or capsules saying things about immigrants can affect an election because it can sway someone's opinion. Where is the line? What do you say to people who worry you're policing some information and not others?

**Hon. Karina Gould:** Legitimate domestic discourse is of course something to be encouraged. I appreciate that during an election and a writ period this is heightened. When it comes to doing things lawfully that is to be encouraged. If there is a coordinated attempt to undermine the system breaking the Canada Elections Act, that is something that Elections Canada, the Commissioner of Canada Elections and the RCMP would be seized with.

Question: I wanted to get back to social media. You did say they have a lot of work to do ahead of them. They're notorious for not being receptive to change or to governments telling them what they like. I wanted to hear from you, in your discussions with them what their response has been so far, not just concretely but do they seem open to what you're looking for?

**Hon. Karina Gould:** I think there's an openness. I think there's an understanding on the part of the social media platforms that they need to do things better, that they have to re-earn the trust of the people that use their platforms. Over the course of the past couple of years there have been several incidents that have weakened the trust people have in their platforms.

I would say given the fact that in C76 we legislated the social media platforms in two areas, with requiring them to have an ad registry during the pre-election and election period as well as banning them from knowingly accepting funding for advertising from foreign sources. There is a receptiveness to work together to ensure that they are doing everything possible to safeguard our elections.

Question: In a way you touched on this in terms of domestic. Your officials were pretty clear that it doesn't matter the source, it matters the impact. While you keep talking about domestic interference or coordinated campaigns falling under the Elections Commissioner they seem to think there could still be a role for the protocol when it comes to domestic interference.

I want to get clarification on that and whether that means something like robocalls which now seems old tech but robocalls telling you to go to the wrong polling station but now there's some more coordinated online campaign of that sort, would that fall under the Elections side of thing or would the protocol have a role to play for that?

**Hon. Karina Gould:** I think where sometimes it's tricky with regards to cyber-attacks is you may know there is something going on but it's difficult to attribute where that's coming from initially. One of the things I would say is as a world we've learned a lot more about how cyber-attacks happen over the past two and a half years.

Whereas the initial thought was simply with regards to hacking and leaking, we now understand there is a much deeper and I would almost say richer ecosystem that Minister Goodale alluded to in the dark web but also posing as domestic sources, coordinated campaigns to try and heighten legitimate domestic issues.

That's where at the time of seeing something happen there may not be the ability to directly attribute where it's coming from. However if it is a domestic actor that is breaking elections law they will be subject to the weight of Canadian law enforcement.

**Moderator:** We have two other people on the list. We've pretty much hit the time that we've been told. Can you hang in for two more questions?

Question: In the event of this protocol being enacted and some kind of announcement being made, what kind of follow up actions would the government take? You raised concerns about bots and (off microphone). What would the next step be if any? Would you just tell people about it and leave it at that?

**Hon. Karina Gould:** I think it would be context dependent.

Question: I want to come back on the (unintelligible) question and I will be more direct. What about false ads and information by political parties? What will you do about that or it's not covered, because we have often false or distorted information by political parties?

Hon. Karina Gould: That's not up to the government of Canada to weigh in on. The only thing I would say is within the updated Elections Act the provisions around false information have been tightened so they can be proven to be true or false. For example, if someone were to accuse me of having a criminal record you can see that I do not have a criminal record but the reason behind that as was recommended by both the CEO at the time and the Commissioner was so they can be enforceable.

Question: (Off microphone) domestic actors.

**Hon. Karina Gould:** That would be up to the Commissioner of Elections Canada.

Question: (Off microphone)

**Hon. Karina Gould:** If a domestic actor contravenes the Canada Elections Act they will be subject to Canadian law and law enforcement.

**Moderator:** I think we've pretty much run --.

Question: If the social media companies won't agree to what you want will you take steps to compel them because they have been fairly intransigent on a lot of these issues globally. The word you keep using is expecting them to cooperate. Are you prepared to compel or legislate or require them to cooperate?

**Hon. Karina Gould:** I think as you would have seen in C76 we did legislate them to do two things and we will continue to have conversations with them. I expect they will follow.

**Hon. Ralph Goodale:** Can I just add to that point? We've had a very vigorous conversation with them over the last three or four years about terrorist propaganda, about child sexual exploitation and about human trafficking. It took a while to get the traction but the responsiveness has increased over that period of time. Many countries are now raising with them this same point about foreign interference in elections.

The topic will not come as a surprise to any of them. They have the experience of the last three or four years on other topics to understand the level of expectation that governments will present them with.

Question: Will they be compelled to report suspicious activity to your committee during the campaign? They might detect it through their algorithms and their security before you might.

**Hon. Karina Gould:** They have ongoing relationships and one of the expectations is to ensure they are open and communicating.

**Moderator:** I'm going to exercise the moderator's prerogative to ask one small question. Facebook for example just broke the pro publica ad collector tool and they changed things to thwart people trying to see transparently what political parties were up to. How far are you willing to go if they won't cooperate with you?

**Hon. Karina Gould:** That needs to be clarified because I've heard conflicting information on that this morning. However if that is the case that's very disappointing, because that was an important tool for the media and the public to hold Facebook to account.

As I said, there have already been two occasions in C76 in which we have legislated social media platforms and they will follow the law. We will continue to have these conversations but of course we'll see how they react.

**Moderator:** How far are you willing to go? Are you willing for example to pull government advertising from a platform that won't cooperate?

**Hon. Karina Gould:** We'll have to continue on our discussions and see how these conversations go. Thank you.

**Scenario Note Technical Briefing Election Security**

This Technical briefing is scheduled to take place on June 25 at 11 am at the National Press Centre. The objective is to provide the media with an update on activities taken to protect the 2019 election since the January 30th media event. Consideration will be given to an additional media engagement session where the council of Deputies would discuss their roles during the election.

The technical briefing will be "not for attribution." Additionally, as the number of media enquiries for information about elections security, this briefing will allow the media opportunity to pose questions to ensure they understand actions the government has taken to date.

The roll out and expects subject matter is below:

| | |
|---|---|
| 5 mins | Representative from DI would articulate updates to the panel terms of reference and indicate from a high level their activities in advance of the elections. He would also give a sense of planning or exercises that have taken place. |
| 5 Mins | The Chair of the SITE task force presents an overview of the type of work being undertaken by the task force. If appropriate, he could provide an unclassified overview of the threat environment, including a high level characterization of foreign interference detected. (This could be supported by a summary of G7RRM trend reporting). |
| 5 mins (TBC) | GAC RRM G7 describes leadership role CDN is taking related to threats to democracy. Outline mandate of RRM (full spectrum of threats, including disinformation) based on unclass/open source info about threat landscape. Identify what RRM can do (trends and tactics) and can't do (broad SM monitoring, focus on individuals, etc) |
| 5 mins (TBC) | Heritage Canada would outline the programs that have been funded as part of the Digital Literacy Initiative announced in January. |
| 5 Mins | Elections Canada would address its own preparedness and efforts they are undertaking with Social Media well provide its own overview of the electoral environment. |
| 40 mins | Questions to officials |

**GoC Election Communications DG Comms Steering Committee**

**June 13, 2019 10:30 am to 11:30 am**

**613-960-7511 Conf ID 8727015#**

Agenda

1. Introduction -- PCO
2. Departmental updates – All
3. Elections Canada Approach to Digital information – Elections Canada (attachment)
4. Website wireframe walkthrough– PCO
    - the link (open on mobile only) https://xd.adobe.com/view/eda6fe66-3760-4a41-456b-89e98131acb5-9b97/?fullscreen&hints=off
    - The PDF (attached)
    - The video screencap (attached)
5. Technical Briefing discussion—all (attachment)
6. Round table

Elections Canada

# Elections Canada's Approach to Digital Information at the 43rd General Election

## Presentation to the Group Of Five DGs Communications

## May 23, 2019

elections.ca

# Presentation objectives

- To describe our current digital environment and Elections Canada's approach to monitoring and responding to information that could interfere with Canadians' ability to register and vote at the 43rd general election

# Current digital environment

- **Opportunities:** Digital forums promote increased engagement, interaction and information sharing and allow Elections Canada to identify and respond to operational issues
- **Risks:** The deliberate dissemination of false information poses threats to our democracy:
  - Affecting voters' behaviour
  - Taking advantage of voters' vulnerabilities and fears
  - Influencing voters' views and opinions
  - Sowing confusion
  - Undermining trust in election results
  - Impacting the desired level of participation

# Types of digital information

- Elections Canada will monitor for three types of digital information:
  - Disinformation: False information that is deliberately spread with the intent to cause harm or to mislead
  - Misinformation: Incorrect information that is shared without intent to cause harm or to mislead – generally a mistake or misunderstanding
  - Operational incidents: Occurrences related to the electoral process that require action by Elections Canada

# *Canada Elections Act* (CEA) provisions

- Elections Canada will refer evidence of potential CEA offences to the Commissioner of Canada Elections
- Bill C-76 amendments to the CEA:
  - New offences related to impersonation and the misuse of computers
  - Requirement for certain online platforms to maintain registries of political advertisements
- The CEA does not:
  - Generally regulate the content of election messages
  - Provide authority to the CEO to block or take down election advertising
  - Provide for an election to be suspended due to disinformation

# Elections Canada's role

- Where the goal is to suppress the ability of certain individuals to vote and/or cause a loss of confidence in the fairness of the election, Elections Canada will act within the limits of its mandate by:
  - Championing electoral integrity and fairness while remaining politically neutral and non-partisan
  - Focusing on detecting and responding to inaccurate information about when, where and ways to register and vote
  - Acting on information related to the administration of the electoral process

# Not Elections Canada's role

- It is not Elections Canada's role to:
  - Manage the Government of Canada's cybersecurity policy
  - Protect political parties' IT systems
  - Regulate the Internet and social media
  - Serve as the arbiter of truth in advertising
  - Correct information about issues, personalities or platform policies as this could be perceived as favouring one political party or candidate over another

# Digital techniques

- Information campaigns aimed at the general population or that target supporters of a particular group or political party
- Techniques include micro-targeted ads, misleading online discussions or videos, impersonation websites and accounts, digital propaganda or other harassing behaviour
- Elections Canada is addressing this issue through three key activities:
  - Collaboration
  - Awareness and engagement
  - Detection and response

# Approach: 1) Collaboration

- Disinformation is a societal issue that extends beyond elections and Elections Canada's mandate
- Combatting disinformation requires collaboration among all those who have a stake in safeguarding the security and integrity of the election, including:
  - The Commissioner of Canada Elections
  - Political entities
  - Government partners and security agencies
  - Social media and online platforms
  - Civil society groups
  - Academics
  - Mainstream media
  - Citizens

# Approach: 2) Awareness and engagement

- Voter information and stakeholder mobilization activities that position Elections Canada as the authoritative source of information about when, where and ways to register and vote
- A repository of Elections Canada communications products and advertising on the website
- Efforts to promote fact-checking services and to encourage Canadians to be vigilant
- Information about what Elections Canada does not do – for example, we do not contact electors by phone or text

# Approach: 3) Detection and response

- The most effective way to deal with disinformation is to counter it with correct information
- Dedicated social media monitoring and response coordination team
  - Supported by a disinformation action group with representation from all business lines
- Use of social media monitoring and analytics tools
- Development of a risk register, playbook and escalation protocol
- Scenario building and tabletop exercises
- Continued research to follow developments and learn from the experiences and best practices of others

# Upcoming Communications Activities

- June 2019 Activities
  - Launch of Pre-writ period Voter Information Campaign
  - Ongoing Stakeholder Mobilization Activities – Inspire Democracy
  - Proactive Media Relations – Getting Ready for the GE Theme
    - Technical Briefings
    - CEO Press Conference
    - CEO Media interviews (TBD)
  - CEO Participation in Group of 5 Press Conference (TBD)
- Summer
  - CEO lower profile
  - Continuation of other above items
- September Pre-writ
  - CEO Press Conference and select interviews
  - Full communication calendar and Stakeholder Mobilization for GE
  - On the ground outreach program in place

# Questions?

WE ALL HAVE
A ROLE TO PLAY
TO PROTECT OUR
DEMOCRACY
Find out how
Expecting Social
Media Platforms
To Act
Combatting
Foreign
Interference
Improving
Organizational
Readiness
Enhancing
Citizen
Engagement
The Plan
SAFEGUARDING
OUR ELECTIONS
Protecting
Democracy
MENU
Government
of Canada
Gouvernement
du Canada

WE ALL HAVE
A ROLE TO PLAY
TO PROTECT OUR
DEMOCRACY

Find out how

Expecting Social
Media Platforms
To Act

Combatting
Foreign
Interference

Improving
Organizational
Readiness

Take a quick overview to
learn what's in each s.

- Digital Citizen Initiative
- Elections Canada
- Glossary

Enhancing
Citizen
Engagement

The Plan

Protecting
Democracy

SAFEGUARDING
OUR ELECTIONS

MENU+

WE ALL HAVE
A ROLE TO PLAY
TO PROTECT OUR
DEMOCRACY

Find out how

Expecting Social
Media Platforms
To Act

• Cyber Safe Campaign
• Rapid Response
Management group

This is a placeholder
action which will be taken

Combatting
Foreign
Interference

Improving
Organizational
Readiness

Enhancing
Citizen
Engagement

The Plan

Protecting
Democracy

SAFEGUARDING
OUR ELECTIONS

MENU

WE ALL HAVE
A ROLE TO PLAY
TO PROTECT OUR
DEMOCRACY
Find out how
• Declaration on Electoral
Integrity Online
• Christchurch Call to Action
• Transparency in online
Political advertising
Expecting Social
Media Platforms
To Act
Combatting
Foreign
Interference
Improving
Organizational
Readiness
Enhancing
Citizen
Engagement
The Plan
SAFEGUARDING
OUR ELECTIONS
Protecting
Democracy

LEARN ABOUT THE FOUR PILLARS
Learn more
Social media and digital platforms
Parliamentarians and political parties
Government of Canada
Canadian Public
SAFEGUARDING OUR ELECTIONS
We all have a role to play
MENU

Learn more
LEARN ABOUT THE FOUR PILLARS
Social media and digital platforms
Parliamentarians and political parties
Government of Canada
• Be cyber safe
• Think critically about what you see online
• Look to Elections Canada for facts about elections
Canadian Public
SAFEGUARDING OUR ELECTIONS
We all have a role to play
MENU

We all have a role to play
SAFEGUARDING OUR ELECTIONS
Canadian Public
Government of Canada
Parliamentarians and political parties
Social media and digital platforms
LEARN ABOUT THE FOUR PILLARS
Learn more

LEARN ABOUT THE FOUR PILLARS
Learn more
Section
Section
Section
Section
Think critically about what you see online
MENU

LEARN ABOUT THE FOUR PILLARS
Learn more
Section
Section
Section
Section
The role of social media & digital platforms
THIS IS WHERE A BLURB WOULD GO!
MENU

Français
Government of Canada
Gouvernement du Canada
MENU
Government of Canada
THIS IS WHERE A BLURB WOULD GO!
Elections Canada
Content TBD
SITE Task Force
Security & Intelligence Threats to Elections Task Force
WE ALL HAVE A ROLE TO PLAY TO PROTECT OUR DEMOCRACY
Find out how

WE ALL HAVE
A ROLE TO PLAY
TO PROTECT OUR
DEMOCRACY
Find out how
• Communications Security Establishment
• Canadian Security Intelligence Service
• Global Affairs Canada
• Royal Canadian Mounted Police
Parlor Rules
Security & Intelligence Threats to Elections Task Force
SITE Task Force
Content TBD
Elections Canada
THIS IS WHERE A BLURB WOULD GO!
Government of Canada
MENU

Draft for discussion

# CRITICAL ELECTION INCIDENT PUBLIC PROTOCOL

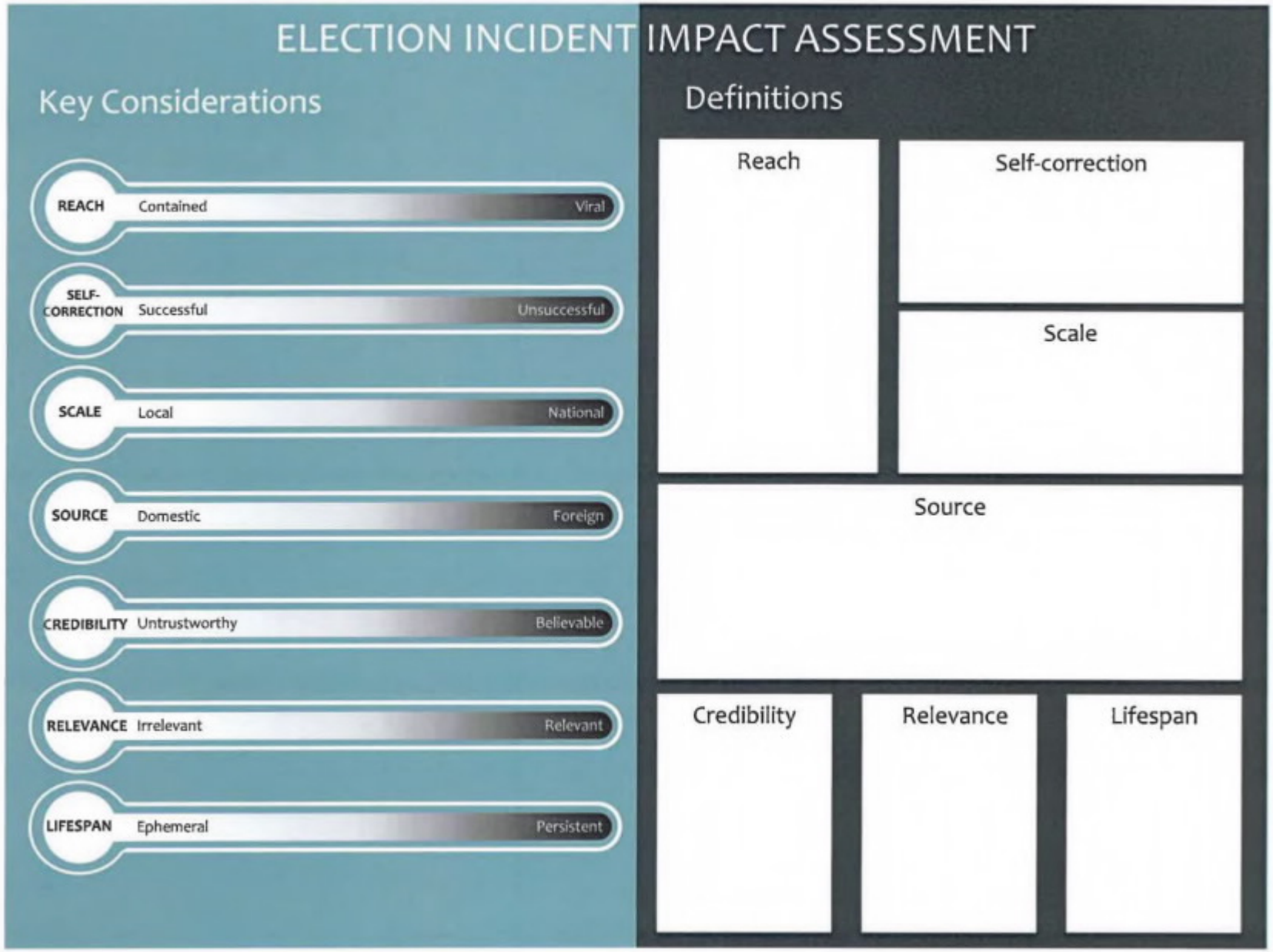
## INCIDENT IMPACT ASSESSMENT



*June 5, 2019*



CAN019677



# ELECTION INCIDENT IMPACT ASSESSMENT

## France
## political campaign leak

On Friday, May 5, 2017, two days before the second and final round of voting for the French presidential elections, a massive trove of communications from the Emmanuel Macron presidential campaign was leaked on the Internet.

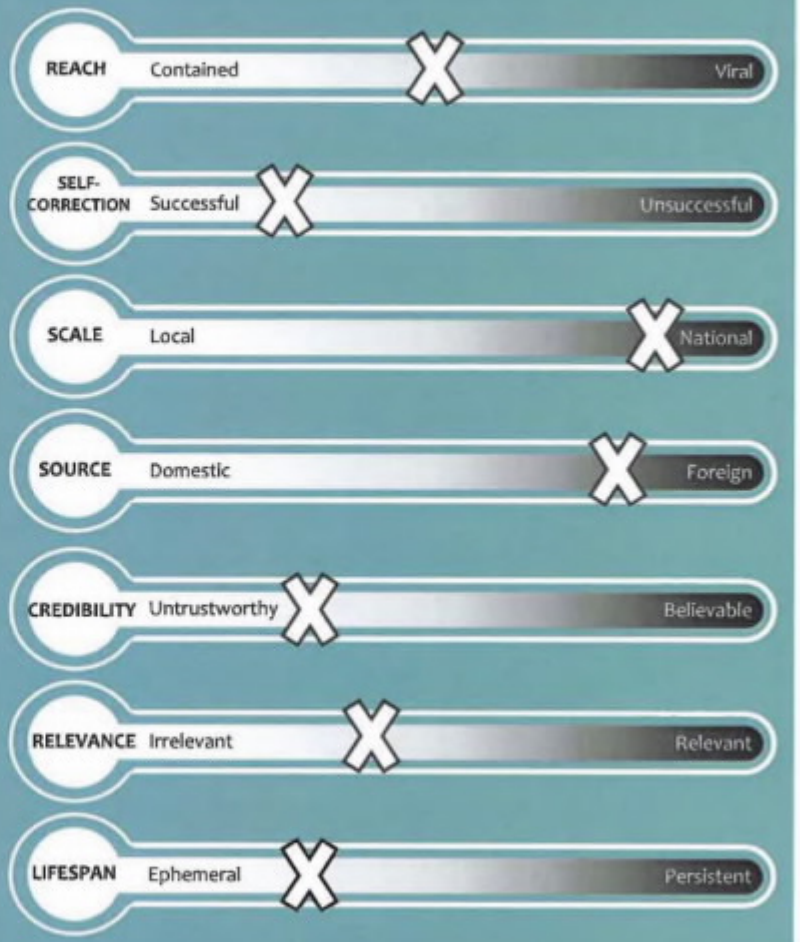
The Macron Leaks, as the breach came to be known, contained 9 gigabytes of stolen communications, or over 20,000 emails.

The attackers released the communications just hours before the 44-hour media blackout period stipulated by French electoral law, when neither news media, nor political campaigns are permitted to directly speak to voters.

The leaks were part of a long-running, Russian state-sponsored operation to discredit the Macron. This campaign also included the diffusion of rumours about Macron's political donors, and personal finances, as well as attempts to infiltrate the campaign through malicious use of computers and spear-phising.

The attackers made numerous errors in the execution of their operation which helped mitigate the effects of the leak. They underestimated the media's resilience in not reporting on the leaks, as well as the tenacity of the Macron campaign, who had falsified emails to prepare, and fought back against the attackers on social media.

## Key Considerations



# ELECTION INCIDENT IMPACT ASSESSMENT

## Germany
## disinformation campaign

In January 2016, Russian and German television companies began airing reports about a German-Russian girl named Lisa, who claimed to have been kidnapped and raped by a group of Muslim Refugees in Berlin.

These reports were widely debunked, but dominated the news cycle for weeks in Russia and Germany.

Despite the story being proven false, Russian diplomats accused German authorities of perpetuating a cover-up, while German officials asserted that their Russian counterparts were partaking in spreading propaganda.

Members of the Russian diaspora across Germany organized dozens of protests and demonstrations.

The Lisa scandal precipitated a rise in anti-migrant sensitivity that aided the far-right Alternative for Germany (AfD) Party months later, in the Berlin state election. The AfD received an unprecedented 14% of votes, and a large number of seats in the legislature, becoming the second largest opposition party.

## Key Considerations